SAN DIEGO STATE UNIVERSITY

INFORMATION SECURITY PLAN

VERSION 1.4

Please send questions and comments to iso@sdsu.edu
Executive Summary

The Information Security Plan applies to San Diego State University and Auxiliary employees, information, systems, processes, and networks (collectively referred to as the University).

San Diego State University is committed to securing information from unauthorized access or modification and preventing damage to systems and networks which are vital to achieving the University’s mission of excellence and distinction in teaching, research, and service. As stated by President Weber in his memo to the University on February 26, 2007, “we also have a fiduciary duty to protect the information entrusted to us by our colleagues, our students, our alumni, and others of our campus community”.

The SDSU Information Security Plan provides University policies, standards, and procedures to appropriately secure information, systems, and networks. The objective of the Information Security Plan is to communicate responsibilities, education, minimum processes, software and configurations, so they can be implemented by the University to minimize risks to information, systems, and networks.

The Information Security Plan consists of this Executive Summary, an Overview, followed by the four sections and appendices:

- **Section 1**: Security Policies and Operational Policies
- **Section 2**: IT Security Incident Response Program
- **Section 3**: Vulnerability Management Program
- **Section 4**: Security Awareness and Training Program
- **Appendix A-P**: Samples and additional details for implementing the plan

Section 1 of the Information Security Plan contains the information security policies, approved by the SDSU Senate, which provide information and technology security governance to the University.

Sections 2 through 4 of the Information Security Plan represent the minimum University standards and procedures required to implement the information security policies, California State University policies, and State and Federal laws. Subsequent to University review, the Information Security Plan is presented to the President’s Cabinet for University adoption.

The Information Security Plan Overview explains, in detail, the University procedures for requesting and reviewing changes to the Information Security Plan policies, standards and procedures. The Overview also describes the University committees and offices involved in managing, reporting, educating, reviewing, and implementing information and technology security. Words and titles, such as “IT manager”, “manager”, “must”, and “should” have important implications which are explained in the Security Plan Overview.

---

1 Appendix N contains the entire text of President Weber’s memo to the campus on February 26, 2007
The roadmap for improvements to the Information Security Plan is based upon a risk analysis model to be explained within the University's Strategic Security Plan. The Strategic Security Plan is a high level document to be developed to outline the multi-year roadmap to continually and intelligently improve information security. The controls, processes, and awareness contained in the current Information Security Plan represent foundations needed to protect against previously measured incidents of malware infections, social engineering, denial of service attacks, and system breaches. The Strategic Security Plan will evolve these foundations each successive year to further protect against known and projected threats against the University.

Although most of the controls in the Information Security Plan were prescribed and accepted prior to release of the plan, University adoption of this formal Information Security Plan establishes a priority to assess and initiate compliance with the Plan within the next calendar year. Many departments will be impacted by the need to focus resources in order to achieve compliance with the Information Security Plan within this timeline. The necessary expenditure of resources by the University is testimony to the commitment to protect information, systems, and networks.
Overview

This section of the Information Security Plan details the procedures for requesting and reviewing changes to the Information Security Plan policies, standard, and procedures. The committees involved with information and technology security are documented and this overview explains the meaning and intention of key words and phrases within the Information Security Plan.

Revisions to the Information Security Plan

The Security Policies, contained in the first section of the Information Security Plan, are reviewed as needed to address new issues and or to provide clarification. The San Diego State University Senate is the University's delegate assembly. Requests for changes to the Computing Security Policy or Acceptable Use Policy must be submitted to the Senate Instruction and Information Technology Subcommittee (IIT). The Senate IIT Subcommittee consists of:

- Nine faculty representatives, one each from College of Arts & Letters, Business Administration, Education, Engineering, Health & Human Services, Professional Studies & Fine Arts, Sciences, Imperial Valley Campus and the Library
- One staff member
- One student member
- Director of Instructional Technology Services or designee
- Academic Affairs Information Technology Coordinator or designee
- IT Security Office designee appointed by Associate Vice President for Financial Operations
- Representative from the IT Manager’s Committee

The Senate IIT Subcommittee reviews and drafts all Security Policy changes and forwards final recommendations to the Senate Executive Committee for discussion and ultimate approval by the University Senate.

The University President has assigned operational responsibility for the Information Security Plan and direction of the IT Security Office to the Vice President of Business and Financial Affairs. The Information Technology Security Office is under direction of the Chief Information Officer who has reporting lines to the Vice President of Business and Financial Affairs. Requests for changes to the operational policies or sections 2-4 of the Information Security Plan are submitted to the Information Security Officer of the IT Security Office. The Information Security Officer drafts revisions to the operational security policies and Sections 2-4 of the Security Plan and follows these steps to receive University feedback regarding the draft document:

1) Internal review by IT Security Office and CIO
2) Reviews by campus committees, campus forms, and Peer review
3) Review by President’s Cabinet
When the document review and update process has completed step 2, the draft document becomes an interim working document until final review and approval by the President’s Cabinet.

The Information Security Plan is reviewed on a yearly basis and changes to policies, standards, and procedures are incorporated into the plan and then resubmitted to the President’s Cabinet for approval according to the three step process listed above. Changes to the Information Security Plan can reflect scheduled implementation of the Strategic Security Plan, changes in risk to the campus, and changes in technology.

**Information Security Committees and Peers**

SDSU is a highly decentralized university with regard to information and technology oversight and implementation. As such, the process of developing, disseminating, and monitoring information security requires collaboration with various University entities. The following committees meet monthly and include security issues, projects, and education on their agendas:

- **IT Managers** – Chaired by University CIO. Non-authoritative, collegial, group designed to provide collaboration for managers with IT responsibility at the divisional level.

- **Senate IIT Subcommittee** – Chair nominated by voting members. Assist the Directors of Instructional Technology Services, the Library, the Academic Affairs Information Technology Coordinator, and other campus Instructional / Information Technology offices, with developing long-range master plans and reviews and recommendations on the mission and services of Instructional Technology Services, the Library and Academic Affairs on instructional and information technologies. The Committee considers any matter referred by the Senate or by the administration of the University and may consider, at its own discretion, other matters relating to instructional and information technologies at the campus and CSU system-wide levels. The committee reviews and provides feedback on campus information technology initiatives as related to instruction, research and operational needs.

- **The Instructional Academic Computing Committee (IACC)** – Co-chaired by Academic Affairs IT Coordinator and Director of Instruction Technology Services. IACC discusses Technology news and issues that affect the campus use of technology and cross college/department reporting lines.

- **IT Security** – Chaired by the Technical Security Officer (TSO). Committee focuses exclusively on information security incidents, tools, and education.

- **The Minimum Workstation and Software Site License Subcommittee (MWSSLS)** – Chair appointed by IT Managers. Subcommittee of IT Managers, the MWSSLS committee is responsible for developing and updating the minimum computer workstation specifications for the campus as well as coordinating software site licenses and volume purchase agreements for the campus.
System Administrators Subcommittee – Chair appointed by IT Managers. Discuss various operating systems and configurations for solving campus and department issues.

The University relies on members of these campus committees to be a liaison for disseminating security information discussed at the meetings and soliciting feedback from their represented departments or colleges to bring back to the meetings or share on the mailing list associated with the committee they serve on.

In addition to collaborating with campus committees, the IT Security Office works with a group of peers to review and refine the Information Security Plan for campus implementation. This Peer Review Group is comprised of:

- Associate Vice President of Financial Operations, BFA
- Campus CIO
- Chair Senate IIT Subcommittee
- Technology Security Officer
- Information Security Officer
- Information Security Professional
- Representatives from each Auxiliary (Associated Students, SDSU Research Foundation, Campanile Foundation, and Aztec Shops)
- Academic Affairs (AA) IT Coordinator
- Student Affairs (SA) Information Security Manager
- CIO University Relations and Development
- Chair of MWSSL and/or System Administrators Subcommittee

The IT Security Office also organizes forum meetings open to the campus, to solicit feedback about the Information Security Plan.

Once the Information Security Plan is adopted, the IT Security Office is responsible for posting, announcing, and educating the University about the plan. The IT Security Office also coordinates with departments and colleges to implement and assess compliance with the Information Security Plan.

**Importance of Titles and Words**

Throughout the Information Security Plan the titles *IT manager* and *manager* are used as identifiers of employees responsible for implementation of security plans, controls, and processes. The titles do not specifically refer to staff with MPP classification. Instead the title *manager* is a general term referring to the faculty or staff that directly manages systems and information.

The verbs *must* and *should* were carefully used throughout the Information Security Plan to direct managers on how much latitude to apply to implementation of the security controls. All deviations from the specific standards in the Information Security Plan require documenting of an exception.
The verb *should* is used to signal that the specific control may not be technically or procedurally possible, or yet fully implemented. When the controls indicated with a *should* are not possible, or in progress, the manager should document either the exception² to the security control, along with the alternate control used to mitigate the risk, or should document the plan for achieving compliance with the standard indicated in the plan.

The verb *must* is used to signal very few exceptions to the control or procedure should exist on campus. All such exceptions must either be specified in the Information Security Plan, or have an exception on file with the IT Security Office.

All exceptions to the Information Security Plan must be reviewed by managers bi-annually to re-evaluate the need to maintain the exception.

---

² Documentation for exceptions is required for noncompliance with either “should” or “must” type controls
# Table of Contents

Executive Summary ........................................................................................................................................ 2  
Overview .................................................................................................................................................... 4  
   Revisions to the Information Security Plan .......................................................................................... 4  
   Information Security Committees and Peers .................................................................................... 5  
   Importance of Titles and Words ........................................................................................................ 6  
1.0 Introduction to the SDSU Information Security Policies ................................................................. 12  
1.1 The SDSU Computing Security Policy .......................................................................................... 12  
   1.1.1 Reasons for a Security Policy ................................................................................................. 13  
   1.1.2 Scope ..................................................................................................................................... 13  
   1.1.3 Privacy Statement .................................................................................................................. 13  
   1.1.4 Authorized Access and Use .................................................................................................... 14  
   1.1.5 Responsibilities .................................................................................................................... 15  
      1.1.5.1 User Responsibilities ....................................................................................................... 15  
      1.1.5.2 System/Network Administrator Responsibilities .......................................................... 16  
      1.1.5.3 Application Developer Responsibilities ........................................................................... 17  
      1.1.5.4 Database Administrator Responsibilities ........................................................................ 17  
      1.1.5.5 Management Responsibilities ......................................................................................... 18  
   1.1.6 Implementation, Enforcement and Appeals ............................................................................ 18  
1.2 The SDSU Computing Acceptable Use Policy .............................................................................. 21  
   1.2.1 Acceptable Computing Use ...................................................................................................... 21  
1.3 SDSU Computing Acceptable Use Policy (Operational Procedures) ............................................ 22  
1.4 SDSU Residential Housing Network Acceptable Use Policy ......................................................... 23  
   1.4.1 Introduction ............................................................................................................................. 23  
   1.4.2 Network Limitations .............................................................................................................. 24  
   1.4.3 User Responsibilities .............................................................................................................. 24  
1.4.4 Access Control .......................................................................................................................... 24  
2.0 Introduction to the IT Security Incident Response Program ......................................................... 26  
2.1 Contact Information and Procedure for Reporting Incidents ....................................................... 26  
   2.1.1 Contact Information ............................................................................................................... 26  
   2.1.2 Reporting Incidents .............................................................................................................. 26  
      2.1.2.1 Non-Emergency Incident ............................................................................................... 26  
      2.1.2.2 Emergency Incident (Urgent/Extremely Urgent): Escalation Reporting Procedure ... 26  
2.2 Types of Incidents ......................................................................................................................... 27  
   2.2.1 Malware Response Table 2.0 .................................................................................................. 29  
2.3 Trojan Horse/Virus/Worm/Key Logger/Spyware Incidents ............................................................. 29  
2.4 Email Incidents ............................................................................................................................... 30  
   2.4.1 Harassment ............................................................................................................................ 30  
   2.4.2 Fraud ...................................................................................................................................... 30  
1.4 SDSU Residential Housing Network Acceptable Use Policy ......................................................... 23  
   1.4.1 Introduction ............................................................................................................................. 23  
   1.4.2 Network Limitations .............................................................................................................. 24  
   1.4.3 User Responsibilities .............................................................................................................. 24  
1.4.4 Access Control .......................................................................................................................... 24  
2.0 Introduction to the IT Security Incident Response Program ......................................................... 26  
2.1 Contact Information and Procedure for Reporting Incidents ....................................................... 26  
   2.1.1 Contact Information ............................................................................................................... 26  
   2.1.2 Reporting Incidents .............................................................................................................. 26  
      2.1.2.1 Non-Emergency Incident ............................................................................................... 26  
      2.1.2.2 Emergency Incident (Urgent/Extremely Urgent): Escalation Reporting Procedure ... 26  
2.2 Types of Incidents ......................................................................................................................... 27  
   2.2.1 Malware Response Table 2.0 .................................................................................................. 29  
2.3 Trojan Horse/Virus/Worm/Key Logger/Spyware Incidents ............................................................. 29  
2.4 Email Incidents ............................................................................................................................... 30  
   2.4.1 Harassment ............................................................................................................................ 30  
   2.4.2 Fraud ...................................................................................................................................... 30
3.5 Change Management .............................................................................................................. 66
3.4 Server Security........................................................................................................................ 63
3.3 Laptop and Mobile Device Security ....................................................................................... 62
3.2 Desktop Security..................................................................................................................... 53
3.1 Information Classification Standard ....................................................................................... 42
3.0 Introduction to the Vulnerability Management Program........................................................ 42
2.12 Finalizing the Incident .......................................................................................................... 41
2.11 Legal or Civil Actions........................................................................................................... 41
2.10 Incident Inquiry Process ....................................................................................................... 40
2.9 Incident Response................................................................................................................... 36
2.9.3 Notification of Incident.................................................................................................... 39
2.9.2 Incident Investigation and Response Team ..................................................................... 37
2.9.1 Incident Containment....................................................................................................... 37
2.8 Incident Investigation Requirements ...................................................................................... 34
2.8.5 Member of NCCN Mailing List....................................................................................... 36
2.8.4 Coordinating with the IT Security Office ........................................................................ 36
2.8.3 Computer Information ..................................................................................................... 35
2.8.2 Turn on Logging .............................................................................................................. 34
2.8.1 Sync with Campus Time Authority ............................................................................... 34
2.7 External Incident Inquiries .................................................................................................... 34
2.6 Undefined Incidents ............................................................................................................... 33
2.5 Inappropriate Use .................................................................................................................... 32
2.5.2 Lost/Damaged/Altered/Unauthorized Equipment ........................................................... 33
2.5.2.1 Unauthorized Network Devices .................................................................................. 33
2.5.2.2 Lost or Missing Equipment ........................................................................................ 33
2.5.2.3 Unauthorized Physical Access ..................................................................................... 33
2.5.1 Unauthorized Data Access ............................................................................................... 32
2.4.6 Sudden High Volumes of Email ....................................................................................... 32
2.4.5 Spam ................................................................................................................................ 32
2.4.4 Attachments ..................................................................................................................... 31
2.4.3 Malware warning ............................................................................................................. 31
2.4.2 Attachments ...................................................................................................................... 31
2.3 Undefined Incidents ............................................................................................................... 33
2.2 Server Security ...................................................................................................................... 36
2.1 Laptop and Mobile Device Security ...................................................................................... 36
2.0 Introduction to the Vulnerability Management Program......................................................... 34
1.6 Incident Investigation Requirements ..................................................................................... 29
1.5 Incident Investigation Requirements ..................................................................................... 29
1.4 Incident Investigating Team .................................................................................................. 27
1.3 Incident Investigation (continued) .......................................................................................... 25
1.2 Incident Investigation ............................................................................................................ 24
1.1 Incident Investigation Process ............................................................................................... 22
1.0 Incident Investigation Process ............................................................................................... 22
3.4.4 Malware Content in Email............................................................................................... 65
3.4.2 Patch Management on Servers......................................................................................... 64
3.3.2 Mobile Data Device Security........................................................................................... 63
3.3.1 Laptop and Mobile Device Security ................................................................................ 62
3.2.3 Standard Hardware and Software Configurations ........................................................... 59
3.2.2 Anti-Virus and Anti-Spyware Management .................................................................... 58
3.2.1 Anti-Virus (AV) ............................................................................................................. 57
3.2.2 Anti-Spyware (AS) ........................................................................................................ 58
3.2.3 Standard Hardware and Software Configurations ........................................................... 59
3.2.2.2 Anti-Spyware (AS) ................................................................................................... 58
3.2.2.1 Patch Compliance Reporting .................................................................................... 56
3.2.1.3 Patch Implementation ............................................................................................... 55
3.2.1.2 Patch Planning .......................................................................................................... 54
3.2.1.1 Patch Planning .......................................................................................................... 53
3.2 Desktop Security ................................................................................................................... 53
3.2.1 Patch Management ........................................................................................................... 53
3.3 Laptop and Mobile Device Security ...................................................................................... 62
3.3.1 Laptop and Mobile Device Security ................................................................................ 62
3.3.2 Mobile Data Device Security ........................................................................................ 63
3.4 Server Security ...................................................................................................................... 63
3.4.1 Server System Builds ....................................................................................................... 63
3.4.2 Patch Management on Servers......................................................................................... 64
3.4.3 Configuration of Services on Servers ............................................................................. 64
3.4.4 Malware Content in Email............................................................................................... 65
3.5 Change Management ............................................................................................................. 66
3.12 Residential Halls ................................................................................................................... 91
3.13 Visitor Security ....................................................................................................................... 92
  3.13.1 Vendors/Consultants ...................................................................................................... 92
  3.13.2 Visiting CSU Staff/Faculty ............................................................................................ 92
3.14 Departmental Assessments ................................................................................................... 93
  3.14.1 Departmental Assessment Form .................................................................................... 94
3.15 IT Security Office Assessments ............................................................................................ 96
4.0 Introduction to the Security Awareness and Training Program ............................................. 98
  4.1 Security Awareness Training ............................................................................................... 98
  4.2 Protected Information Security Awareness ........................................................................ 99
  4.3 Residential Student Security Course ................................................................................... 99
4.4 Security Training for IT Management and Technical Support ............................................. 100
  4.4.1 Strategic Managers ....................................................................................................... 100
  4.4.2 IT Security Officers ....................................................................................................... 100
  4.4.3 Operational Managers ................................................................................................. 102
  4.4.4 Technical Support ........................................................................................................ 103
4.5 Additional Security Activities ............................................................................................. 104
Appendix A: Acronyms .............................................................................................................. 105
Appendix B: Glossary .................................................................................................................. 108
Appendix C: Final Authorities .................................................................................................... 114
Appendix D: Determining Access to Protected Information ..................................................... 115
Appendix E: Patch Management Plan Examples ...................................................................... 116
Appendix F: Acquiring Anti-Virus Software for Home Use ....................................................... 125
Appendix G: Windows XP Workstation Standard Build Sample ............................................. 126
Appendix H: Windows 2003 Server Standard Build Example ................................................... 132
Appendix I: Application Security Attacks and Countermeasures ............................................ 135
Appendix J: Backups and Backup Strategies ............................................................................. 146
Appendix K: Encryption ............................................................................................................... 154
Appendix L: Data Center Physical Security ............................................................................... 156
Appendix M: Recommended Sources of Security Training ....................................................... 157
Appendix N: Memorandum from President Weber ................................................................. 158
Appendix O: Process for Retaining Computing Systems or Storage Drives ............................. 160
Appendix P: References ............................................................................................................. 162
Appendix Q: Version Review Log ............................................................................................. 166
1.0 Introduction to the SDSU Information Security Policies

San Diego State University has adopted the following four information security policies:

- The SDSU Computing Security Policy
- The SDSU Computing Acceptable Use Policy
- The SDSU Computing Acceptable Use Policy (Operational Procedures)
- The SDSU Residential Housing Network Acceptable Use Policy.

1.1 The SDSU Computing Security Policy

The mission of San Diego State University (SDSU) is to provide high-quality education for undergraduate and graduate students, and to contribute to the solution of problems through excellence and distinction in teaching, research, and service. Computers and network resources, including the World Wide Web, play an important and essential role in fulfilling the educational mission of the University. In keeping with this mission, the University endeavors to provide a safe and secure computing environment.

Computing resources (hardware, software, and the data) are vital University assets. All users of SDSU computing resources need to be aware of and respect the value of these resources. By using these resources all users are part of a community responsible for ensuring that data is kept confidential, reliable, and available, and that the integrity of SDSU computing resources is not jeopardized.

San Diego State University recognizes that local, state, and federal laws relating to copyrights, security, and other statutes regarding electronic media and intellectual property bind all members of the University. It also recognizes the responsibility of faculty, management, and system administrators to take a leadership role in implementing existing policies.

To ensure that all members of the SDSU community have a clear understanding of the University's policies regarding computing resources, this document, the SDSU Computing Security Policy, was written and its guidelines implemented. It provides a framework for the implementation and enforcement of computer and network security policies at SDSU. The document assists the faculty, staff, and students in understanding the need for and the means of protecting SDSU's computing resources.

Faculty who require or recommend the use of University technology resources in their courses are encouraged to notify students in their course syllabus of this policy and its possible effect on their academic activities.

---

3 The term University in this document refers to all colleges, departments, and auxiliaries associated with San Diego State University
4 "General Catalog, 1999-2000", San Diego State University
1.1.1 Reasons for a Security Policy

The SDSU Computing Security Policy defines the minimum standards for a common level of security that is to be implemented across all computing and network resources at SDSU. This policy may be supplemented by additional policies and guidelines created by the individual campus units. The supplemental policies will address each unit's specialized security needs with the understanding that they are consistent with the standard defined in the SDSU Computing Security Policy. It is the responsibility of the individual campus units to inform their subset of users regarding any documents specific to their processing environment.

This policy makes an effort to explain the rationale and intent of the policies contained in this document, and where appropriate, provide common examples of forbidden or unauthorized activity. Where examples are provided, they are not intended to be a complete list of authorized or unauthorized activities and are provided only to clarify the intent of the policy. This document also assumes as a condition of use the exercise of common sense, common courtesy, and a respect for the rights or property and privacy of the University and other users.

Issues concerning the "appropriate use" of computing resources, other than those dealing with security or legal issues, are not covered by the SDSU Computing Security Policy

1.1.2 Scope

The SDSU Computing Security Policy applies to all SDSU computing and network resources including computers, software, data, and communication networks controlled, administered, or accessed directly or indirectly by users at SDSU. Privately owned computer systems, when attached to the campus network and/or resources, are subject to the same responsibilities and regulations as pertain to University-owned systems.

The SDSU Computing Security Policy only covers computer security and is not a substitute for other campus policies related to campus computing.

This document addresses five key principles of security and the responsibilities that each individual has:

- Privacy of data
- Data integrity
- Service integrity
- Legal issues
- Authorized use.

1.1.3 Privacy Statement

The University supports each individual's right to privacy when using SDSU computing resources, and will take reasonable steps to ensure security of these resources. However, the University cannot guarantee absolute privacy of electronic communication and computing resources. Each user must recognize that risks exist with regard to the confidentiality of personal
email, data, files and activity logs due to system limitations, software bugs, unauthorized activity, and potential system failures.

Data contained on SDSU computer systems is accessible to authorized personnel. These individuals are responsible for conducting normal system administration activities including diagnosing or correcting problems. Additionally, should suspicious activity become evident and at the request of the appropriate administrative authority, files may be examined by system personnel to determine if a user is acting in violation of the policies defined in the SDSU Computing Security Policy, other University policies, and state or federal statutes. Access to University computer systems and accounts is generally monitored. In addition, systems and accounts may also be more closely inspected or monitored when:

- Activity from a specific account prevents access to computing or networking resources by others
- Usage patterns indicate that an account is responsible for unauthorized or illegal activity
- There are reports of violations of policy or law taking place
- It appears necessary to do so to protect University resources or data or to protect the University from liability
- It is required by and/or consistent with law.

As a public institution, data on SDSU computer systems may also be made available to the public through public record laws. All requests for such data should be immediately forwarded to campus legal counsel.

### 1.1.4 Authorized Access and Use

Access to University information resources may be granted based on the following: relevant laws and contractual obligations, the requester's need to know, the information's sensitivity, and the risk of damage to or loss by the University. Access may be temporarily or permanently revoked for violation of security policy, other campus policies and CSU policies.

The University reserves the rights to limit, restrict, or extend computing privileges and access to its information resources. Data owners, whether departments, auxiliary units, faculty, students, or staff, may allow individuals other than University faculty, staff, and students access to information for which they are responsible. Methods for such access should not violate any license or contractual agreement, University policy, or any federal, state, county, or local law or ordinance; nor degrade the performance of the University community. Access by non-University members is subject to approval by and at the discretion of the system administrator(s) responsible for the information resource(s) involved.

Every authorized user is responsible for the integrity of these resources. All users of computing systems must respect the rights of other computing users, respect the integrity of the physical facilities and controls, and respect all pertinent license and contractual agreements.
1.1.5 Responsibilities

1.1.5.1 User Responsibilities

A user is one who has authorized access to University computing resources. Everyone on or off-campus who accesses a University computing resource, through whatever authorized (or unauthorized) means, is considered a user and is bound by the user responsibilities stated in this policy.

A) Users are ultimately responsible for the effect(s) of computing activity when using a computer.

B) Accounts created for an individual are for the use of that individual only. Computer accounts, passwords, and other types of authorization are assigned to individual users and must not be shared with others. Users are responsible for any use of their account.

C) Use only those computing resources for which authorization has been issued. Do not attempt to obtain system privileges to which authorization has not been granted or give unauthorized access to others.

D) Do not violate the security policy on any computer or network facility, interfere with the authorized computer use of others, or interfere with the normal running of services on any computer system or network. This includes unauthorized modifications to software or hardware of any computer or network, propagating viruses, or excessive network traffic that interferes with the use of others.

E) Users are responsible for the data and information that they are entrusted with and must not disclose confidential or sensitive information without authorization from the data owner. Confidential data transferred over networks should be encrypted to ensure security.

F) Never attempt to intercept, capture, alter, or interfere in any way with the normal transmission data on any computer or network, without prior authorization from the person or persons responsible for that resource.

G) Observe all applicable policies of external computers or networks when using such resources.

H) Report unauthorized use of computing resources or observed gaps in system or network security to your project director, instructor, supervisor, system administrator, or other appropriate University authority immediately upon discovery. Provide system administrators with information about computing activities when a reasonable request is made.

I) Protect their password so that others cannot gain access to their account. Guidelines for good passwords can be found in the password selection part of the Security Plan section of this document.
1.1.5.2 System/Network Administrator Responsibilities

System/network administrator is a user who has special access to one or more than one University computing resource. This special access includes control over the function of said computing resource(s). Technically, one is a system/network administrator if one exercises direct control over the following on a computing resource:

- Hardware
- Software
- Access level (optional)

System/network administrators are bound by all user responsibilities. In addition, they are bound by the responsibilities enumerated for system/network administrators. System/network administrators may also be bound by other responsibilities and definitions herein as appropriate to their designated tasks.

A) A system administrator manages systems, networks, and servers to provide available software or hardware to users for their University computing. A system administrator, with appropriate supervision and authority from management, is responsible for the security of a system, network, or server and is responsible for enforcing this and other campus policies. Access to system administrator accounts and passwords must be limited and on a "need to know" basis.

B) May take reasonable action as authorized by the provisions of this security policy. In addition, action may be taken based on other campus policies, management, or lawful grounds to inspect, monitor, and/or suspend access privileges determined to be necessary or appropriate in order to maintain the integrity of the computer system, network, or protection of other users.

C) Has special access to information and other special computing privileges and will use such access only in performing official duties. Such access shall not be used to satisfy idle curiosity. Access to users' information shall be governed by relevant University policies and procedures as well as State and Federal laws.

D) Must develop, test, maintain, and document effective computer and network security procedures and take reasonable precautions to guard against corruption of software, damage to hardware or facilities, or unauthorized access. This includes installing system patches, security software, and conducting periodic security audits as appropriate for the resource being managed. They must be aware of network topology issues that affect the security of their systems and data. Systems should be configured to run only necessary system services which limits the potential vulnerability of the system. Appropriate backup procedures and disaster recovery plans must be developed.

E) Shall take reasonable and appropriate steps to see that all the terms of the hardware and software license agreements are faithfully fulfilled on all systems, networks, and servers for which they are responsible.
1.1.5.3 Application Developer Responsibilities

An application developer is a user who has access to a University computing resource for the purpose of developing software for use on that system or for any other system deemed appropriate and permissible. Application Developers may be employed by the University in this capacity and/or other capacities as well. For the purposes of this security policy, an Application Developer is one who does any of the following:

- Writing program code
- Writing HTML, CGI or other World Wide Web-based content
- Writing SQL code or other user interface-related tasks
- Facilitating data transmission routines
- Any user performing any like functions as part of the regular curriculum or their course of study.

Application Developers are additionally bound by all the user responsibilities. They may also be bound by other responsibilities and definitions herein as appropriate to their designated tasks. Application Developers shall:

A) Ensure that applications are written in a method consistent with this and other applicable security policies.

B) Apply data transfer methods that maintain the integrity and security of the data using encryption methods when applicable.

C) Apply security patches and close security holes in applications when they are known.

D) Test applications for common security risks.

E) Document code so that others can maintain it.

F) Document software installations so that others can perform maintenance.

1.1.5.4 Database Administrator Responsibilities

A database administrator is a user who has special access to a University-owned or used dataset. Such special access includes control over access to this data, access to the software functioning to present the data and control over said software. The database administrator is bound by all user responsibilities as well as the responsibilities enumerated for database administrators. Database administrators may also be bound by other responsibilities and definitions herein as appropriate to their designated tasks.

A) A Database Administrator (DBA) must maintain knowledge of the data within their trust and is expected to be familiar with the functions to which the data applies, the structure and functioning of the database management systems in which the data resides, and the methods available for accessing the data.
B) A DBA, with appropriate supervision and authority from management, is responsible for the security of the database and is responsible for enforcing this and other campus policies. Access to DBA accounts and passwords must be limited and on a "need to know" basis.

C) Working with the data owner and/or management, a DBA must define the sensitivity of the information in the database and must develop guidelines and procedures for requesting access to database and information in the database. A DBA has special access to information contained in the database and a DBA's access to such information shall be governed by relevant University policies and procedures as well as State and Federal laws.

D) A DBA must protect the database and the information contained in the database from unauthorized access or modification and must develop, test, maintain, and document effective database security procedures.

1.1.5.5 Management Responsibilities

A Manager/Supervisor is defined, for purposes of this document, as an individual who oversees others in the above defined areas, to wit:

- Users
- System/network administrators
- Database administrators
- Application developers

A) Review access of their users

B) Ensure that users comply with security policies and procedures

C) Monitor use to identify problems

D) Remove access when users leave the department or University

E) Translate policies into operational procedures

F) Provide appropriate funding and resources to implement policies and procedures

G) Promote security awareness and training

1.1.6 Implementation, Enforcement and Appeals

A system administrator, network administrator, application developer or DBA shall take action to temporarily limit access to computing resources for the purpose of maintaining integrity of the resource based on the defined security standards of that resource (system) when he or she:
☒ Observes a violation of this policy
☒ Notices an unusual degradation of service or other aberrant behavior on the system, network, or server for which he or she is responsible
☒ Receives a complaint of computing abuse or degradation of service
☒ Is alerted by system-monitoring or management software that indicates a potential security intrusion

Depending on the severity of the violation, users may be subject to any or all of the following:

A) Temporary loss of computing and network access
B) Permanent loss of computing and network access
C) University disciplinary actions
D) Civil proceedings
E) Criminal prosecution

The system administrator shall notify the user of any such action as soon as possible and the user will have an opportunity to respond before any restrictions are made permanent. If the violation is non-serious or unintentional, common sense, reason and sensitivity should be used to resolve issues in a constructive and positive manner without escalation.

If the issue cannot be resolved informally, or if, in the opinion of the system administrator or the user, the violation warrants action beyond a system administrator's authority, the case shall be referred to other authorities, such as the University disciplinary body appropriate to the violator's status:

<table>
<thead>
<tr>
<th>Violator's Status</th>
<th>University Disciplinary Body</th>
</tr>
</thead>
<tbody>
<tr>
<td>Students</td>
<td>Judicial Review</td>
</tr>
<tr>
<td>Staff</td>
<td>Employee's Supervisor or Human Resources</td>
</tr>
<tr>
<td>Faculty</td>
<td>Faculty Affairs</td>
</tr>
<tr>
<td>All</td>
<td>Law Enforcement; when the administrator the law has been broken</td>
</tr>
</tbody>
</table>

Such appeals should be handled by the appropriate disciplinary body expeditiously, so as to minimize the disruption of crucial teaching and research tools.

In all cases where enforcement action is taken, the system administrator must keep accurate records and logs and produce them as required by campus disciplinary bodies or law enforcement officials.
1.1.7 Security Resources

1.1.7.1 Security Audits

In an effort to assess the vulnerability of the campus computing and network environment, periodic audits may be necessary. Such audits may be particular to a specific system or the entire campus computing/network environment, and may be conducted by on-campus personnel or an outside vendor.

Except in extreme cases, the system administrator and their supervisor will be involved in the audit of their systems. This includes prior knowledge that their system will be audited and providing a copy of the results of the audit.

1.1.7.1.1 IT Security subcommittee

The IT Security subcommittee is a forum for technical security concerns, issues and problems. Meetings occur on a regular basis and the entire campus community is encouraged to participate.

The IT Security subcommittee is charged with reviewing and revising this document on at least a yearly basis or as needed.

1.1.7.1.2 Security Related Web Pages

- SDSU Security Web Page
- COAST
- CERT

1.1.8 Legal and Policy Issues

All existing laws (Federal and State) as well as University regulations and policies apply, including not only those laws and regulations specific to computers and networks, but also those that may apply generally to personal conduct.

Misuse of computing, networking, or information resources may result in loss of computing privileges. Additionally, misuse can be prosecuted under applicable statutes. Users may be held accountable for their conduct under any applicable University or campus policies, procedures, or collective bargaining agreements. Complaints alleging misuse of SDSU computing resources will be directed to those responsible for taking appropriate disciplinary action.

1.1.8.1 Federal Statutes

- Federal Family Educational Rights and Privacy Act of 1974,
- Federal Privacy Act of 1974
- Federal Electronic Communications Privacy Act of 1986
- Federal Copyright Law
- Federal Computer Fraud and Abuse Act of 1986
1.1.8.2 State of California Statutes

- State of California Education Code, Section 67100 et seq.
- State of California Information Practices Act of 1977 (Civil Code Section 1798 et seq.)
- State of California Public Records Act (Gov. Code Section 6250 et seq.)
- State of California Penal Codes, Section 502
- California Code of Regulations, Title 5, Section 41301, Student Discipline

1.1.8.3 CSU Policies

- 4CNet Acceptable Use Policy
- (4CNet Acceptable Use Policy currently being revised)

1.1.8.4 SDSU Policies

- SDSU Senate Policies
- SDSU Judicial Procedures Regulations
- (Future SDSU AUP)

1.2 The SDSU Computing Acceptable Use Policy

1.2.1 Acceptable Computing Use

A) Computer users shall be liable for all activities on their accounts. All relevant federal and state laws and all University regulations shall apply. The University shall reserve the right to limit, restrict, or extend computing or communications privileges and access to its information resources.

B) Acceptable Use

- University computing and communications resources shall be used for the University-related activities for which they are assigned
- Proper copyright permissions shall be obtained and sources shall be properly cited
- Users shall not engage in activities that compromise computer security, circumvent controls, disrupt services, or violate computer etiquette.

C) Legality and Enforcement

---

5 Approved by the San Diego State University Senate on April 3, 2001; http://security.sdsu.edu/policy/aup.html
University policies shall not supersede federal or state laws. Illegal actions may result in prosecution.

Violations of University computing policies may result in the revocation of access or the discontinuance of an account or the loss of computing privileges.

D) Privacy. Computer files, electronic mail, and computing accounts are not absolutely private and may be subject to access by various authorized persons, as well as to access in compliance with the California Public Records Act.

E) Operational procedures shall be determined by the Instructional Technology committee of the Senate and reviewed on a periodic basis. Current operational procedures are available at http://security.sdsu.edu/policy/aup-operational.html.

1.3 SDSU Computing Acceptable Use Policy (Operational Procedures)

In accordance with the University Policy File, section VII-A-9 (also available at http://security.sdsu.edu/policy/aup.html, the Instructional Technology Committee is charged with developing and reviewing the operational aspects of the Computing Acceptable Use Policy. Current procedures are below and also at http://security.sdsu.edu/policy/aup-operational.html.

The computing and network resources at San Diego State University are intended to support the mission of teaching, research and day-to-day communications related to service to the community. All users of SDSU computing and communications systems, whether directly or indirectly managed by the campus, must respect the rights of other computing and communications users, respect the integrity of the physical facilities and controls, and respect all pertinent license and contractual agreements.

SDSU Computing users should:

- Keep shared resources, such as network and servers in mind during peak usage times and not unduly overload such resources
- Use University computing and communications resources only for the University-related activities for which they are assigned, and for incidental personal and/or day-to-day communications related to service to the community. (Note: most assigned computer accounts are not intended to be shared. Consult your system administrator before sharing a password, there may be a better way.)

SDSU Computing users should not:

- Use University computing and communications resources for non-University commercial activities without prior written authorization from the University. If the University grants such authorization, the University may assess appropriate charges to recover the costs of providing such services. This applies to all University-owned and University-leased

---

6 Approved by the San Diego State University Senate on February 15, 2000; http://security.sdsu.edu/policy/aup-operational.html
computers, network resources, and computing and communications facilities related to funded research. Substantial use of computing resources for off campus activities (web sites, mass e-mailings, ...) also requires prior written authorization.

- Post material to electronic bulletin boards, news groups, chat rooms, or mail lists which is illegal, inappropriate or otherwise at variance with accepted codes of network etiquette (e.g., Usenet rules published in news.announce.newusers).

SDSU Policies do not supersede federal or state laws. Actions that are illegal and may result in prosecution include, but are not limited to:

- Violation of applicable federal or state laws and campus regulations, including but not limited to the transmission of threats, harassment, defamation, obscenity, and pornography
- Copyright infringement. This includes activities such as making software available for copying on your computer and connecting that computer to the SDSU network.
- Making unauthorized copies of computer data or documentation (CA PC 502(c)(2))
- Using a computer system without permission or authorization (CA PC 502(c)(3))
- Adding, deleting, altering or destroying data or software without authorization (CA PC 502(c)(4))
- Disrupting services or causing a denial or service to a computer system or network without authorization (CA PC 502(c)(5))
- Introducing a contaminant into a computer system or network (CA PC 502(c)(6)).

Violations of SDSU computing policies may result in the disabling of an access/account and/or loss of computing privileges. A student whose access has been disabled or suspended or revoked may appeal the University's action to a review committee (see Computing Disciplinary Action Appeals Procedures). Additionally, violations may subject the user to disciplinary action under University regulations, and criminal prosecution under applicable statutes. SDSU reserves the right to disable or deny access without notice to halt or prevent suspected violations of computing policies. If you are unsure about the permissibility of any behavior or use, send mail to aup@sdsu.edu to request clarification.

1.4 SDSU Residential Housing Network Acceptable Use Policy

1.4.1 Introduction

SDSU provides high-speed Ethernet connections to all campus residential housing complexes including the SDSU Residence Halls, Piedra Del Sol, University Towers, Hardy Apartments, Aztec Apartments, and the Fraternity Complex. This document describes what use is acceptable and appropriate for your residential network connection. By connecting to or using a network connection in your residence, you agree to abide by these policies. We strongly recommend that you review the policies here to fully understand them.

This document is subject to change, and can be referenced at:

http://security.sdsu.edu/policy/housing-aup.html.
In addition to this AUP, you must abide by all other campus and CSU policies (including the SDSU Computing Acceptable Use Policy and the SDSU Computing Security Policy) as well as current State and Federal law.

Comments or questions regarding this policy can be directed to the SDSU Computing Security Officer via email at: security@sdsu.edu or by calling (619) 594-0142.

1.4.2 Network Limitations

All residential housing networks on campus are protected by firewalls as well as packet shaping devices. This ensures that everyone can use their fair share of the network resources and that potential security intrusions from the internet are limited. All network use is logged.

Residential network connections provide bi-directional connectivity to and from the SDSU campus as well as outbound connections to the internet. Inbound connections from the internet to your computer are not permitted by the firewall. Running servers on your computer accessible from the internet is not allowed.

Due to these limitations, some applications may not be available through the firewall. Other applications may be administratively blocked. Peer-to-peer music sharing applications are currently blocked due to copyright and liability concerns. Other applications may be limited if they have adverse effects on the network. A current list of limited applications can be found at: http://security.sdsu.edu/policy/limited-apps.html

1.4.3 User Responsibilities

It is the responsibility of each resident to use SDSU computer and network resources appropriately using common sense, common courtesy, and a respect for the rights or property and privacy of the University and other users. Access is a privilege that can be revoked due to misuse. By connecting to or using a network connection in your residence, you agree to the terms and conditions of this Acceptable Use Policy, other campus computing policies, and current State and Federal law. Furthermore, you agree to accept responsibility for any misuse by other individuals who use your computer or network connection.

Violations of this Acceptable Use Policy will be adjudicated by Judicial Procedures Office, Business Affairs, Academic Affairs, SDSU Human Resources, or law enforcement officials as appropriate. The SDSU Computing Security Officer may temporarily suspend network privileges of any SDSU user while suspected violations are being investigated or adjudicated, even if it affects network services of roommates.

User responsibilities include:

- The University's networks are shared resources. Excessive use of network resources, which inhibits or interferes with the use of these networks by others, is not permitted.
- Users may not run any programs that interfere with SDSU computing or network services. In particular, DHCP and proxy servers are expressly forbidden.
Users must follow proper SDSU network registration procedures. Users may not use or spoof any network address not specifically assigned to them by the University.

Any use, receipt, or transfer of software or data must observe copyright laws, license restrictions and University policies.

SDSU may not be used to provide Internet access to anyone not formally affiliated with the University. Connections to your computer from outside the University, either directly or via proxy, are not allowed.

SDSU may not be used for commercial or profit-making enterprise. Use of these resources for commercial gain is in opposition to the non-profit status of the University.

SDSU services, equipment, wiring or jacks may not be altered nor extended beyond the location of their intended use.

Users may not use SDSU to attempt to circumvent protection schemes or exercise security loopholes in any computer or network component.

Viewing, copying, altering or destroying any file, or connecting to a host on a network without explicit permission of the owner is a violation of this policy. Unauthorized network sniffers are forbidden and violate Federal wiretap laws.

Users may not share University system passwords, use another person's account, even with permission, or allow use of an established connection by someone other than the registered user.

Users may not forge or otherwise misrepresent another's identity through any form of communication.

University network resources may not be used to defame, harass, intimidate or threaten any other person(s). University harassment policies cover all uses of the SDSU network, including email correspondences and newsgroups.
2.0 Introduction to the IT Security Incident Response Program

This Security Incident Response Program provides governance and risk management to the San Diego State University campus in response to infractions of Local, State, or Federal IT computing laws as well as infractions of the SDSU Computing Security Policy. This IT Security Incident Response Program will explain:

- How to detect an incident
- Whom to contact during an incident
- How to prepare for an incident
- Steps that must be taken to investigate and respond to the incident.

2.1 Contact Information and Procedure for Reporting Incidents

2.1.1 Contact Information

The Information Technology Security Office (ITSO) consists of the Technology Security Officer (TSO), the Information Security Officer (ISO) and staff. The IT Security Office must be notified of campus IT security incidents to protect the security of the network and to assure compliance with laws regarding notification of breaches. Follow the directions below for reporting incidents.

Many sections in this SIRP refer the user to their IT Support Staff. See http://www-rohan.sdsu.edu/~facstaff/index.htm for campus IT support staff contact information.

2.1.2 Reporting Incidents

2.1.2.1 Non-Emergency Incident:

For non-emergencies, send an e-mail to itso@sdsu.edu. If e-mail is unavailable, call 619-594-0142 (if after 4:30 p.m., leave a message). Examples of non-emergency incidents include:

- Phishing emails from non-SDSU computer
- Scanning from non-SDSU computer

2.1.2.2 Emergency Incident (Urgent/Extremely Urgent): Escalation Reporting Procedure

When it is urgent that the IT Security Office be contacted immediately for incident response, please use the following escalation procedures:

1. Urgent
   Examples of urgent incidents include:
   - Suspicious materials present on server
   - Malware on a computer with protected information

A. Send an e-mail to security@sdsu.edu. This will send an alert to the Technology Security Officer (7 days a week, 24 hours a day). If e-mail is
unavailable, call 619-594-0142 (Monday-Friday, 8 a.m. to 4:30 p.m., PST). If the incident occurs after 4:30 p.m., leave a message.

B. If no response from the IT Security Office within 24 hours, repeat Step A.

2. Extremely Urgent
A computer being actively hacked or clearly breached is an example of an extremely urgent incident

In the event of an extremely urgent incident, follow these escalation procedures:

A. Send an e-mail to security@sdsu.edu at any time of day or night. This will send an alert to the Technology Security Officer (7 days a week, 24 hours a day). If e-mail is unavailable, call 619-594-0142 (Monday-Friday, 8 a.m. to 4:30 p.m., PST).

B. If no response after 30 minutes:

1. During Business Hours: call 619-594-5901 (Business and Financial Affairs Division, Monday-Friday 8 a.m. to 4:30 p.m., PST) and staff will page the IT Security Office for immediate response. If no response after 10 minutes, repeat this step.

2. After Hours: If the incident occurs after 4:30 p.m., and you have completed Step A and waited 30 minutes with no response, call SDSU Public Safety at 619-594-1991.

For non-emergencies, the Technology Security Officer can be reached at 619-594-4242 and the Information Security Officer can be reached at 619-594-4049.

2.2 Types of Incidents
This section of the SIRP explains indicators of computer hacking, which must be immediately reported to the IT Security Office.

Malware Response Table 2.0 below lists dos and don’ts for users and IT support staff to perform once a hacking incident is suspected.

An intrusion of computer systems via the network is often referred to as “hacking”. There are many ways to detect a hacking incident. Some indicators of hacking on the computer might be unauthorized administrator/root/user accounts, unauthorized use of a valid account, a sudden slow down of a computer, or unknown software installed on the computer. Indicators of hacking from network monitoring might be unauthorized port scanning, password cracking, banner capturing, packet sniffing, or denial of service software running on the computer. Another common sign of uninvited hackers may be the presence of unauthorized copyright material.

Hacking software can turn off malware protection so that the hacking software is not scanned and detected.

Hacking attempts may be reflected in logs with lots of failed logons or other failed connection attempts. Users may experience complete loss or serious slow down of a computer if it has hacking software installed, it attempts to attack other computers, or if the computer is being hit with a denial of service attack.

It is critical that these types of hacking symptoms, successful and failed, be reported to the IT Security Office for investigation. Although one computer may deflect an attack, another computer may fall prey to the attack. **Successful attack reports must be escalated immediately and the computers cease to be used, including use by IT support staff.**

If a system is suspected of being compromised, to avoid inadvertently destroying valuable evidence needed to protect other systems or to prove that protected information was not accessed, users and IT support staff must not:

- Install or run any additional services, patches, upgrades, or other fixes
- Run anti-malware scans or backup software

The IT Security Office has forensic software to preserve as much of the evidence as possible from a compromised computer. **IT support staff must not investigate the computer.** As necessary, the IT Security Office will sequester the computer for further investigation and provide the appropriate manager with a receipt for the computer and a copy of the forensic process.

Reports of hacking or compromise of a computer do not follow normal department or divisional reporting guidelines. **Hacking reports must be escalated immediately to the IT Security Office** to maximize the protection to the other campus systems and networks, and to minimize the risk to the University. Users and IT support staff must follow normal management reporting procedures **after** the IT Security Office has been alerted. The IT Security Office will work in cooperation with Public Safety, other appropriate SDSU departments, and law enforcement to investigate the incident.
2.2.1 Malware Response Table 2.0

<table>
<thead>
<tr>
<th>For incidents involving Trojan horses, worms, key loggers, and hacking</th>
<th>Do</th>
<th>Do not</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Use the computer as little as possible.</td>
<td>1. Perform backups</td>
<td></td>
</tr>
<tr>
<td>2. Allow scheduled tasks to continue until advised otherwise by ITSO</td>
<td>2. Install patches or service packs</td>
<td></td>
</tr>
<tr>
<td>3. If the computer contains protected information, immediately report incident to ITSO prior to steps 4 &amp; 5</td>
<td>3. Install upgrades</td>
<td></td>
</tr>
<tr>
<td>4. Report incident to IT support staff</td>
<td>4. Reconfigure any services or application settings</td>
<td></td>
</tr>
<tr>
<td>5. Report incident to management</td>
<td>5. Install anti-virus software or upgrades or run an unscheduled scan</td>
<td></td>
</tr>
<tr>
<td>6. Install spyware software or upgrades or run an unscheduled scan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Format the disk drive</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Explore or investigate the computer further</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. Create an image or copy information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10. Disconnect the computer from the network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11. Power off the computer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12. Look/touch/save/back up a suspected file or protected information</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2.3 Trojan Horse/Virus/Worm/Key Logger/Spyware Incidents

This section of the SIRP explains different types of infection incidents and the appropriate action to take when these infections are detected.

Another common incident type is malware infections, such as a

- Trojan Horse
- Virus
- Worms
- Key Logger
- Spyware

Malware can be discovered when they run scripted attacks on another computer, or when they perform other noticeable actions on the network. In these cases, where activity is discovered on the network, the user may initially be contacted by the TSO, or other IT support staff, to investigate the suspicious network traffic.
Alternately, the user may see an alert on his or her computer when running (manually or automatically) a malware detection scan. Users must immediately report alerts to their IT support staff and discontinue use of the computer until the alert is resolved.

Malware may send information back to hackers, allowing unauthorized access to information. The IT Security Office needs to be aware of all findings of Trojan horse/worm/key logger software to determine if information could have been shared and if further actions are needed. Spyware, which might send password or other protected information to a hacker, must be reported to the IT Security Office. It is very important that the report be escalated immediately and the computers cease to be used to avoid contaminating important evidence.

Table 2.0 above lists dos and don’ts for users and IT support staff to perform when a Trojan horse/worm/key logger incident is suspected.

### 2.4 Email Incidents

*This section of the SIRP explains different types of email incidents and the appropriate action to take when these incidents occur.*

To facilitate communication among University employees and to direct students and visitors to University resources, the University maintains a directory of employee and departmental email addresses. Unfortunately spammers and other malicious hackers can abuse this openness by gathering the University addresses for inappropriate email messages.

#### 2.4.1 Harassment

An email can be harassing or abusive. Users should save copies of harassing or abusive emails and initiate a complaint with the Office of Employee Relations and Compliance at 619-594-6464.

#### 2.4.2 Fraud

The following types of e-mail generally indicate an attempt to defraud an e-mail recipient:

- Quick moneymaking schemes
- Desperate calls for help
- Helping someone from a foreign country get his or her inheritance
- Sending chain letters to benefit a child with cancer
- Phishing, pharming and/or spear phishing attacks

Phishing involves using emails that are allegedly sent from a trusted source (such as a well known company, bank or financial institution), directing users to visit a web site to invite users to update their password, provide personal or financial information or run some type of software. Phishing relies on users clicking on links which look like they will go to a particular web site but actually go elsewhere (the web address looks legitimate, but it is also forged).
Pharming hijacks DNS entries so that even the phishing-aware user who explicitly types in the web site they want (such as http://www.sdsu.edu) will end up at a different web site anyway. Pharming can be caused by something as simple as a malware script exploit turning off the security options, or as complex as a malware program actually changing the web browser to function differently. Pharming can be prevented by keeping anti-malware definitions current, using host firewalls, and avoiding installing toolbars or helpers downloaded from the Internet.

Spear phishing differs from phishing in that it targets a specific department, division or college, seeking unauthorized access to protected information, and allegedly comes from IT support staff or other professionals in a position of authority from within that department, division or college. As with phishing, the email will attempt to trick users into divulging personal or financial information or credentials.

In general, campus IT support staff do not send unsolicited email to users requesting users follow a web link to install software or change their password. When in doubt, users should confirm the email with the sender or a campus IT support staff (i.e. send a new email asking the sender if the email was legitimate – don’t reply to the forged email address to confirm).

Users must be aware that chain letters involving money or valuable items and promising big returns are illegal. Both starting and forwarding moneymaking or for-profit types of chain letters are against the law. Non-moneymaking chain letters violate the SDSU Computing Acceptable Use Policy in that they can impact the performance of the mail server and hinder the delivery of mail on campus.

Users should forward fraudulent email, after removing attachments, to fraud@mail.sdsu.edu

### 2.4.3 Malware warning

Another email incident is where a user is advised that they emailed malware to another email address. If uncertain whether or not malware might have been sent, users can contact their IT support staff for assistance. If several malware-warning emails are received users should contact the IT Security Office to report an incident.

### 2.4.4 Attachments

The campus email server utilizes anti-malware scanning software to minimize malicious attachments in email. See [http://tns.sdsu.edu/faqs.htm#vir1](http://tns.sdsu.edu/faqs.htm#vir1) for a list of filenames and extensions blocked from receipt by the e-mail server. The anti-malware scanning software relies on signature technology, where the malicious attachments have been researched and signatures identified, however, hackers are constantly designing new attachments unknown to the scanning software. Users must not save or open attachments from unknown senders. When in doubt, contact your campus IT support staff for assistance. Emails containing suspicious attachments must be deleted. Do not forward email unless directed to do so by IT support staff or the IT Security Office.
2.4.5 Spam

Spam, or unsolicited email, is a particular problem with open University email addresses. Spam causes a type of denial of service attack, typically being sent to multiple email addresses on campus, clogging mail servers and filling up individual mailboxes. The campus mail server, mail.sdsu.edu, utilizes anti-spam software. Some client software allows for threshold settings that users can control to help lower the occurrence of spam. Visit http://tns.sdsu.edu/email.htm#spamview for information on the spam scanning software, instructions on how users can adjust their individual spam settings and other measures users can take to avoid receiving email spam. Users can forward spam email to the email administrator (for example, forward to spam@mail.sdsu.edu for campus email server).

2.4.6 Sudden High Volumes of Email

One sign that a system or server has been compromised is the unexpected emailing of large amounts of email (i.e. spamming). IT managers of email systems should have IT support staff utilize automatic warnings to catch this anomaly. IT support staff should first check with the sender to confirm whether or not the mass mailings were intentional. If not, IT support staff should report the incident to the IT Security Office at security@sdsu.edu. It is very important that the report be escalated immediately and the computers cease to be used to avoid contaminating important evidence.

The current campus enterprise anti-virus solution, McAfee anti-virus, has a built in deterrent to block unauthorized outgoing email connections. IT managers should ensure that IT support staff are checking anti-virus logs to catch this anomaly and follow up.

2.5 Inappropriate Use

This section of the SIRP explains action to take when someone violates the SDSU Computing Security Policy.

The SDSU Computing Security Policy provides policy concerning appropriate use of IT equipment and data. Violations to this policy must be reported to the IT Security Office for investigation, who will coordinate with appropriate departments as needed.

2.5.1 Unauthorized Data Access

This section of the incident program explains the appropriate action to take when unauthorized access to protected or sensitive data occurs.

In a situation where someone has received unauthorized access to data, such as sending non-public mail/email to the wrong recipient, incorrect computer access settings, or other non-hacking incidents, the user/IT support staff or manager must contact the IT Security Office to report the incident. The IT Security Office will investigate to determine whether or not sensitive information was compromised as a result of the access. It is important to remember that while sensitive information may not be directly compromised, the IT Security Office investigation will examine all aspects of the access to determine whether or not sensitive information was
compromised indirectly. **It is very important that the report be escalated immediately** and the computers cease to be used to avoid contaminating important evidence.

### 2.5.2 Lost/Damaged/Altered/Unauthorized Equipment

*This section of the SIRP explains the actions to take when equipment has been lost, damaged, altered, or is unauthorized for use on the network.*

#### 2.5.2.1 Unauthorized Network Devices

All firewalls, routers, switches and wireless access points and other network appliances directly connected to the network must be approved, installed, and maintained by the IT Security Office or Telecommunications and Network Services (TNS) personnel. Suspected rogue network equipment must be immediately reported to the IT Security Office at security@sdsu.edu.

#### 2.5.2.2 Lost or Missing Equipment

Any lost or missing computing equipment or storage devices that contain University information (including palm pilots, laptops, desktop computers, external drives, CD-ROMs, DVDs and USB storage devices) containing protected information must be reported immediately to Public Safety and the IT Security Office. The IT Security Office will work in cooperation with Public Safety law enforcement to investigate the incident and ensure no protected information has been compromised. **Users and IT support staff must follow normal management reporting procedures after the IT Security Office has been alerted.**

#### 2.5.2.3 Unauthorized Physical Access

Reports of unauthorized physical access to computers or network equipment must be **escalated immediately** to both Public Safety and the IT Security Office. The IT Security Office will work in cooperation with Public Safety law enforcement to investigate the incident and ensure the viability of the equipment and that no protected information has been compromised. **Users and IT support staff must follow normal management reporting procedures after the IT Security Office has been alerted.**

### 2.6 Undefined Incidents

*This section of the SIRP explains actions to take for an incident not otherwise defined in this program.*

Previous sections of this IT Security Incident Response Program defined common incidents and whom to contact. If an incident occurs involving computers or University information which is not defined in this Program, please contact the IT Security Office at security@sdsu.edu to report the incident and receive instructions on how to proceed.
2.7 External Incident Inquiries

This section of the program explains what to do when entities outside of SDSU report an incident or need information to perform their investigation.

There may be times when an SDSU employee is contacted by someone outside the campus about an alleged incident. The contact may come from law enforcement or the general public via email, letter, subpoena, warrant, or phone call.

- Campus inquiries regarding computing activity, must be escalated to the IT Security Office before being acted upon.
- Campus inquiries from law enforcement via email, letter, subpoena, warrant, or phone call must be directed to the Business and Financial Affairs Associate Vice President of Administration at (619) 594-5901.

The ISO and TSO will work with the inquirer, Public Safety, and other appropriate departments to resolve SDSU involvement in external incidents.

2.8 Incident Investigation Requirements

This section of the IT Security Incident Response Program provides measures to take prior to an incident to aid in the incident response and investigation. The only situation worse than having a serious incident on campus is not being able to determine the source or vulnerability that caused the incident and whether or not the incident is still in progress.

Recognizing that absolute security is an impractical goal, after implementing reasonable security prevention mechanisms discussed in the Vulnerability Management Program of this plan, the University must be prepared for inevitable security incidents. Incident preparation helps to provide necessary information and increases the chance that the source of the incident can be detected, prevented, or stopped and that intruders can be prosecuted to the fullest extent of the law.

2.8.1 Sync with Campus Time Authority

In order to know how an incident occurred, there must be log information stored about the computing environment and the log information must be time synced so that all logs reflect correctly the timeline of the incident activity. In order to have all University systems at the same date and time, the campus network timeservers maintain the official time clock for the campus. IT support staff need to time sync their servers and desktops with ntp1.sdsu.edu and ntp2.sdsu.edu so that all log data is time sync for usefulness in an incident investigation.

2.8.2 Turn on Logging

The most important tool during an IT security incident investigation is log information. Logging information should be retained (either locally on the computer, on a central authority, or on backup tapes) for a year, since many incidents may not be detected immediately. Logging can
provide details of hacking activity and can confirm whether or not protected information was accessed.

IT support staff must enable operating system and application logging to capture important activities performed on the computer. Choices of what to log are dependent on the system type, the software capabilities, and the type of information stored on the computer.

All systems must store successful and failed login attempts, password changes, and anti-malware results. Servers must also log privileged (root or administrator) user activity. All University critical servers should copy their logs to a remote server (mail server, web server, database server, DHCP server, etc). Typically desktop logs are not stored centrally, but this is an option to consider for desktops with protected information. With centralized logging, hackers cannot cover their tracks by removing the log data from the server. Centralized logging also provides a single place to retrieve logs if an incident has occurred.

When possible, database applications should log successful and failed login attempts and privileged usage. Copies of database logs from servers with protected information should also be sent to a centralized logger.

2.8.3 Computer Information

During an incident response, limited information may be available to the TSO about a compromised computer, such as NetBIOS, IP address, and Ethernet address information. The TSO may know the building a computer resides in, but not which department within the building is managing the compromised computer.

IT support staff should maintain a list of servers, desktops and laptops, (and should also maintain a list of copiers and printers) to be capable of locating all computer systems connected to the University network that they support. With this information, IT support staff will be able to quickly confirm the ownership of systems to the IT Security Office during an incident.

The IT Security Office recommends that each Division on campus identify a standard naming convention for computer name/NetBIOS/user login that can aid in identifying IT support staff and end users during an incident. Sample naming conventions:

- Computer name/NetBIOS (15 characters composed of)
  - Example 1:
    - 3 letter college abbreviation
    - 2 letter department abbreviation
    - First initial, last name (up to 9 characters)
  - Example 2:
    - 2 letter building abbreviation
    - First initial, last name (up to 12 characters)
  - Example 3 (hides the user):
    - 7 character tag ID
    - 2 letter building
User name standards:
  - Example 1 (preferred):
    - Email name on file with TNS directory
  - Example 2:
    - First initial
    - Last name (up to 14 characters)
  - Example 3:
    - 5 character abbreviation for course
    - Numerical number up to 10 digits

2.8.4 Coordinating with the IT Security Office

At times campus IT support staff may run software to test or audit systems they manage, which may appear to be hacking. To avoid unnecessary incident investigations, IT support staff must email the IT Security Office at security@sdsu.edu to provide advance notification of port scanning and auditing activity. The IT Security Office will need to know the source and destination IP addresses of the systems to be port scanned. IT support staff must only port scan or attempt to audit systems within their area of responsibility after prior coordination with the IT Security Office and following other applicable Division/Department procedures.

2.8.5 Member of NCCN Mailing List

The campus Network Configuration Change Notice mailing list is used to announce scheduled changes to the network. IT managers should ensure that IT support staff receive these NCCN notices. If the change is scheduled to occur on a critical date or time, the IT manager can contact the Network Manager to request a reschedule. If the change does result in a loss of service, the IT manager should have a designated IT support staff coordinate status with TNS and provide an update to their department as appropriate.

2.9 Incident Response

This section of the Security IT Incident Response Program explains the incident investigation process and procedures followed by the IT Security Office, the Security Incident Response Team (SIRT), and appropriate management during and after an incident.

When an incident has been reported, the IT Security Office will open an investigation into the details of the incident. Top priorities for the IT Security Office during an incident are:

- Scoping the incident
- Containment of the incident
- Protection of protected information
- Continuation of mission critical functionality.
2.9.1 Incident Containment

The TSO and ISO work together to contact IT support staff of systems involved in an incident, giving contact priority to those systems that might contain protected information. If the incident is still in progress, and there exists a threat to protected servers or critical systems, the IT Security Office may enlist the services of the TNS department to shut down network connections to prevent spread of the incident and also prevent a hacker from removing valuable evidence of the crime. Time permitting; the IT Security Office will contact appropriate management to forewarn of the shutdown procedure. Management will work in conjunction with the IT Security Office to contact IT support staff during the shutdown procedure.

The process of contacting IT support staff can take several days, depending on the configuration of IP address, Ethernet address and NetBIOS identification information and depending on the scope of the incident and difficulty in locating the administrators or owners. The IT Security Office will post incident information to the IT Security mailing list. IT support staff should convey ongoing incident communication to affected end-users.

IT support staff may be required to remove systems from the network by the IT Security Office and halt all activity on the systems until the IT Security Office or law enforcement advise. IT support staff may not receive a call back from the IT Security Office or law enforcement for hours or days, depending on the scope of the incident and the number of systems involved. IT support staff should utilize email as much as possible to contact the IT Security Office for instructions. The ISO will create an incident email contact mailing list to keep IT support staff apprised of the incident as much as possible. If the network is down, and the IT Security Office cannot notify the University of an incident, there will be a system status message recorded on the incident hotline, 619-594-5393, for IT support staff to refer to and leave messages.

Compromised systems may be mission critical systems that, if halted, will result in harmful impact to University operations. End users may also have a critical need to access information stored on a compromised computer. Managers or IT support staff need to advise the IT Security Office of these critical needs so that the IT Security Office can examine possible alternatives to removal from the network. The TSO may take forensic images of systems, or retain hard drives for investigation. Departments have responsibility for replacing systems and components to resume production. Only an IT Security Office-authorized designee or law enforcement can take a forensic image of a disk or file of a compromised system under investigation.

2.9.2 Incident Investigation and Response Team

Within one business day after a compromised computer incident is contained, the IT Security Office will convene the Security Incident Response Team (SIRT) to meet and outline further steps in the investigation. The SIRT will be chaired by the Business and Financial Affairs Associate Vice President of Finance. The SIRT is comprised of the CIO, ISO and TSO and a designee from:

---

8 Appendix O explains the IT Security Office process for retaining systems or storage drives.
Additional management and information experts may be invited to provide information to the SIRT, particularly from departments affected by the incident, and as needed representatives from the Center for Human Resources, Faculty Affairs, and Student Rights and Responsibilities. One designee from Associated Students, Foundation, and Aztec Shops will also be invited to join the SIRT if affected by the incident. Legal counsel will be invited as advised by the SIRT.

Appropriate management and the Security Incident Response Team will ultimately weigh the risk of compromised systems being online, or accessed, against the risk of shutting them down. The IT Security Office may enlist the assistance of Public Safety to confiscate compromised systems as needed to protect the evidence, or in response to requests from law enforcement. End users can expect to be without access to compromised and/or confiscated systems for extended periods of time.

The IT Security Office will work in conjunction with on-campus departments, such as Public Safety to investigate and resolve incidents. The IT Security Office will also be responsible for coordinating with off-campus entities.

The ISO will be responsible for documenting the incident, including meeting minutes and the incident response report. The IT Security Office will provide meeting minutes and status reports to all members of the SIRT. Each SIRT designee must have the authority to make risk management decisions on behalf of the department or division he/she represents. The Business and Financial Affairs Vice President will be responsible for keeping the President’s Office and the CSU ISO appraised of the incident. All members of the SIRT, and subject matter experts, must be prepared to provide the President and Cabinet with a briefing, if requested. Information regarding the incident and details will be held protected and on a need-to-know basis until advised otherwise by the SIRT.

All Security Incidents resulting from illegal actions will be reported to the SDSU Public Safety department for further investigation and prosecution. The SIRT will direct the IT Security Office to file an official police report, handing over the investigation to law enforcement, based on information provided by the ISO, TSO, and Public Safety designee. Once a police report has been filed, the incident becomes a criminal investigation led by appropriate law enforcement. As indicated by the enforcement section of SDSU Computing Security Policy, all University faculty and staff must cooperate fully with a criminal investigation by providing both accurate information and relinquishing data and computer systems to authorities or to the IT Security Office acting on behalf of law enforcement, in a timely manner.
Any computers that have been confiscated by law enforcement will first be returned to the TSO for distribution to the original University department owner. The TSO will be responsible for releasing compromised computers and data back to the IT manager. The IT manager must confirm in writing, for incident documentation purposes, that the compromised system(s) will be reformatted and rebuilt properly before connecting them back onto the campus network. As a precaution, the TSO may require that new computer name(s) and IP address(es) be used for the rebuilt computer(s) to prevent further hacking attempts or denial of service attacks. The TSO will scan rebuilt computers to ensure no vulnerabilities exist before authorizing Internet access to them. If TNS was enlisted to assist with the incident, the TSO will provide authorization to restore network access, when confirmation is received that the computer was rebuilt and only clean data copied back onto it, and all users with accounts have changed their passwords. Departments must keep the TSO apprised of any urgent need to return confiscated computers to production.

2.9.3 Notification of Incident

Senate Bill 1386 (also known as California Civil Code 1798.29 or the California Database Notification Act) requires the University follow its notification process immediately to notify all users whose protected information could have been accessed as a result of a computer compromise.

Senate Bill 1386 defines confidential information as one of three pieces of information, when associated with the user’s last name and first initial; if the information is not associated with the user’s name information, then the University is not required to follow the notification process:

1. Social security number, or last 4 digits of SSN with DOB, or Tax ID
2. Driver's license number or California Identification Card number
3. Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

If the last four digits, or more, of the Social Security number, coupled with a date of birth, are stored on the compromised computer, then item number one, Social Security number, will assumed to have been met, since most financial institutions utilize the last four digits as a means to authenticate transactions coupled with the date of birth. Any other partial elements of the above items will not be deemed enough information to meet the definition, or the intentions, of the law.

All encryption algorithms, should meet the minimal campus requirements for encryption. According to the law, if either the name information or the confidential information stored on the compromised computer is encrypted, no University notification process is required.

The University notification to the individuals must take place immediately after law enforcement has determined the notification will not impede the criminal case. In order to comply with the law, each department involved will place sending notifications as their highest priority, aside

See [http://www.privacy.ca.gov/code/ipa.htm](http://www.privacy.ca.gov/code/ipa.htm) to view entire text of California Civil Code 1798.29.
from critical operational duties, by gathering the list of individuals to notify as soon as possible and assigning someone to perform the notification process and coordinate with the ISO.

The ISO should strive to produce notices within two weeks to a month after discovery (depending on the number of files and computers involved in the incident). The University notices will be paid for by the department(s) responsible for managing the breached computer. In the case of shared management of compromised systems, all departments will divide external costs related to notification and inquiry processing. Costs may also include per use charges for an address locating subscription service and the professional services of a subcontracting company which the IT Security Office may enlist to assist with the incident. The ISO will document and keep the SIRT apprised of each step of the notification process, including any delays or risks that may develop. If notices have not been mailed within one month of discovery, the ISO will advise the SIRT weekly of reasons for delay in the notification schedule.

The University’s incident notice consists of sealed notice or letter, printed with official SDSU logo, addressed to the individual at the last recorded address registered with the affected University department, the Registrar, or Center for Human Resources. The University will forward any notices returned with address forwarding information.

The content of the notice will be approved by the SIRT and the President’s Office, and copied to the Business and Financial Affairs Vice President. The notice will contain minimal information explaining the incident, with a reference to a web site page that provides additional details, a contact for incident inquiries, and helpful references to individuals regarding identity theft and fraud. All web site contents will be reviewed and approved by the SIRT and the President’s Office. The SIRT will determine if other methods of notice need to be added to an incident, such as a University-wide email, indexed web page to the SDSU home page, or a press release to the media as indicated by the guidelines in California Civil Code 1798.29.

### 2.10 Incident Inquiry Process

Subsequent to an incident, the University can expect several inquiries from notified users, their parents/spouse, security vendors, and law enforcement. The ISO will draft an Incident Communication Guideline to be used by SIRT designated University individuals to respond to any phone calls/emails/letters/walk up traffic with inquiries regarding the incident. In general the Incident Communication Guideline will direct employees:

1. Not to offer unsolicited information.
2. Advise the inquirer the incident is under investigation (if so)
3. Direct the inquirer to a web site for incident information
4. Provide incident web site or phone contact to submit additional questions
5. Direct reporters to SDSU Marketing and Communications with no additional comments.

The Incident Communication Guideline will be distributed, at a minimum, to the President’s Office, campus Telephone Operators, the Business and Financial Affairs Division Office and any

---

10 About 1 to 4 percent of the total number of notified users will contact the University for additional information.
campus departments mentioned in the notice, web site, campus email, and press releases. Any calls to campus help desks must be directed to the IT Security Office.

Notifying departments will decide whether to handle inquiries directly or to outsource this task to a subcontractor (as approved by the SIRT). The ISO is responsible for training the team performing incident response whether in-house or outside contractor. All media or journalist inquiries will be directed to the Marketing and Communications SIRT designee at 619-594-2585. Reports of identity theft or fraud related to the incident will be directed to the ISO. Reports of network attacks or other compromised computers will be directed to the TSO. Subpoenas for civil action must be served at the Business and Financial Affairs Divisional Office to the Associate Vice President of Administration.

2.11 Legal or Civil Actions

Subsequent to an incident, the University may be reviewed by a governing state or federal agency or a civil action could be brought against the University. The Business and Financial Affairs Division, in coordination with the President’s Office, will represent all complaints and agency inquiries submitted to the University as the result of an IT security incident. Legal counsel will be solicited as needed to respond to complaints or actions. Payment of fines, penalties, or retributions levied by agencies or the courts will be the responsibility of the compromised departments.

2.12 Finalizing the Incident

The incident can be closed when the SIRT is confident that sufficient time has elapsed to respond to inquiries, address any legal or agencies actions, gather incident costs, and close the incident action items. Law Enforcement actions can delay an incident closure for several years. The incident response report will be distributed to the SIRT, affected departments’ management, and any requesting law enforcement and agencies. The report may also be provided to other departments as needed to address disciplinary actions.

As appropriate, and as permitted by the SIRT and investigating law enforcement, the IT Security Office will be responsible for reporting the incident and action item progress and final resolution to the Instructional Academic Computing, Senate Instructional & Information Technology, and IT Manager Committees on campus. The incident reporting to the committees will be limited to the details necessary to increase security awareness and prevention of similar incidents.
3.0 Introduction to the Vulnerability Management Program

The Vulnerability Management Program (VMP) provides the minimum standards and procedures to be followed by the San Diego State University to protect University systems from potential exploitation via inherent or newly discovered vulnerabilities. These standards and procedures are in keeping with Local, State and Federal IT technology and telecommunications laws, as well as the SDSU Computing Security Policy. The VMP will explain security mechanisms for:

- Information Classification
- Desktops
- Laptops and Mobile Devices
- Servers
- Configuration Management
- Accounts
- Applications
- Remote Access
- Network
- Physical and Environmental
- Residential Halls
- Visitors
- Departmental Assessments
- IT Security Office Assessments

The VMP prepares managers and staff to effectively contend with the threats and vulnerabilities to systems, networks, and information entrusted to the University. Some managers have oversight over campus servers, applications, network infrastructure, and datacenters (mail server, People Soft, calendar server, portal, telecommunications, etc.). Other managers are faculty responsible for classroom labs, applications, and systems for teaching coursework or performing research. Still other managers are responsible for technology tools (desktops, printers, faxes, PDA’s, etc.). At times the roles of manager and IT support staff may be one and the same (the same person who manages a system is responsible for applying the appropriate security controls).

Auxiliaries and departments may adopt additional or higher security standards than those listed in the VMP to further increase the security of the resources and information they manage.

This program applies to information in both electronic and non-electronic forms.

3.1 Information Classification Standard

Information is classified according to its sensitivity to loss or harm from disclosure. Information classification is the process of assigning labels to information in order to organize it according to its sensitivity to loss or harm from disclosure.
The CSU draft Data Classification Standard is based on federal laws, state laws, regulations, CSU executive orders, and University policies that govern the privacy and confidentiality of information.

The CSU draft Data Classification Standard applies to all information generated and/or maintained by the CSU (such as student, research, financial and employee information) except when superseded by grant, contract, or federal copyright law.

### 3.1.1 Protected Information Levels

SDSU has adopted the draft CSU Data Classification standard as a minimum information classification standard. This standard outlines three levels of classification to which information must be secured. At the end of this section are tables specifying secure methods for handling the information and the University authorities for approving the handling method.

#### 3.1.1.1 Protected Level 1

Protected level 1 information is information primarily protected by statutes, regulation, other legal obligation or mandate. The CSU has identified standards regarding the disclosure of this type of information to parties outside the University and controls needed to protect the unauthorized access, modification, transmission, storage or other use. Included in this level are:

- Passwords or credentials
- PINs (Personal Identification Numbers)
- Private key (digital certificate)
- Name with credit card number
- Name with Tax ID
- Name with driver’s license number, state identification card, and other forms of national or international identification in combination with SSN
- Name with Social Security Number
- Name with birth date combined with last four of SSN
- Medical records related to an individual
- Psychological counseling records related to an individual
- Name with bank account or debit card information (and/or with password)
- Employee name with personally identifiable employee information
  - Mother’s maiden name
  - Employee net salary
  - Employment history
  - Biometric information
  - Electronic or digitized signatures
  - Parents and other family member names
  - Birthplace (city, state, country)
  - Race & Ethnicity

---

1 Credit card number with expiration date and/or card verification code is also considered protected information
• Gender
• Marital status
• Personal characteristics
• Physical description

3.1.1.2 Protected Level 2

Protected level 2 information must be guarded due to proprietary, ethical or privacy considerations. The final authorities for approving departmental procedures for the use, storage and dissemination of protected level 2 information are listed in Table 3.2. University standards will indicate the controls needed to protect the unauthorized access, modification, transmission, storage or other use of:

☐ Student name with personally identifiable educational records

  • Birth date (full: mm-dd-yyyy)
  • Birth date (partial: mm-dd only)
  • Courses taken
  • Schedule
  • Test scores
  • Advising records
  • Educational services received
  • Disciplinary actions
  • Photograph
  • Most recent educational agency or institution attended
  • Participation in officially recognized activities and sports
  • Weight and height of members of athletic team
  • Grades
  • SDSU identification number (RedID)
  • Race & Ethnicity
  • Gender
  • Transcripts
  • E-mail addresses

☐ Employee name with personally identifiable employee information

  • Birth date (full: mm-dd-yyyy)
  • Birth date (partial: mm-dd only)
  • Emergency contact home address
  • Emergency contact personal telephone number

---

12 Media for educational records may include written documents (including student advising folders), computer media, microfilm and microfiche, video or audio tapes or CDs, film, and/or photographs.
13 Considered directory information by FERPA, but considered non-directory information by SDSU for SDSU student employees.
• Emergency personal contact information (name, cell phone, pager)
• Personal vehicle information
• Personal email address
• Parents and other family members names
• Payment history
• Employee evaluations
• Background investigations
• Photograph (voluntary for public display)

☐ Other

• Legal investigations conducted by the University
• Sealed bids
• Trade secrets or intellectual property such as research activities
• Location of highly sensitive or critical assets (e.g. safes, check stocks, etc.)
• Library circulation information
• Vulnerability or incident information

### 3.1.1.3 Protected Level 3

Protected level 3 is information that is regarded as publicly available. This information is either explicitly defined as public information (such as state employee salary ranges), intended to be available to individuals both on-campus and off-campus (such as employee work email addresses), or not specifically classified elsewhere in the protected information classification standard. Publicly available information may still be subject to University review or disclosure procedures to mitigate potential risks of inappropriate disclosure.

☐ Student information designated as Educational Directory Information:

• Student name
• Major field of study
• Dates of attendance
• Degrees, honors and awards received

☐ Student Employee information designated as Educational Directory Information:

• Student employee name
• Enrollment status
• Department employed
• Work telephone number
• Work e-mail address
• Status as student employee (such as TA, GA, ISA)
Employee information with personally identifiable employee information:

- Employee title
- Employee work email address
- Employee work location and telephone number
- Employing department
- Employee classification
- Employee gross salary
- Name (first, middle, last; except when associated with protected information)
- Signature (non-electronic)
- SDSU identification number (RedID)

SDSU may disclose Educational Directory Information without prior written consent, unless the student has requested the information stay confidential using the "Confidential Directory Information" option in the SDSU WebPortal. Students may change their "confidentiality" status at any time through the SDSU WebPortal.

Non-University (personal) information (both electronic and non-electronic), such as personal credit reports, personal bank statements, or even contact information from a synchronized cell phone should not be stored on University systems as the University does not assume responsibility for securing this information and many systems may not be secured for this information by default. Personal information does not just pertain to first party personal information (yours), but also to any third party personal information (someone else’s).

### 3.1.1.4 Procedures for Protected Information

Figure 3-1, shows the IT manager for each department setting secure procedures for their department. The procedures would incorporate the standards within the Information Security Plan, but may also include other departmental, University and CSU policies and procedures not included in the Information Security Plan. The IT manager for each department is responsible for setting secure procedures for their department. SDSU IT Security Officers can be consulted to clarify standards defined within the Information Security Plan, but the appropriate Authority listed in Appendix L is the final approval authority for departmental procedures. The IT manager should state if operational approval is required every instance the procedure is followed or if approval is granted by following the procedure itself.

Table 3-1 below illustrates the minimum security standard for handling protected information. This table summarizes the content listed in other sections of the Information Security Plan in a one page reference.

Table 3-2 lists the final authorities for approving departmental procedures. Faculty and MPP staff with oversight of information should enlist these authorities when devising secure procedures and processes in their areas. In other words, this chart identifies the final approval authority from Figure 2-1 broken down by specific protected items and organizations.
All protected level 1 and level 2 information handling must be in accordance with approved departmental procedures. Note that access approval to protected level 1 information would also be reviewed by the Vice President, College Deans, or Auxiliary Executive in accordance with the Protected Level 1 Authorization Access Approval process (as described in section 3.1.2).

**Figure 3-1: Creating Secure Departmental Procedures**
<table>
<thead>
<tr>
<th></th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmitted via FAX</td>
<td>1) must be attended at both ends until completion</td>
<td>with approved procedures</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>2) with approved procedures</td>
<td>with approved procedures</td>
<td></td>
</tr>
<tr>
<td>Transmitted outside of SDSU</td>
<td>1) must be encrypted</td>
<td>1) should be encrypted</td>
<td>with approved procedures for aggregate data</td>
</tr>
<tr>
<td>network (includes remote</td>
<td>2) with approved procedures</td>
<td>2) with approved procedures</td>
<td></td>
</tr>
<tr>
<td>access)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transmitted in internal</td>
<td>1) must be encrypted</td>
<td>with approved procedures</td>
<td>with approved procedures for aggregate data</td>
</tr>
<tr>
<td>SDSU network</td>
<td>2) with approved procedures</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Included in Email content</td>
<td>1) must be encrypted</td>
<td>1) should be encrypted</td>
<td>with approved procedures for aggregate data</td>
</tr>
<tr>
<td></td>
<td>2) with approved procedures</td>
<td>2) with approved procedures</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Permanently stored on</td>
<td>with approved procedures</td>
<td>with approved procedures</td>
<td>yes</td>
</tr>
<tr>
<td>desktop computer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(should be accessed via secure file server)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stored on personally-owned</td>
<td>no</td>
<td>with approved procedures</td>
<td></td>
</tr>
<tr>
<td>equipment or at personal</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>home</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stored in database</td>
<td>1) should be encrypted</td>
<td>with approved procedures</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2) with approved procedures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stored on mobile device</td>
<td>1) must be encrypted</td>
<td>1) should be encrypted</td>
<td>with approved procedures</td>
</tr>
<tr>
<td></td>
<td>2) with approved procedures</td>
<td>2) with approved procedures</td>
<td></td>
</tr>
<tr>
<td>Stored on server</td>
<td>1) should be encrypted</td>
<td>with approved procedures</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2) with approved procedures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Left unattended in work area</td>
<td>1) with approved procedures</td>
<td>with approved procedures</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>2) physically secured if accessible by unauthorized individuals</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Paper disposal</td>
<td>1) shred immediately</td>
<td>1) shred</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2) physically secured until shredded</td>
<td>2) with approved procedures</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3) with approved procedures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronic media disposal</td>
<td>1) electronically overwritten or destroyed</td>
<td>1) electronically overwritten or destroyed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2) secured until disposed</td>
<td>2) secured until disposed</td>
<td></td>
</tr>
<tr>
<td>Document, container and</td>
<td>1) should be labeled as</td>
<td>1) should be labeled as</td>
<td></td>
</tr>
<tr>
<td>media labeling</td>
<td>Protected Level 1</td>
<td>Protected Level 2 or Confidential</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>2) should be physically secured</td>
<td>2) should be physically secured</td>
<td></td>
</tr>
<tr>
<td>Left on voice message</td>
<td>1) must have password protected voice messaging</td>
<td>1) must have password protected voice messaging</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>2) with approved procedures</td>
<td>2) with approved procedures</td>
<td></td>
</tr>
<tr>
<td>Discussed verbally</td>
<td>in private area</td>
<td>in private area</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sent through campus mail</td>
<td>1) in sealed container</td>
<td>1) in sealed container</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>2) not visible outside container</td>
<td>2) not visible outside container</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3) tagged “Confidential”</td>
<td>3) tagged “Confidential”</td>
<td></td>
</tr>
<tr>
<td>Sent through postal/common</td>
<td>1) in sealed container</td>
<td>1) in sealed container</td>
<td>yes</td>
</tr>
<tr>
<td>carrier mail</td>
<td>2) not visible outside container</td>
<td>2) not visible outside container</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3) tagged “Confidential”</td>
<td>3) tagged “Confidential”</td>
<td></td>
</tr>
</tbody>
</table>

NOTE: Where several categories apply, use the highest level of security or contact the IT Security Office to clarify (that is, use level 1 versus level 2, and so on)

*Except for Credit Card information for payments to the University which may not be faxed under any conditions

May be technically infeasible for SQLNet, printers, some file sharing, FAX, and copiers

Received email attachments, even encrypted, must be saved to a secure location and deleted from the email

Call phones used for authorized university purposes may store, with approval, and must be encrypted.

The name of the individual does not have to be encrypted

As supported by the application. Documents includes forms. Stamps/stickers with “Confidential” labeling acceptable

Term “Container” does not refer to laptops or mobile devices

In accordance with Federal, State, and Local laws. Does not refer to email.

When possible, best to hand deliver protected level 1 & 2 information

Table 3-1: Handling Protected Information
<table>
<thead>
<tr>
<th>Level</th>
<th>SDSU</th>
<th>The Research Foundation</th>
<th>Aztec Shops</th>
<th>The Campanile Foundation</th>
<th>Associate Students</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>Authority listed in Appendix C</td>
<td>Director of Computing Services</td>
<td>MIS Director</td>
<td>Authority listed in Appendix C</td>
<td>Authority listed in Appendix C</td>
</tr>
<tr>
<td>Mother's maiden name</td>
<td>SDSU IT Security Officers</td>
<td>SDSU IT Security Officers</td>
<td>SDSU IT Security Officers</td>
<td>SDSU IT Security Officers</td>
<td>SDSU IT Security Officers</td>
</tr>
<tr>
<td>Name with Credit card information, bank account, or debit card</td>
<td>Controller for Financial Information</td>
<td>Director of Finance and Accounting</td>
<td>Controller</td>
<td>The Research Foundation Director of Finance and Accounting</td>
<td>Controller</td>
</tr>
<tr>
<td>Name with SSN (including last 4 with birthdate), Tax ID, driver's license, state ID card, or international ID</td>
<td>Authority listed in Appendix C</td>
<td>Authority listed in Appendix C</td>
<td>Authority listed in Appendix C</td>
<td>Authority listed in Appendix C</td>
<td>Authority listed in Appendix C</td>
</tr>
<tr>
<td>Employee Information</td>
<td>Associate VP Faculty Affairs OR Associate VP Administration</td>
<td>Director of Human Resources &amp; Legal Affairs</td>
<td>Senior Director Administrative Services</td>
<td>The Research Foundation Director Human Resources &amp; Legal Affairs</td>
<td>Business Services Manager</td>
</tr>
<tr>
<td>Medical or psychological counseling records</td>
<td>Campus or Department Privacy Officer</td>
<td>Campus Privacy Officer</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Vulnerability or incident information</td>
<td>SDSU IT Security Officers</td>
<td>SDSU IT Security Officers</td>
<td>SDSU IT Security Officers</td>
<td>SDSU IT Security Officers</td>
<td>SDSU IT Security Officers</td>
</tr>
<tr>
<td>Non-directory Educational Records</td>
<td>SDSU Registrar</td>
<td>SDSU Registrar</td>
<td>SDSU Registrar</td>
<td>SDSU Registrar</td>
<td>SDSU Registrar</td>
</tr>
<tr>
<td>Employee Information</td>
<td>Associate VP Faculty Affairs OR Associate VP Administration</td>
<td>Director of Human Resources &amp; Legal Affairs</td>
<td>Senior Director Administrative Services</td>
<td>The Research Foundation Director Human Resources &amp; Legal Affairs</td>
<td>Business Services Manager</td>
</tr>
<tr>
<td>Legal investigations</td>
<td>Associate VP Administration</td>
<td>Director of Human Resources &amp; Legal Affairs</td>
<td>Senior Director Management Services</td>
<td>Chief Financial and Information Officer</td>
<td>Associate Director</td>
</tr>
<tr>
<td>Sealed bids</td>
<td>Contract &amp; Procurement Manager</td>
<td>Purchasing Manager or Director Facilities Planning &amp; Management</td>
<td>Controller</td>
<td>The Research Foundation Purchasing Manager</td>
<td>Controller</td>
</tr>
<tr>
<td>Grants/Proposals</td>
<td>Director of Research Affairs</td>
<td>Director of Sponsored Research Development</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Trade secrets or intellectual property</td>
<td>The Research Foundation Director of The Technology Transfer Office</td>
<td>Director of The Technology Transfer Office</td>
<td>Controller</td>
<td>The Research Foundation Director of The Technology Transfer Office</td>
<td>N/A</td>
</tr>
<tr>
<td>Location of critical assets</td>
<td>Authority listed in Appendix C</td>
<td>Chief Financial Officer</td>
<td>Controller</td>
<td>Chief Financial and Information Officer</td>
<td>Controller</td>
</tr>
<tr>
<td>Library circulation information</td>
<td>Library &amp; Information Access Dean</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Educational Directory Information Records</td>
<td>SDSU Registrar</td>
<td>SDSU Registrar</td>
<td>SDSU Registrar</td>
<td>SDSU Registrar</td>
<td>SDSU Registrar</td>
</tr>
<tr>
<td>Level 3 employee Information</td>
<td>Director Center for Human Resources</td>
<td>Director Human Resources &amp; Legal Affairs</td>
<td>Senior Director Administrative Services</td>
<td>The Research Foundation Director Human Resources &amp; Legal Affairs</td>
<td>Business Services Manager</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>Authority listed in Appendix C</td>
<td>Authority listed in Appendix C</td>
<td>Authority listed in Appendix C</td>
<td>Authority listed in Appendix C</td>
<td>Authority listed in Appendix C</td>
</tr>
</tbody>
</table>

Table 3-2: Approvers for Protected Information Procedures
3.1.2 SDSU Protected Level 1 Authorization Access Approval

SDSU has established the following access approval procedures to satisfy the requirements stated in the March 28, 2003 memorandum from Chancellor Reed. Campus Auxiliaries should also perform an authorization process, at least 3 times a year, to review authorized access to protected level 1 information and provide written confirmation of access approval by the executive staff corresponding to the University Divisional Vice President’s.

A) Have the President, or Vice President of Business and Financial Affairs acknowledge approval of Dean/ Vice President management of all confidential information in the CSU, including current access.

1) Delegation of approval has been signed to Vice Presidents and the College Deans. The Vice President of Business and Financial Affairs will acknowledge the approval of the Vice President’s and Deans.

2) Each Vice President /Dean will gather approvals performed by appropriate manager in their Division/College who has oversight of the information, and has reviewed the University memo “Determining Access to Confidential Data”\(^{14}\), and therefore understands the need to limit access and thereby risk to protected level 1 information. The “appropriate” manager referred to throughout this procedure is the Faculty/MPP manager who manages the collection/storage/distribution of the information, not the system administrator who created the account or access.

For example, many employees have access to SIMS/R protected level 1 information. The manager of SIMS/R will list the faculty/staff he/she authorized to have SIMS/R protected level 1 accounts. The managers of employees (end-users) with protected level 1 SIMS/R accounts will not list their employees, since they only requested the accounts; they did not authorize the accounts.

3) The University will perform the approvals three times per year as approved by the CSU Senior Director of Information Security Management. The dates for Vice President of Business and Financial Affairs signature will be March 1\(^{st}\), July 1\(^{st}\), and November 1\(^{st}\).

4) Delegation of approval will be renewed by the Provost on an annual basis, during the March 1\(^{st}\) semester submission.

5) Protected Level 1 information includes all forms of electronic and non-electronic information (including passwords to that information).

6) The first month of input will include approval of all current authorized protected level 1 access and the repeating cycle will be either a full list again of authorized access, or add/change/delete’s whichever is most convenient for the manager granting access to the information.

\(^{14}\)“Determining Access to Confidential Data” can be found in Appendix D
B) The approval for access must be in a written review that justifies the employee’s need to access as a part of their job duties:

1) The written review can be a memo with a list of employees with similar access or it can be an account request form. The manager must sign the memo/account request form. Scanned electronic memos/forms with signature are acceptable.

2) The memo/account request form must include a brief justification tying the access to the employee’s job. Some memo samples (note the same statements could be made by a manager on an account request form):

Submitted February 2007 for College of Education employees with access to Social Security Numbers:

“These individuals have access to social security numbers and birthdates as they review admission applications to various teacher education programs and to credential applications.

Doe, John
Doe, Jessica”

Submitted March 2007 for College of Education employee access:

“These individuals have access to social security numbers because they work with students’ scholarship applications when assisting students with eligibility information.

Doe, Jane
Doe, Jim
Doe, Jack”

3) The manager will create a spreadsheet with columns containing:

- Employees by last name/first name
- Red ID for employees
- Listing the type of information, with enough detail to match to account request or memo

In the cell for a particular employee row and information column will be a date indicator. The indicator identifies when a written justification was filed with the IT Security Office.

Sample spreadsheet of the access justified in B2:

<table>
<thead>
<tr>
<th>Last, First Name</th>
<th>Red ID Number</th>
<th>Admission Apps with SSN</th>
<th>Scholarship Apps with SSN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Doe, Jane</td>
<td>800111222</td>
<td>Feb 07</td>
<td>March 07</td>
</tr>
<tr>
<td>Doe, John</td>
<td>800222345</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Doe, Jim</td>
<td>800333444</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Doe, Jack</td>
<td>800456789</td>
<td>Feb 07</td>
<td>March 07</td>
</tr>
<tr>
<td>Doe, Jessica</td>
<td>811765432</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4) Justification memo/account request forms are turned in once, when access is granted, but the spreadsheet will be turned in every time there is an add/change/delete to any element in the table.

5) If there are no changes to the spreadsheet the manager can send a memo to the Division Vice President /Dean indicating no changes. The email should be printed and be part of the authorization packet for the Division/College.

C) All employees with protected level 1 or 2 access must sign a confidentiality document.

1) The Center for Human Resources (CHR) provides a listing of employees on a yearly basis who have not signed a confidentiality statement. Managers must compare the list of employees with access against this CHR list to ensure that everyone has signed the statement. Anyone who has not signed the form must fill out the confidentiality statement found on the CHR web site\(^\text{15}\) and turn it in with memos/account request justifications to the Division Vice President /Dean. Managers must contact the Information Security Officer if anyone refuses to sign the form.

2) As of 2004, all new employees have signed the statement as part of new employee orientations in the CHR.

3) Confidentiality statements are filed separately in the CHR and retained until separation from the University.

D) Documentation must be filed in the IT Security Office

1) The designee’s for the Vice Presidents of University Advancement and Student Affairs, and the Deans of Academic Affairs will forward their divisional packets signed by the Vice President /Dean to the Vice president of Business and Financial Affairs each quarter.

2) The Vice President of Business and Financial Affairs will acknowledge the approval of the other division management, approve the Business and Financial Affairs division, and forward all authorization documents to the IT Security Office.

3) The IT Security Office will file the authorization packets by quarter and retain only the past year as confirmed by the CSU Auditor. Confidentiality statements are filed separately in the CHR and retained until separation from the University.

\(^\text{15}\) [http://bfa.sdsu.edu/ps/Revised62503Confidentiality%20Statement.pdf](http://bfa.sdsu.edu/ps/Revised62503Confidentiality%20Statement.pdf)
3.2 Desktop Security
This section of the VMP explains desktop security\textsuperscript{16} in terms of patch management, anti-virus, and anti-spyware implementation as well as documenting standard builds and authorized software.

3.2.1 Patch Management
A proactive patch management plan is a cost effective measure to counteract threats, and is required by the SDSU Computing Security Policy; Management Responsibilities. A patch management plan includes all forms of software revisions such as patches, upgrades, hot fixes and configuration changes. A patch management plan\textsuperscript{17} also includes mechanisms for creating, maintaining and reporting a detailed asset inventory (as outlined in section 3.2.1.1). As this often involves a heterogeneous environment, the patch management plan should include procedures for all operating systems and standard applications.

IT management is responsible for ensuring the implementation of a patch management plan, and for ensuring that it stays current. IT management also needs to ensure that a complete inventory is maintained for all systems (desktops and laptops), to generate regular compliance reports demonstrating the patch management plan is working accurately and effectively.

Due to the assessment and reporting features that are required to keep track of which desktops have and which have not been patched, along with the sheer volume of information about new vulnerabilities; departments should utilize a centralized patch management solution.

Patch management labor costs may be minimized by utilizing the lowest number of servers to patch the maximum number of University desktops. For example, two departments\textsuperscript{18} with similar operational requirements may find it advantageous to utilize a shared patch management solution.

IT management should have regular meetings with IT support staff to discuss the status of the patch management plan to evaluate risks. Topics at these meeting may include new vulnerabilities, patch size, network throughput and system limitations, additional tools or assistance, and special requirements or restrictions. These meetings should be scheduled at least monthly, since many patches have a monthly cycle.

3.2.1.1 Patch Planning
IT managers should ensure that IT support staff generate an inventory to be used in the patch management plan. The inventory should include:

\textsuperscript{16} Personal or non-SDSU systems being used on campus should be held to the same standards of desktop security as SDSU systems
\textsuperscript{17} Examples of a patch management plan may be found in Appendix E
\textsuperscript{18} The term “department” is used throughout this document, but may also be used to represent multiple departments, or even a division; depending on the context of use.
- Computer Name
- Computer Asset Tag (optional)
- System Type (such as server, desktop, laptop, etc.)
- Operating System and Version (such as Windows XP Professional, SP2)
- Software Installed (with version information)
- IP Address
- MAC Address
- Domain or Workgroup Information
- Physical System Location
- User Information
- System Speed, RAM and Disk Size, and Available Space
- Hardware manufacturers (optional but recommended).

With the exception of System Type, all of the above inventory items would preferably be dynamically auto-generated by patch management or inventory software tools.

IT support staff are responsible for understanding the patch requirements of the various operating systems they administer (such as Macintosh, Windows, UNIX and Linux). They will also be aware of preset release dates for vendor patches. For instance, Microsoft uses what it calls “Patch Tuesday” (the second Tuesday of every month) to release all security patches that have accumulated over a period of one month. For preset patch releases, IT support staff has a known, anticipated date around which they can schedule patching.

Since installing one patch might inadvertently uninstall or disable another patch. It is the responsibility of IT support staff to research the dependencies between patches, and to understand any special installation sequence that may be required.

IT support staff must be members of the SDSU IT Security mailing list\(^19\). This mailing list forwards security announcement and vulnerability notifications from mailing lists such as bugtraq, US Cert, eEye VICE, and Secunia, as well as other respected security publications such as Chief Security Officer, Network Computing, Computing Magazine, SANS and InfoWorld.

IT support staff must also join vendor/user operating system and application security mailing lists to be alerted to emerging security and patch bulletins appropriate to the standard software they administer.

Reading the mailing lists should be one of the first tasks performed at the start of the day, continuing every few hours during the day so that IT support staff quickly become aware of vulnerabilities or potentially infected desktops.

Security patches should be deployed within one week of release. IT support staff must be able to coordinate with IT management to deploy emergency patches immediately, in case of active exploits identified on the University network.

\(^{19}\) For information on how to join mailing lists, see the TNS electronic mail page at [http://tns.sdsu.edu/faqs.htm#maj](http://tns.sdsu.edu/faqs.htm#maj)
Patch management progress must be reviewed by IT management, and obstacles resolved and updates charted on a continuous basis.

### 3.2.1.2 Patch Implementation

In order to facilitate testing of patches before implementation, a multi-tier deployment is recommended\(^\text{20}\). In a multi-tier patch deployment, the patch is first tested, and then deployed. A minimum of two tiers are required. In the first tier, the patch is installed on a sample group of desktops, which are then observed for unexpected or unwanted behaviors. If no such behaviors are observed, the patch is then safe to be deployed to the next tier of the desktops.

In some cases, it may be preferable to conduct the testing of the patch over more than one tier. For instance, IT support staff may want to test it against the operating system first, then against the applications; in which case a third tier can be used. Below is an example of how such a three tier patch deployment might be performed:

1) The patch is deployed on a sample group of test (non-production) servers and desktops, which are then monitored for adverse reactions. Testing should be performed on a selection of desktops that represent the configuration of the *operating system software* on the remaining desktops to be patched.

2) When dealing with upgrades or patches, IT support staff should inspect or test the software to determine compatibility with other existing software, or identify any other undesired interactions. If there are no adverse reactions resulting from the first deployment, then the same patch is installed on a larger number of servers and workstations with *application software* that is representative of the remaining desktops to be patched. IT support staff should install the patch on representative production desktops. Users of these desktops should be notified of the patch deployment and instructed to report any adverse effects to IT support staff.

3) IT support staff must check services after patching to ensure that no services were started that should not be running

4) If there are no adverse reactions discovered from the second patch deployment, then the patch is deployed to the remainder of the production desktops. For large deployments, care should be taken to throttle the deployment so as to not affect the patch server capabilities.

An important part of the patch process is the system’s capabilities as they relate to the size of the patch. The available desktop space will be known from the asset inventory. IT support staff must determine details of the patch such as size and other dependencies. This information will enable IT support staff to review the patching issues with IT management, and recommend the best course of action regarding deployment. For instance, IT support staff can ensure there is enough space on each system for the new patches, or allow for a longer period of time for a very large deployment.

---

\(^\text{20}\) Although a multi-tier deployment is recommended when time allows; in situations where there is a threat to the University and/or patching is critical, the most expedient method of patching must be employed.
patch to install on a slow system. Optimal and maximum patch deployment sizes and rates must be agreed upon beforehand to avoid negatively impacting the desktops.

In some cases, it is not possible to deploy a patch to some desktops in a timely manner (such as mobile devices or laptops), in which case, it is preferable to configure the mobile systems to perform automatic updates\(^2\). For automatic updates, the desktop, laptop or mobile system should be set to check for, download, and install patches at least twice a day. Mobile systems should still be scheduled to check in with the patch management software at least twice a month so that the inventory is updated and the IT manager can track patch deployment.

During and after patch upgrades, IT support staff must review the logs on the patch management server to confirm that installation completed successfully and follow up on any problems.

Depending on the capabilities of the patch management software, a patch roll back capability might be available. IT managers should include a process for returning the software to its previous state if available.

**3.2.1.3 Patch Compliance Reporting**

IT support staff are responsible for compiling patch management plan reports for IT management. These should include:

1) A listing of patches deployed with installation reporting
2) A listing by computer of uninstalled patches
3) Documentation of issues or concerns
4) Patch exceptions

IT management will use reports to assess the effectiveness of their patch management plan. Metrics for assessing the effectiveness may depend on such things as homogeneity of environment, resource availability, and so on. After patch testing has been completed and the patches are ready for deployment, all affected systems should be patched within seven days. Extending this interval has the potential of exposing the University computing resources to additional risk.

In situations where systems cannot be patched, IT management must be notified and determine an exception course of action to mitigate the potential vulnerability. Exceptions may arise due to software conflicts or hardware or software limitations.

Exceptions must be fully documented for periodic review, and the IT manager should consult with the IT Security Office on the mitigation mechanisms.

\(^2\) If administrative privilege needs to be granted to a laptop user to complete this task, the risks of using a privileged account should be explained to that laptop user by IT support staff.
IT management will need to review patch exceptions every six months. The prime focus of this review process is to examine options and possibilities that may have changed in the ensuing six month period.

### 3.2.2 Anti-Virus and Anti-Spyware Management

Anti-virus and anti-spyware software should be running as described below on all systems where users open email, browse the Internet, or receive shared files.

Anti-virus and anti-spyware are just one control to detect and avoid malware infections. The best control against infections is to avoid opening email and attachments from unknown users and to browse only “work” related web sites.

#### 3.2.2.1 Anti-Virus (AV)

SDSU has a site license for University and Auxiliary use of McAfee anti-virus (AV) and McAfee ePolicy Orchestrator (ePO) console. Among other things, ePO provides for the central logging and management of McAfee AV agents. As such, most systems at the University should have AV and ePO (or similar products) installed as defensive controls to detect and thwart known AV viruses. The McAfee AV product also contains signatures for the top 200 spyware malware.

IT support staff should ensure the following standards are followed when administering AV and ePO (or other centrally managed anti-virus protection software):

- The anti-virus client should be installed with active protection turned on
- IT support staff should set AV clients to perform daily on demand scans, preferably at the lowest use time on the desktop to minimize the impact to users
- The AV clients should be set to search for updates at least twice a day from the ePO console or from the McAfee site directly if the ePO console is unavailable

---

22 Departments can use software other than McAfee and/or Counterspy, as long as that software can be centralized, and update twice a day.

23 ePO also includes Rogue Detection settings that can be used to automatically disable the wireless network connection on a laptop when it is plugged into the wired network, thus preventing creating a bridge between networks.

24 Details on criteria and procedures for acquiring free copies of anti-virus software for home use may be found in Appendix F.

25 Active protection refers to the ability of the anti-virus software to actively scan the contents of the host system’s memory and file system, to detect and block or delete active viral code before an infection to that host system can occur.

26 The term “on demand” scans is used by McAfee to refer to user initiated or user scheduled scans, whereas “on access” scans refers to real time scans that are continuously running as background processes; other anti-virus and/or anti-spyware vendors may use different terminology for this same functionality.
The ePO console should be set to update the virus signature (DAT) files on an hourly basis.

IT support staff should run an ePO daily report (or a daily report from whichever centrally managed anti-virus system is being used) of infections found in the last 24 hours (or last 3 days on Monday) from on demand scans. Any viruses reported from on-demand scans (other than files in the attachment directory) must be reported to the IT Security Office at security@sdsu.edu. In other words, these viruses may have been installed and running on the desktop before signatures were available to identify them, and the IT Security Office needs to investigate possible repercussions from the infection.

IT support staff should check log entries to ensure that On-Access Scan updates have completed correctly. Correctly completing updates should show log entries of process initiation, process execution and process termination, without time gaps or unexplained absences of detail.

IT support staff should check regularly for agents with outdated DAT files as this can be an indicator of an infection; typically the first thing viruses do is shut off the AV. IT support staff should check the ePO report of outdated DATs daily to be able to respond to critical systems with unresponsive AV. Many desktops have outdated agents due to vacations, surplus, spares, or traveling laptops. IT support staff should follow up immediately for any systems that are known to be booted and in use, but with outdated agent DATs. At minimum, IT support staff should follow up within 5 weeks for any desktops with outdated agent DAT files.

In addition to the standards previously described, IT support staff can use the ePO console’s rule creation capability to create a rule that targets a threat, or the threat type. This is useful for situations where a virus is spreading, and no corresponding DAT file has yet been released.

### 3.2.2.2 Anti-Spyware (AS)

SDSU has purchased licenses for SunBelt Counterspy AS and McAfee AS.

Areas that are deploying McAfee AS also need to include installation of the ePO console to manage both AV as well as McAfee AS. The McAfee AS product contains the extensive list of over 37,000 known AS signatures. The reporting of AS infections is blended into the AV reporting.

The standards for all AS are very similar to AV, although the definition of spyware is greyer and can unintentionally include authorized software. IT support staff should ensure the following standards are followed when using both Counterspy AS and McAfee AS with ePO (or any other centrally managed anti-spyware protection system being used):

- AS clients should be installed with active protection turned on.
The AS console should be set to update signature files on an hourly basis

AS clients should be set to search for updates at least twice a day from the AS console or from the vendor site directly (McAfee or Sunbelt) if the AS console is unavailable

IT support staff should set AS clients to perform daily scans, preferably at the lowest use time on the system to minimize the impact to users. Unlike AV, some software reported as spyware, might be authorized software. If so, IT support staff can set the AS software to by-pass these exceptional files. IT support staff should use caution when setting exceptions to AS scanning, as it is better to dismiss daily reports of false spyware than to shut off scanning potential areas of infection (for instance, it would not be appropriate to by-pass scanning of Internet Explorer plug-ins to avoid false reports of the files used for Oracle)

IT support staff should run a daily report of infections found in the last 24 hours (or last 3 days on Monday) from scans. Any spyware reported from scanning (other than cookies or adware or contained in files in the attachment directory) must be reported to the IT Security Office at security@sdsu.edu. In other words, this spyware may have been installed and running on the desktop before signatures were available to identify it and the IT Security Office needs to investigate possible repercussions from the infection

IT support staff should check regularly for agents with outdated signature files as this can be an indicator of an infection; typically the first thing spyware does is shut off the AS. IT support staff should check the report of outdated agents daily to be able to respond to critical systems with unresponsive AS. Many desktops are outdated due to vacations, surplus, spares, or traveling laptops. IT support staff should follow up immediately for any systems that are known to be booted and in use, but with outdated agents. At minimum, IT support staff should follow up within 5 weeks for any desktops with outdated agent DAT files.

In addition to the standards previously described, IT support staff can use the ePO console’s rule creation capability to create a McAfee AS rule that targets a threat, or the threat type. This is useful for situations where spyware is identified and no corresponding signature has been released.

3.2.3 Standard Hardware and Software Configurations

IT management should ensure a standard hardware and software configurations are applied through the department, whenever possible. A centralized repository for all system images can be used for ease of access, updating and documentation; as well as creating an infrastructure that can grow with the needs of the department.

A typical standard build process for a desktop or laptop system might include processes to:

1) Sanitize the hard drive
2) Load and configure the appropriate operating system modules
3) Turn off unwanted services
4) Schedule and load the appropriate service packs and patches
5) Schedule and update drivers
6) Configure the network settings
7) Configure other hardware settings (video, sound, and so on)
8) Test required operating system functionality
9) Schedule, load and update anti-virus and anti-spyware software
10) Schedule, load and update patch management and inventory software
11) Configure security on screen savers and power options
12) Rename and set passwords for appropriate system accounts
13) Load and configure the appropriate application software
14) Test all required application software functionality.

The exact instructions in the standard build for desktop systems will be decided by the specific needs of the department. IT management needs to meet periodically with IT support staff to review and document specific requirements or changes to incorporate into the standard build and deployment process; such as changes to the current operating system, or the introduction of new standard applications.

3.2.4 Authorized Software

To be considered authorized, software must meet a number of criteria, including:

- It has to be approved by the IT manager
- It must perform definitive functions which support the department’s mission and the needs of the University
- It must be legally licensed for the department’s use.

The IT manager should assess the potential risks and benefits of any software before approving its use. Inappropriate software, such as peer-to-peer file sharing which violates copyright regulations, or installing personal use software, such as screen savers, games and utilities, should not be authorized due to security concerns.

IT support staff must not take actions that are contrary to the licensing agreement of the authorized software. For instance, it is generally not permitted to:

- Make copies of the software for use on desktops for which it has not been purchased
- Put copies of the software on the network unless restricted to authenticated and authorized access
- Obtain copies of software from others without paying the appropriate licensing fee.

IT support staff should utilize system security settings to prevent users from loading or executing unauthorized software on their desktops; as this capability increases the chances of infection by malware, unexpected software interactions, or the introduction of software that may subvert or bypass security controls.

---

28 Sample documentation for Windows XP workstation builds can be found in Appendix G
When dealing with new or custom authorized software, IT support staff should inspect or test the software to determine:

- Compatibility with existing authorized software
- Discover and disable any system utilities that might be used to compromise the operating system or logical access controls
- Identify any other unforeseen interactions, such as starting a new insecure service that IT support staff will need to discover how to turn off and keep off.

IT management will ensure that configuration management procedures for authorized software are followed. Configuration management is the process of keeping track of and documenting approved changes to the system, in order to ensure that they do not unintentionally or unknowingly diminish the security or usability of the system.

### 3.2.5 Centralized Desktop Management Software

IT management should ensure the use of available centralized management software to create and manage:

- Desktop images and installations
- User accounts and privileges
- Desktop system policies and services.

Managing desktops, user accounts, and security policies is critical to the overall success of each department. Performing these tasks locally on each system, however, is inefficient. In addition, inconsistent local management may introduce errors and lead to increased support calls.

Centralized desktop management helps to reduce operational and support costs, and improve security through consistent standard application. In addition, centralized management affords overall change and configuration control, and simplifies many security lockdown processes.

An example of centralized management software is Microsoft’s Active Directory, which provides a hierarchical structure such that IT support staff can delegate and manage the various computer and user accounts in accordance with departmental management guidelines. Delegated administrative support would allow for different departments to share a single Active Directory implementation, and yet be solely responsible for their area or Organizational Unit (OU). In this way, control can be segmented according to areas of support.

IT managers are encouraged to provision the minimal number of centralized management servers necessary to manage their organization (such as at a divisional or college level), to leverage the costs and ease of management. Because of the desktops dependency on the centralized server, IT managers should ensure a fully automated backup server is deployed to provide dynamic redundancy.
3.3 Laptop and Mobile Device Security

This section of the VMP explains issues specific to laptop and mobile device security in terms of access protection, patch management and anti-virus/anti-spyware maintenance. Otherwise, all issues discussed in the desktop security section also apply to laptops and mobile devices.

3.3.1 Laptop and Mobile Device Security

IT support staff should configure laptops and mobile devices to automatically download and install patches at least twice per day. While connected via the wired SDSU network, users must disable the wireless connection to prevent bridging the two networks. If the technology allows, docking stations should be configured to automatically deactivate the wireless network on the laptop.

In addition to the information on the make, model, serial number and tag number of the laptops or mobile devices, IT support staff should document an inventory of all items described in section 3.2.1.1.

If protected level 1 information is stored on a laptop, the information must be encrypted. Although, partial encryption (encrypting only the folder or files containing the protected level 1 information) can be used, full disk encryption should be used to prevent protected level 1 information or user credentials being accessed in the event of the laptop or hard drive being stolen. IT support staff should configure laptops with a commercially supported version of full disk encryption that uses a strong encryption algorithm such as Advanced Encryption System (AES) or triple-DES. Key escrow should be utilized to ensure authorized access to the disk contents in the case of an emergency or access after an employee leaves the University.

Users of laptops and mobile devices (that are not considered primary or desktop systems) should have IT support staff service them at least once per month to ensure that anti-virus, anti-spyware and patch management software is working correctly.

Users must not store login instructions (such as passwords, access codes, remote access numbers or account information) and authentication technology with the laptop or mobile device. When traveling, users must ensure that the laptop or mobile device is locked in a non-visible, secure location.

When the laptop is in use at the office or in a meeting, users must take appropriate measures to prevent the laptop from being stolen.

If a laptop or mobile device is stolen or missing, contact the issuing department immediately. However, if the device contains protected level 1 information, contact the IT Security Office first, in accordance with the Security Incident Response Program.

---

29 Users of non-SDSU or personal laptop are held to the same standards as users of SDSU laptops.
30 See Appendix K for more information on full disk encryption, encryption standards and key management.
3.3.2 Mobile Data Device Security

Mobile data devices such as flash memory drives, micro hard disks, CD and DVD technologies, can pose a security risk. All mobile data devices should be password protected whenever possible. Mobile data devices containing protected level 1 information must be encrypted and stored in a secure location at the University or at another site approved by IT management (including off-site backup services).

CD-R and DVD-ROM are suitable for containing protected information due to their write-once only capability. Flash memory drives, micro hard disks and CD-RW should not be used to store protected information due to their re-usable nature (which could expose protected information that either was or still is stored on the media).

3.4 Server Security

This section of the VMP explains issues specific to server security in terms of server system builds, patch management and anti-virus/anti-spyware maintenance. Otherwise, all issues discussed in the desktop security section apply also to servers.

3.4.1 Server System Builds

IT management must ensure that server system build configurations are documented by IT support staff\(^{31}\). At minimum, this should include:

- Server Name
- Operating System and Version (such as Windows Server 2003, SP2)
- Security Patches
- File System Configuration
- Group Policies
- Local Accounts
- Services Running
- Application Software Installed (with version information)
- Network Settings (including IP address, DNS settings, and so on)
- Domain Information
- Shares with Permissions
- Physical System Location
- User Information
- System Model, Speed, RAM and Disk Size, and Available Space
- Hardware manufacturers (optional but recommended).
- System Image Information (for Rebuilds)

\(^{31}\) Sample documentation for Windows 2003 Server standard builds can be found in Appendix H
IT management must ensure that servers are configured with appropriate redundancies. For example, if necessary, servers should be implemented with a RAID system (either hardware or software based) and/or dual power supplies.

IT support staff should monitor server resource usage, and notify the IT manager in case of problems of potential resource availability.

Documentation for servers behind an internal network firewall needs to be provided to the TSO for review a minimum of two weeks prior to the proposed date of connection to the network.

### 3.4.2 Patch Management on Servers

Due to the operational nature of some servers, patch management often requires a more flexible approach by IT support staff with regard to maintenance schedules. In any case, servers should be updated in a timely manner to reduce vulnerability both for the individual servers and their impact on other networked devices at the University.

IT managers must ensure a pre-arranged patch management schedule exists for each server. This will allow both the server users and IT support staff to effectively schedule their time with regard to the patch management plan.

### 3.4.3 Configuration of Services on Servers

One of the most common vulnerabilities found during SDSU network assessments are unnecessary services running on servers. Servers must be installed with the minimum number of services required to perform their intended function.

IT support staff must tailor installs to only to the services needed. Microsoft Windows 2000, most versions of Linux, and the Sun Solaris operating systems are among the operating systems with excessive services in the default installation.

To examine running services:

- On Windows operating systems the Computer Management console has a link to services. Using the free tool, fport, at [www.foundstone.com](http://www.foundstone.com) under the resources tab, can also help IT support staff to tie open network ports to services running on the system.
- On UNIX, IT support staff can use a combination of ps/netstat/lsof to determine processes running. IT support staff may have to install lsof from a third party if not available with the default operating system.
- For Mac OS X most services are turned off in the sharing panel of the system preferences application, otherwise IT support staff may have to modify the startup scripts.

---

32 This does not refer to host firewalls on systems
One of the services that IT support staff should utilize is system logging\textsuperscript{33}. In addition to retaining a local copy of all logs, copies of key system logs (such as system start up logs, login authentication logs, application transaction logs, and so on) should also be forwarded to a secure central logging server to avoid unintentional or deliberate tampering.

Documenting all system changes will allow IT support staff to compare annotated recordings with saved copies of log files for forensic investigation by the IT Security Office. On critical servers, integrity software such as Tripwire, should also be installed to assist in tracking changes to critical files or folders.

Additionally, server log files must be monitored for critical messages such as:

- Changes to critical system files
- Unusual activity in system logs
- Security patch installation status
- Resource thresholds such as disk space and CPU or memory usage
- Active processes
- Open ports
- Active network connections
- System backup status
- All root or administrator events
- New systems file creation.

Much of the above may be automated with scripts. IT support staff should make use of test servers to experiment with system services or scripts, to build familiarity and check for new vulnerabilities. Once there is a high degree of confidence regarding the security of a script, it can then be used on production servers in accordance with their change management process.

### 3.4.4 Malware Content in Email

IT managers should ensure that servers running email services scan email content before it is delivered to the user’s mailbox to identify viruses and/or spyware and quarantine or delete the malware content from the email before it has been delivered. The user should still receive a notification of the removal of the malware from the email in case there was an error in the identification of the malware content.

\textsuperscript{33} The CSU standard for retention of logs is 6 months to 1 year. Some areas, such as financial, may require longer periods of time according to regulatory requirements. A good rule of thumb is to keep the system logs the same period of time required for the information stored on the server.
3.5 Change Management
This section of the VMP explains how change management can be used to securely control configuration changes to documentation and information and systems.

Change management is the management of changes made to hardware, software, firmware and/or documentation, from baseline, through the end of the life of that system or document.

3.5.1 Change Management of Documentation

Change management is used to track changes made to documentation. Not all documentation needs to be controlled by a change management process. The use of document change management is most appropriate to documentation which is used by two or more individuals as a guidance mechanism; such as this Information Security Plan. IT managers are responsible for incorporating the correct documentation change management in their departments.

Documentation should incorporate the following minimum configuration:

- Document title
- Version number (starting with 1.0)
- Page information (such as page 3 of 27)
- Date of the current version
- Appropriate labeling (such as “draft” or “copy”)
- Appropriate security level tagging (such as “protected level 1”).

Documentation should also contain a change log (either in the front or back of document), and interim versions should be kept as needed for an audit trail.

Available tracking software should be utilized to assist in the capture and documentation of working changes, until the changes are finalized, such as Microsoft Office tracking of changes.

Documents intended for internal department use may have a relatively short review cycle. Once the document is created or changed, it should be reviewed by someone (other than the author) who is familiar with the document contents for accuracy. The document might also be reviewed by someone who is not familiar with the content for clarity, before being incorporated into production.

Documentation intended for inter-departmental or University use may have a longer review cycle; being critiqued and refined a number of times by different departments before being finalized for production.

3.5.2 Change Management of Information Systems

The goal of a change management process for information systems is to track details of changes made to information systems. The level of detail, and number of people involved in the change management process will depend on factors such as the number of IT support staff and/or IT
managers involved in managing the system, the scope of users of the system, and the criticality of the system.

In some cases, the change management process may be very simple. For instance, if a faculty member manages and supports a system used for laboratory assignments, and needs to change the configuration or permissions on that system, the change should be documented for future reference by that faculty member or other authorized staff or faculty member.

If a change affects a number of users or a critical system, such as updating firewall rules or server patches, or if access to protected information is involved; then a minimum change management process should include:

- A description of the change and reason
- Who authorized the change
- The date and time the change was made
- Details of who made the change
- A description of how the change was implemented
- A description of how the change was tested/monitored

The documentation should provide information to track changes in configuration. It is important to be able to ascertain who did what and when, and what the resulting occurrences were. It is also important to include a rollback process to restore operations if a change has undesired effects.

In cases where IT support staff need approval from an IT manager before making a change:

- The IT support staff who require a change to be made to an information system should submit a change request to the appropriate IT manager
- The IT manager must assess the request for potential areas of impact (such as changes to an email server which is also utilized by other departments)
- If multiple potential areas of impact exist, there needs to be a mechanism to communicate the request to have it considered by the other parties that may also be affected
- If the change request is denied, the requestor can refine and resubmit the request for future consideration
- If protected information is involved in the change, the IT support staff must verify that the appropriate manager of the directory or server containing the protected information has signed for approval to access the information before any changes are made.

If the proposed changes have the potential to affect multiple departments, then a more involved process may be required. For instance, if IT support needs to make changes to a server (such as an upgrade) that will make it temporarily unavailable to multiple departmental staff who regularly utilize its services, then:
The planned changes should be submitted to a configuration management team
Appropriate authorization should be secured
An implementation date should be set and the upgrade scheduled
The upgrade should be announced prior to implementation
Affected staff should have a chance to discuss options
A follow up reminder should be sent just before the upgrade
Appropriate precautions (such as backups) should be completed
The upgrade should be completed and tested
The server should be brought back online and restored access confirmed
Users should be notified the system is available
The process should be documented.

Given the decentralized nature of information systems operations at SDSU, a similar process should be adopted for changes that will affect multiple departments, or even be University wide (such as changes to the mail server or the network). Differences in those processes should be more evident at the start of the process, such as increased coordination between IT support staff from each impacted department being required. This increased coordination should be both proactive and committee led. Pre-planning should be utilized at each stage of the process to ensure that the requirements of each department are considered and/or achieved.

3.6 Account Management
This section of the VMP explains issues dealing with the creation and maintenance of all types of user accounts, including operating system based, application based, local and server based accounts, as well as secure account usage and password selection for those accounts.

3.6.1 Account Creation and Maintenance
IT management is responsible for ensuring that users have accounts, which enable them to perform the functions of their job. IT support staff is responsible for creating and maintaining these accounts, as approved by IT management. To protect both the personnel and the information involved, the creation and maintenance of accounts must be done according to an account management process, which includes written management authorization. The account management process must cover:

- Creating and assigning accounts
- Accessing another user’s account(s)
- Disabling, reassigning or deleting accounts.

3.6.1.1 Creating and Assigning Accounts
Three different types of user accounts are discussed in this section:

- Standard
- Privileged
- Generic
1) **Standard User Accounts:**

Standard user accounts (those without administrative privileges) are created and assigned directly to the user, and are uniquely associated with that user. Only the assigned user must know the password to their assigned account. Managers should ensure that users are not requested or coerced to reveal their personal password.

2) **Privileged User Accounts:**

Privileged user accounts (those with administrative privileges, or accounts such as “root” or “Administrator”) should be assigned to users who are required to perform system administration functions, or functions that ordinary user accounts are unable to do.

IT management should ensure that user accounts are assigned only enough privileges and permissions to enable the user to achieve their job functions and responsibilities. For example, some Windows XP users might need to be power users to modify their laptop printer, but they do not need to have administrative authority to enable them to make changes to their operating system.

In some situations users with standard privileges may need elevated access to run specific application software. In these cases IT support staff should adjust the permissions on the specific files or directories associated with the application software for that standard user account. Caution must be exercised since viruses and other malware operating under this user account would also assume this elevated access.

Users who are assigned privileged user accounts (those with system or application administrative access) should also be assigned a standard user account. The privileged user account should only be used for specific and occasional privileged usage (such as system configuration). The standard user account should be used at all other times (such as for daily logins). If the user needs to run an occasional privileged command from their standard account, they can use the “run as” for Windows or “sudo” for UNIX to temporarily elevate their processing privilege for a specific task.

Both the standard user account and privileged user accounts should be associated with a single user. Exceptions to this may be necessary in specific instances when application installation and operation require generic-named accounts (for example, “Oracle”). Care should be exercised when establishing, and assigning, generic accounts due to reduced ability to appropriately attribute actions to a particular individual. Rather than allowing shared use of a named user account, IT staff should create additional named accounts or a shared generic account, even on a temporary basis.

3) **Generic User Accounts:**

Generic accounts are pre-created user accounts (such as User1, User2, User3 and so on), and are the responsibility of the IT manager to which they are assigned. As required, the IT manager can
reassign a generic account to an individual user. Once the account is assigned, the user must then choose his or her unique password, so that the account can then be uniquely attributable to that user. When the user is finished with the account, it must then be reassigned back to the responsible IT manager. The assignment and reassignment of a generic account must be documented by the IT manager with the date, time and name of the user.

Some shared generic accounts are read-only, and often assigned to a group, such as “CustomerSupport”, and may be used for looking up public information in a kiosk or in another services type environment. Since shared generic accounts have limited access, and are assigned to a group, they can be configured to have a longer expiration time, such as six months or by semester.

All generic accounts require a justification approved by the IT manager, who should document the request.

### 3.6.1.2 Accessing another User’s Account or Information

At times, there may be a need for one University user’s account, or files, to be accessed by another University user. Authorization for granting access to account information must come from the appropriate MPP manager of the user’s files being accessed. Managers need to ensure a written process exists to grant operational access to and/or control of a terminated or otherwise indisposed employee’s information/account to the employee’s supervisor (or another employee). This process must include a request to change the password of the account being accessed, so that the employee to whom the account belongs will know that it has been accessed. The Associate Vice President for Faculty Affairs (for faculty employees) and the Associate Vice President for Administration (for non-faculty employees) can approve operational procedures for access to employee accounts and files, for University business, without notification to the employee (as per Table 3.2).  

On occasion the University conducts investigations for infractions of University policy or unlawful activity which requires a non-operational need to access to accounts or files. This non-operational need to access employee accounts and files must be approved by the Associate Vice President for Administration (as per Table 3.2).

### 3.6.1.3 Disabling, Reassigning or Deleting Accounts

Requesting managers are responsible for tracking and documenting the utilization of user accounts in their charge, and must ensure that accounts are disabled or deleted when an employee transfers or is terminated. Requesting managers are also responsible for tracking the expiration dates on generic, shared generic or temporary user accounts. Approving managers should be notified whenever an employee is terminated, or alternatively, a list of active accounts

---

34 Public Request Acts for access to information must be submitted only to the Associate Vice President for Administration.
should be sent periodically to approving managers for confirmation that employees are still using them.

IT support staff are responsible for disabling or deleting the accounts as instructed by IT management, and for generating a list of active accounts on a quarterly or semesterly basis for review by IT management.

### 3.6.2 Secure Account Usage

1) **Using Any User Accounts**: All users are responsible for keeping their password confidential. Users must not share account access information with another user, embed passwords into programs, or write down and leave unattended account information.

Users should schedule resource intensive operations such as transferring large files, mass emailing, and large print jobs at off-peak times, to ensure sufficient resources are available for other users.

User accounts should only be used for University related activities. Only software that has been authorized by the IT manager for University use should be installed on systems. Inappropriate software, such as peer-to-peer file sharing, and personal use software (such as screen savers, games and utilities), should not be authorized due to security concerns.

Instant messaging (IM) is an increasingly popular method for communicating over the Internet. As with any technology that has information security risks, IM should only be used for University business. IM is a real-time supplement to and, regarded by some, as a replacement for e-mail. However, IM also has inherent security issues which IT managers and IT support staff need to understand:

- Instant messaging networks provide the ability to not only transfer text messages, but also the transfer of files. Consequently, instant messengers can transfer worms and other malware
- Instant messengers can also provide an access point for backdoor Trojan horses
- Hackers can use instant messaging to gain backdoor access to computers without opening a listening port, effectively bypassing desktop and perimeter firewall implementations
- Finding victims doesn’t require scanning unknown IP addresses, but by selecting from an updated directory of buddy lists
- In addition to client-initiated file transfers, all the major instant messaging networks support peer-to-peer file sharing where one can share a directory or drive. This means that all the files on a computer can be shared using the instant messaging client, leading to the spread of files that are infected with a virus or other malware
- Information being communicated with IM is vulnerable to unauthorized viewing.
Users should log out or lock their workstation if leaving it unattended for more than a few minutes. User accounts should automatically password lock the desktops after no more than 15 minutes of inactivity, as an added measure of security.

2) **Using Privileged Accounts:** Users with privileged accounts (such as IT support staff) should be especially vigilant regarding the heightened capabilities that their accounts allow.

In addition to ensuring that their desktop systems are patched with security patches, anti-virus and anti-spyware as soon as possible (for instance, within two days of the patch being released), being cautious about the installation of non-authorized software onto their desktop systems, and being careful about browsing non-trusted web sites; users should use secure protocols (such as SSL or SSH) when connecting to servers from their desktop systems using their privileged user accounts.

There are some special privileged accounts (or roles) that are built-in to the system by default, such as “root” (or super user) in UNIX and Linux, “Administrator” (or Power User) in Windows, “enable” in Cisco, or “oracle” in Oracle. These special privileged accounts require special consideration:

- IT support staff should avoid using “root” or “Administrator” for direct logins
- The passwords for privileged accounts should be changed every three to six months; or immediately when a system administrator departs or is transferred This applies especially to accounts which use shorter passwords, or those associated with devices without access control lists
- Privileged accounts should not be configured to automatically lock out the account for console login (either through inactivity or unsuccessful login attempts), but should be configured to lock out the accounts from remote access or network login. This is to prevent self-induced denial of service when an incorrect password is used.

Unused default accounts that are built-in to the system (such as the “Guest” account in Windows) should be left disabled, or if needed, should have the password changed and/or direct login disallowed.

### 3.6.3 Passphrase Selection

Passphrases should be used whenever the technology allows (Windows 2000 and 2003 systems will allow the use of passphrases, where as some UNIX systems will not). A passphrase:

- Serves the same function as a password
- Are generally longer than a password and may include whole words
- Are easier to remember because they are based on phrases that mean something to the user. For example; "Only 3 more weeks until vacation time!"
Systems using passphrases should be configured to use passphrases of 17 characters or more.

Wherever possible, passphrases should be used instead of passwords. Not only is a multi-word passphrase harder to crack than single word password, but the complexity may extend the period of time required between selecting new passphrases.

### 3.6.4 Password Selection

The key to good password selection is a password that is hard for an attacker to guess or crack, and yet a user is able to remember it without having to write it down.

1) **Choosing a Good Password**: Passwords should be a minimum of eight characters in length, and should contain at least three of the following four classes of character types:

- Upper case alphabetic characters
- Lower case alphabetic characters
- Numeric digits
- Symbols (such as !, @, #, *, ?).

Additionally, passwords should not contain:

- Any sequences of more than three character types in a row (so “abc” would be an acceptable part of the password, but “abcd”, “5416” or “**!#” would not)
- Hacker language (such as P@$$w0rd)
- Words from any dictionary in any language
- Words from any dictionary in any language spelled backwards

Other ideas for strengthening passwords include the use of the Unicode character set (for example, ALT+128 is the character Ç, while ALT+0128 is the character €). When using symbols in a password, users should be aware of any special functions that the application they are logging into uses. For instance, when logging into Oracle, the “!” character cannot be used in a password.

Examples of poor passwords choices that should never be used include:

- Family member or pet names (such as Jimmy or Rex)
- Birthdays
- Phone numbers
- Addresses lived at (current or previous)
- Model of car (such as Ford or Toyota)
- License plates (such as “JBC1998” or “MRMOOSE”)
Words people associate with you (such as “Keep Smiling” or “Have A Good Day”)  
- Hobbies (such as “DivingSanDiego” or “Kayak”).

2) **Supporting Good User Password Selection:** In order to ensure that users follow good password procedure for both standard and privileged accounts, IT support staff should ensure that they:

- Configure password to expire every 90 days or semester. The system should be configured to provide advanced warning of password expiration.
- Configure the password history to the highest setting that the technology will allow to prevent users from ever reusing their old password.
- Enable technology that prevents brute force attacks and configure the system to lock or delay after 15 minutes (or less) of inactivity, or after 15 unsuccessful login attempts.
- For accounts without access to protected information, the user account may automatically unlock after a period of ten minutes or so. For accounts that have access to protected information, IT support staff should manually unlock the user account (in order to protect against automated or scripted brute force attacks).
- Configure the settings of both applications and operating systems to use the strongest level of encryption for passwords.

Other ideas for supporting good password selection may include utilizing existing technology to prevent users from bypassing limited history controls by changing their passwords repeatedly.

Additionally, IT support staff should test user account password strength on a quarterly or semesterly basis (by running password cracking programs on the password file for one day to two weeks), and generate a list of accounts that are beneath the standard password strength threshold for follow up by the IT manager.

If a user reports being locked out of their account, but has not attempted to login 15 times unsuccessfully; IT support staff should investigate server logs to ensure that a hacking attempt has not occurred.

IT managers should develop a process by which IT support staff can appropriately identify users before resetting their passwords.

If a password is generated, or reset, by IT support staff; it should be set to a temporary, strong password. The user should be forced to change the password the next time the user logs into the system or application.
3.7 Application Security
This section of the VMP outlines methodologies by which the security of applications can be tested, and vulnerabilities mitigated.

The realm of application security covers the growing myriad of SDSU web browsers, web servers, front-end application servers, back-end application servers and database servers, all connected with protocols such as HTTP, HTTPS or SQL.

There has been a marked shift in Internet attacks, away from the network layer, towards the application layer (such as exploiting PHP vulnerabilities, cross site scripting and so on).

Web services are typically used to present public interfaces, and as such are employed as building blocks by many web applications, which in turn interface them with databases, and so on. However, there has been a distinct increase in attacks aimed at the application layer, with web applications becoming one of the most focused upon areas for potential intruders:

“The statistics are alarming: Gartner estimates 75 percent of attacks against Web sites take place at the application layer. Most of the vulnerabilities documented by Symantec in the second half of 2005 were found in Web application technologies. And a majority of the 20 most severe vulnerabilities in the US-CERT database are Web application flaws.”

Due to the extensive use of web based services at the University, IT support staff need to understand the security implications behind this use of the web. For example, a typical web services application might consist of a web browser and a web server. A security control in the browser (such as a JavaScript) can be set up that prohibits the user from entering a specific text string (such as the word “centralization”) into an input screen that gets sent to the web server. However, if a hacker places a proxy server between the web browser and web server, the information can be intercepted after it is sent from the browser, modified to include the word “centralization”, and forwarded to the web server. This example illustrates that security controls on the client side alone are not sufficient, and that there needs to be security controls verifying the input and output on the server side as well.

3.7.1 Application Security in the System Development Cycle

The most effective place to address application security is during the development of the application. A 2004 Gartner Research study concluded that the cost of addressing security vulnerability during the development cycle is less than 2 percent the cost of removing such a defect from a deployed production application. IT programmers and developers need to

understand how application security can be built into the system development cycle, by testing for and mitigating vulnerabilities at each stage of the cycle.

Regardless of the development methodology, security based techniques need to be incorporated at each phase of the development cycle in order to ensure resistance to attack in the final product. Broad principles, rather than specifics are outlined in this section, so that IT support staff can understand the principles involved in building security into the five phases of the development life cycle; requirements analysis, design, implementation, testing and deployment, and maintenance.

1) Requirements Analysis: Security vulnerabilities not addressed during this phase will be compounded in later phases. IT support staff needs to be able to state not only what the system should do, but also what it should not do. For each use case (what the system should do) that is written, a misuse or abuse case needs also be created to describe how a malicious user might interact with the system. Specific security objectives need to be defined and translated into concrete requirements.

2) Design: The priority in the translation of requirements to application functionality is to ensure the incorporation of security principles such as secure access, storage and processing within the application design. Designing security into the processing aspects of an application means setting boundaries and defining reactions to undesired events. During this phase, issues to be addressed will include such things as:

- Choice of algorithm and key strength for encryption processes
- Use of secure protocols (such as IPSec, SSL or Secure RPC)
- Mechanisms for authentication and access control
- Mechanisms for implementing the rules for all forms of information input and interaction
- Mechanisms for memory separation and isolation of sensitive information.

3) Implementation: A focus on security in the requirements and design phase will set the stage for writing secure code. However, mistakes occur, and controls need to be in place to catch improper implementation procedures. Such controls include processes such as coding standards, code review (manual or automatic), unit testing and defect management.

Creating proper error handling, avoiding dangerous code constructs, implementing input validation, implementing encryption and ensuring secure endpoint communications are all part of secure code writing.

---

Secure code writing is in turn dependent on rigid secure code standards. The coding standards need to be meticulously maintained, up to date, and available for reference by all IT support staff. The coding standards will handle such things as; safe handling of string and integer results, methods of input information validation, handling of temporary files, authentication of code libraries, use of non-constrained methods, proper error handling, and code review criteria.

Cross-checking techniques need to be used for code review and unit testing. Security defects uncovered by this process need to be prioritized, and then assigned to be repaired and retested within a specified period of time.

4) Testing and Deployment: Security tests need to be focused on what should not happen, so testing needs to be used during the integration and system testing phases to uncover previously unknown problems. This testing involves special attention to the software’s operating environment (network connections, configuration and customized set up), as well as the functional testing of security components. IT support staff need to be looking for functionality that should not be there, such as unintentional side effects and behaviors that are not specified in the design or implementation test plans.

Even an otherwise secure application can be left exposed by a misconfiguration or error during the setup process. During the deployment process, IT support staff need to use security checklists to; review configuration files, review enabled services and open ports, review access to sensitive files and directories, and ensure logging is enabled for forensics and incident response.

5) Maintenance: This requires special emphasis on understanding the existing security infrastructure of the application; much of which IT support staff needs to have gained during the previous stages of the development process. IT support staff needs to review proposed changes in terms of risks that they impose on the overall security of the system, and maintain documentation tracing back to the appropriate configuration management process. Any changes that are required to be made during this stage will have to go through the Implementation, and Testing and Deployment cycles again for validation and verification. The change management procedures outlined in section 3.5 can be used to track and document changes in this phase.

Whenever code has been created by non-University consultants, managers should consider hiring an additional consulting company to perform code checks for potential vulnerabilities.

3.7.2 Application Security in Commercial or Legacy Systems

The rationale for buying Commercial-Off-The Shelf (COTS) software is that they will eliminate development time by taking advantage of existing, market proven, vendor supported products, thereby reducing overall system development costs.

IT managers need to ensure that IT support staff investigate security issues with implementation of COTS software prior to procurement. IT managers need to discuss with IT support staff who has access to the system and in what capacity, how the system will be used, if the system will
contain protected information, and what are the potential threats to the system or system information.

IT support staff need to research security implementation of the COTS software based on the criteria discussed with IT management. IT support staff need to understand the standard hardening procedures and vendor recommended security configurations. These procedures might involve such things as not using default passwords, or securely configuring file and access permissions, or shutting down unneeded services.

The IT manager needs to analyze the results of the security investigation, and make a decision regarding any controls and countermeasures that may be required to lower risks. The IT manager should contact the TSO if the assessment involves protected level 1 information. The IT manager needs to ensure that the final controls and configurations are appropriately documented in the system/application build documentation.

Appendix I lists some of the more common application attacks\(^\text{38}\) that IT support staff need to be aware of, along with the countermeasures aimed at preventing them. This list is not intended to be exhaustive; rather it is intended to give IT support staff a starting point from which they may start protecting SDSU applications by testing and mitigating flaws in:

- The application dependencies on the host operating system and other applications
- The application user interface (front end)
- The application server (back end).

### 3.8 Remote Access Security

This section of the VMP explains issues dealing with Remote Access Security in terms of the responsibilities of staff and faculty when accessing the SDSU computing resources from an offsite location.

Remote access connectivity introduces a number of security challenges, such as ensuring:

- Secure connections to the SDSU network
- Only authorized users connect to the network
- CSU and/or SDSU protected information and/or licensed information is stored only on SDSU issued laptops and desktops, and not on unauthorized personally owned computers
- Protected information is protected in transit against eavesdropping
- The SDSU network is protected against security problems on remote computers that may pose a risk to SDSU computing resources
- Software licensed for SDSU use only.

3.8.1 Securing the Remote Computer

When accessing critical systems or those containing protected level 1 information, faculty, staff and students must ensure that their remote computer meets the same protection standards of encryption, anti-virus, anti-spyware, patching, and host firewall outlined in section 3.2 of the Information Security Plan before connecting to SDSU systems and accounts.

In addition, the remote computer must prevent access by unauthorized individuals (spouses, children, roommates, etc) to SDSU information and systems. Technologies such as unique user accounts and password protected screen savers that lock within 15 minutes or less of non-use must be applied to remote systems to prevent unauthorized use of the remote connection to SDSU.

Remote computers must be installed with operating systems that provide for adequate network security. Operating systems such as Windows 98, ME, and NT do not have sufficient network security built into them.

3.8.2 Remote Access to Secure Web and Messaging Applications

When connecting to campus email and calendar systems using client software applications, the applications must be configured to use secure settings, with protocols such as POPS, IMAPS, and SSL.

Campus email and calendar software utilize secure protocols at these links:

Email: [https://mail.sdsu.edu](https://mail.sdsu.edu)
Calendar: [http://calendar.sdsu.edu](http://calendar.sdsu.edu)

3.8.3 Remote Programmatic, Management, and File Transfer Access to Computing Resources

When remote access to development and administrative services, and server based applications is necessary, the risk level to SDSU computing resources is higher because whole systems could be affected by allowing access from the Internet. In these cases, secure session protocols such as SSH and SFTP must be used.

Similarly, when remote desktop control is necessary, it should be over Virtual Private Network (VPN) technology. Remote access through non-secure methods such as FTP, AFP, and remote desktop should only be used when no other alternatives are available, such as anonymous FTP. Furthermore, if insecure protocols are necessary no protected information (such as SSN, 39 Transmission of protected level 1 and level 2 within the SDSU network must also be encrypted according to approved policies.
Educational records, medical records), should be viewed, or transferred, using these insecure protocols to ensure the information cannot be accessed by unauthorized users.

Encrypted remote connection desktop software, such as RDP, pcAnywhere®, VNC, should be used within a VPN connection to ensure the connection from the remote desktop to the SDSU network is properly secured.

IT managers should document the justification and authorization to use VPN accounts along with a signed agreement from the employee to adhere to proper securing of the remote computer and connections. Included in the documentation should be:

- The type of remote network connection (such as wireless, dial-up modem)
- The applications the remote computer will be running within the VPN connection specific to SDSU computing resources
- The authorized tasks (such as applying patches, verifying backups, troubleshooting errors) for the remote connection
- Confirmation that the remote system follows SDSU desktop standards for unique accounts, patch management, anti-virus, anti-spyware, and that the remote host has a hardware/host firewall
- No SDSU protected level 1 information should be stored on the remote system.

### 3.8.4 Network Access to Level 1 Information or Critical Systems

Faculty and staff who require network access to networks containing protected information (such as HR, SIMS/R, SHS) or critical systems (such as the campus email and web servers, calendar server, Physical Plant control systems) via a remote connection are considered to be operating at the highest risk level. IT managers should use discretion in requesting/granting remote access to protected level 1 information. However, if necessary, this type of connection would necessitate a privileged VPN connection, and would require a documented authorization process including the TSO.

IT managers should provide an SDSU managed laptop to employees needing network access to SDSU systems, and/or to use non-web applications, to access protected level 1 information and/or critical systems via their privileged VPN remote connection. The managed laptop should be used only for University related activities and not for other personal use.
3.9 Information Security

This section of the VMP explains issues dealing with information security in terms of defining limitations on the storage of protected information, backing up of information, preparing equipment for surplus, securely retaining information, and the use of encryption.

3.9.1 Storing Protected Information on SDSU Systems

SDSU protected level 1 information should not be stored on SDSU laptops or desktops\(^{40}\). Protected level 1 information should be stored on secured databases or file servers, or off-line media, such as CD and DVD storage. Off-line media should be encrypted\(^ {41}\), and must be stored in a secure location at the University or another site approved by management (including off-site backup services).

Users who need to have exceptions to these standards for storing protected level 1 information on laptops must have Dean, Vice-President, or executive level signed approval.

3.9.2 Sending Protected Information within and outside of SDSU

Sending SDSU protected level 1 and level 2 information, both within and outside of the University, must follow approved procedures, which will include:

- When using either campus mail or an outside carrier, the protected information must be sealed, not visible from outside and marked “Confidential”
- When using voice messaging, the recipient messaging system must be password protected

3.9.3 Use of FAX equipment

When faxing SDSU protected level 1 information, the FAX must be attended, with someone physically present at both ends of the FAX machine waiting to send and remove the FAX upon completion. IT managers must create approved procedures to be followed when faxing SDSU protected level 1 information.

When faxing SDSU protected level 2 information, the FAX does not need to be attended, but approved procedures should be followed.

3.9.4 Use of Personal Equipment

Personal equipment may include devices such as personal laptops, personal desktops, personal digital assistants (PDAs), iPods\(^ {®}\) and cell phones (such as BlackBerry\(^ {®}\), Treo\(^ {®}\) and iPhones\(^ {®}\)). SDSU protected level 1 information must not be stored on any personal equipment. Additionally, users must not send or forward emails containing protected level 1 information to

\(^{40}\) Exceptions must be documented and registered with the IT Security Office
\(^{41}\) See Appendix K for more information on encryption and encryption standards
personal email accounts. Employees are permitted to store voluntarily submitted protected level 2 information on personal equipment. Final approval authority for storing protected information on personal equipment is listed in Table 3.2.

Personal laptops being used at the University must not be connected to the network behind an internal firewall without authorization.

Users should adopt the same anti-virus, anti-spyware and patch management standards for personal equipment as exist for University systems. In addition, users should utilize host firewall software on their personal equipment.

3.9.5 Use of File Servers

IT managers are responsible for ensuring that access to information stored on file servers is limited to authorized users. Access to information should be granted according to required job duties. Protected level 1 information which is stored on file servers should be encrypted.

3.9.6 Use of Databases

IT managers are responsible for ensuring that access to protected information in databases approved according to required job duties. Access control should include a combination of file read/write privileges, and access control lists on the database data objects. Databases should be configured to encrypt protected level 1 elements.

3.9.7 Backups

Backups are an integral part of ensuring the security of systems information and data. A backup plan must address the following scenarios:

- The recovery of files accidentally deleted
- Hardware failure
- Incident response investigation
- Disaster recovery

IT managers are responsible for ensuring that an appropriate backup plan is developed, and IT support staff implement the plan. The backup plan should include items such as the schedule for the backups, encryption of protected information, daily checking of the backup logs, regular verification of backed up information, excluding the quarantine directory, and regular testing of the restoration from backup media.

The frequency of backups may depend upon how often information changes, how important those changes are, and the speed of the backup resources. There are three main types of backup strategy that IT managers should be aware of; full, incremental and differential backups. IT managers should work with IT support staff to determine which backup strategy, or combination
thereof, works best with which frequency, in order to be able to restore information in a timely manner.

### 3.9.7.1 Storing and Retrieving Backups

Multiple backup media should be utilized in the backup process. Corruption or loss of information may occur if multiple backups are stored on one media. For example, if all daily backups are stored on one tape and that tape is corrupted, all those backups would be unavailable.

For recent backups which may need to be retrieved quickly, the offsite location could be another building at the University. In the case of longer term and archive backups, the storage location should be off the SDSU campus.

For critical information, two backups are recommended in case the media of the initial backup becomes corrupt. If, for any reason, a backup should fail, IT support staff should notify IT management.

A common cause of failed backups is faulty or overused media. The backup plan should address renewing backup media regularly, as well as a retention schedule to specify how long archived backups will need to be kept, and correct procedures for backup media disposal. Failed media containing protected information should be sent to material management for destruction.

IT management should ensure that restores are scheduled to ensure that the backup information can be restored and the media test is functioning. Depending on the number of backup media and the volume of information being backed up, scripts can be used to automate the test restoration process. A typical script might select sample information to be restored from the beginning, middle and end of a backup.

For more information on backups and backup strategies, see Appendix J in the back of this document.

### 3.9.8 Disposal of IT Resources

The Material Management Office auctions surplus computers and disk drives to the public, and destroys media that are not reusable. IT support staff are responsible for ensuring that all information, operating systems and other software (including all media) have been removed (sanitized) from the equipment sent to surplus. Management needs to ensure that proper documentation of all items for surplus are provided to the Materials Management Office when systems/media are picked up. Surplus documentation is vital to the campus inventory reconciliation process.

The IT Security Office recommends writing over the hard drive once to sanitize any remnants of information or software. Writing over the hard drive in this manner still leaves the drive usable.
Using the built-in ATA ANSI standard Secure Erase\textsuperscript{42} command for newer ATA drives (more recent than 2001) bigger than 15GB can result in an acceptable level of sanitization, without compromising the usability of the drive.

Defective media (hard drives, tapes, etc) must be removed from systems and labeled for destruction so that Material Management can shred them to prevent access to information or licensed software.

Degaussing is another popular sanitization technique. Since the operational requirements to execute degaussing effectively could result in serious bodily harm to individuals, the IT Security Office does not recommend degaussing as a sanitization option for any electronic media.

Managers should ensure that CD-ROMs and DVDs which are no longer required are shredded (especially those containing protected information), either by Material Management or within their own department. Media containing protected information which cannot be shredded immediately should be secured until disposed of according to approved procedures.

### 3.9.9 Retention of IT Resources

Retention applies to the correct storage and disposal of both computer hardware containing electronic information, and of media containing information records. The data authorities responsible for creating and implementing campus retention schedules and procedures include:

- The Registrar for Educational Student Records
- The Director of the Center for Human Resources for Employment Information
- The Campus Privacy Officer for Medical Information
- The Controller for Financial Information
- The Associate Director for Associated Students
- The Chief Executive Officer for the Research Foundation
- The Chief Executive Officer for Aztec Shops
- The Chief Executive Officer & Chief Information Officer for the Campanile Foundation

Managers are responsible for creating retention schedules for information not covered by these campus data authorities. This should include, but not be limited to, a retention schedule for email.

The retention schedules should document:

- Compliance with applicable local, state and federal laws and regulations concerning information and records retention, and applicable guidelines established in the Office of General Counsel Records Access Manual publication

\textsuperscript{42} Guidelines for Media Sanitization, NIST Special Publication 800-88
The period of time during which specific information and records have operational, legal, fiscal or historical value

The period of time during which information and records must be stored in their primary storage location, and the point in time when the records can be reasonably transferred to a secondary storage facility, destroyed, or transferred to historical archives

Methods and procedures of information and records storage, retrieval, disposition and disposal to ensure compliance with information classification, legal and operational requirements.

Management should ensure that a process is created to provide physical and environmental protection and accountability for information retained on hard drives, DVDs, CDs, tapes, thumb drives, diskettes, printouts and other media.

IT support staff should physically label all controlled media (media containing protected information), media containers, and documents. Special markings or colored labels may be used in order to identify special handling instructions, storage locations, access authorization, and include enough information to return it to its owner.

IT support staff should log and secure all controlled media for reasons of accountability and traceability. Logs may track information such as control numbers, the times and dates of transfers, names and signatures of individuals involved, and so on. IT managers should conduct periodic spot checks to confirm that all controlled items are accounted for, and that all items are in the custody of individuals named in the control logs.

Physical access controls such as locked doors, desks, file cabinets, or safes should be used for protection against stolen, lost, destroyed, or replaced media. Physical access to and handling of protected information, in particular, must be in accordance with approved procedures.

IT management will ensure that a process for secure information disposal is set up. This disposal process will include sanitization techniques such as overwriting (using a program to write 1’s, 0’s or a combination onto the media), and destruction (shredding or burning of media).

### 3.10 Network Security

*This section of the VMP explains issues dealing with protecting the security of the SDSU network.*

#### 3.10.1 Border Firewall

The SDSU border firewall provides SDSU protection by allowing only necessary network traffic into the University network, while deflecting unauthorized communications.

IT managers who wish to request access through the border firewall should submit a request to the Border Firewall Registration System at [https://security.sdsu.edu/border](https://security.sdsu.edu/border). The Border Firewall
Registration System is a web based interface with explanations of the information required. The registration system provides a CSV output file of the request for the IT Manager's records.

All border firewall requests must be approved by appropriate management and the IT Security Office. In some cases, requests may be provisionally approved until a more secure solution can be found. In addition, all servers allowed a border exemption must be properly maintained and secured to SDSU security standards. The server administration agreement found at [https://security.sdsu.edu/border/server-agreement.html](https://security.sdsu.edu/border/server-agreement.html) must be agreed to before firewall exemptions will be granted. The IT Security Office will periodically do a security scan of servers with border exemptions to help ensure that security standards are being maintained. Any serious security problems must be mitigated or servers may lose their border firewall exemptions.

### 3.10.2 New Internal Firewalls

Due to the required planning involved, the process of implementing new internal firewalls may take several months to complete. The phases of implementation will include:

- An initial meeting with the TSO to discuss security goals
- The TSO will determine the necessary firewall architecture and scope the rule sets required (such as inbound traffic to servers, or traffic between desktops and servers, etc)
- IT support staff will confirm the operational needs of the supported application in reference to the firewall rule set. This is typically done by:
  - Vendor consultation
  - Technical documentation
  - Using a network sniffer to evaluate specific port needs
- The sample of network traffic should be analyzed to discover which ports and services will need to be allowed to pass through the firewall
- A work order for TNS will need to be generated specifying which systems will need to be relocated (both logically and/or physically), or new network access created
- Before activating the firewall rules, IT support staff should develop all possible tests and scenarios for communication through the firewall
- After going live, IT support staff should perform all tests of communication through the firewall to identify problems while the TSO is scheduled. Problems identified later will require a new firewall request.

IT managers and support staff should understand additional firewall zones add complexity to the design process. Firewalls using a single zone will talk only with the outside, and present the least complicated design. Firewalls with two or more zones will need to communicate both with the outside, and between internal zones.
3.10.3 Requesting Access through an Existing Internal Firewall

IT support staff who require access through one of the internal SDSU firewalls under the management of the TSO should email their request to firewall@sdsu.edu. Information required includes:

- Destination port number(s) needed (such as ports 21, 22, 80, and so on)
- Network protocols needed (such as TCP or UDP)
- Application that will be needed (such as HTTP or FTP)
- Reason for the request (such as a new application has been installed)

The TSO will contact the requestor to review and process the rules. The access request process typically takes about two weeks to complete.

3.10.4 Firewall Logs

All network traffic entering and exiting the SDSU network is logged at the firewalls. The TSO may use the contents of the firewall logs to confirm, scope, and/or follow up on an incident. IT management who wish to review the firewall logs for acceptable use issues or employee investigations should contact the Center for Human Resources. The contents of the logs are strictly controlled for reasons of privacy.

3.10.5 Intrusion Detection Protection Systems (IDP)

Intrusion Detection Prevention Systems (IDP) are implemented to detect and prevent malware. All IDP devices are managed by the IT Security Office.

3.10.6 Wireless Network

Wireless network access is available throughout the University. Wireless network access is intended for community use, similar to connections from home. Wireless network access should not be used for University business. All University systems should be connected via the wired network. Laptops connected via the wired network must have the wireless connection disabled.

Utilizing the wireless network access requires a registration process for the first time of use, after which access is automatic. All University acceptable use policies apply to the wireless network, as well as the wired network. IT managers should contact the TSO for evaluation of any systems needing wireless connections.

3.10.7 Domain Name Service (DNS)

The TSO is responsible for the authoritative DNS servers (130.191.200.1 and 130.191.1.1) for the University.
IT support staff who requires DNS changes to be made, or seek to implement an internal DNS, can submit their request via the Domain Name Service link. Requestors can expect DNS requests to take about five business days to complete.

3.10.8 Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP) is available on most campus networks to provide dynamic IP addresses and other networking information. Since DHCP IP addresses can change, if static IP addresses are required for a server or desktop, please contact your departmental IT coordinator or contact TNS for assistance.

3.10.9 Mitigation of Network Risks

During an active or imminent network attack, the TSO will review the vulnerability status of systems/devices connected to the SDSU network and, as time allows, attempt to contact IT management and support staff of the vulnerable systems, either individually or via the SDSU security mailing list, to convey the need to patch/fix vulnerable systems/devices immediately.

Vulnerable systems and devices that remain connected to the SDSU network can be subject to loss of network or selected service access, depending upon the vulnerability, number of users, impact to the University, and information contents. Blocking systems at the SDSU border firewall or completely removing systems/devices from the network is a drastic measure taken as a last resort to protect San Diego State University from network downtime, unlawful access to information, or other liability.

The following guidelines will be used by the IT Security Office to categorize systems/devices that pose a serious threat and therefore must be taken off the network or have services filtered, in order to protect the network or information:

1) A system/device may be taken off the network immediately if it is determined to have an infection/breach; or the system/devices has a vulnerability that is remotely exploitable, an exploit exists that leverages this vulnerability, and the exploit is currently being used on the SDSU network.

2) A system/device may be taken off the network within 1 work day if it is determined to have a vulnerability that is remotely exploitable, an exploit exists which leverages this vulnerability, but the exploit is not yet present on the SDSU network.

3) A system/device may be taken off the network within 1 calendar week if it is determined to have a vulnerability that is remotely exploitable, but no exploit is currently known that leverages this vulnerability.

43 [http://security.sdsu.edu/services/dns/]
4) A system/device may be taken off the network within 1 calendar month if it is determined to have a vulnerability that is locally exploitable, which could result in unauthorized access to the system/device or unauthorized access to Confidential/Sensitive information.

Systems that are taken off the network should then follow the steps outlined in the SDSU Security Incident Response Program Malware Table 2.0.

Network risks are further mitigated by the border firewall which blocks unauthorized sessions initiated outside the firewall. The following guidelines will be used by the IT Security Office as a baseline set of requirements for systems accessible behind the border firewall:

- Dangerous protocols, such as NetBios and MySQL, will continue to be blocked
- Mail server access will not be expanded
- Exemptions for clear text protocols, such as telnet, POP3, IMAP and ftp, will not be granted
- Other protocols, such as smtp, http and remote access, may be temporarily allowed pending mitigation
- All systems applying for an exemption will be subject to a security scan to check for vulnerabilities. IT management should ensure that system patches are up to date.

3.11 Physical and Environmental Security

This section of the VMP explains issues dealing with Physical and Environmental Security from the perspective of the measures taken to protect systems, buildings and related supporting infrastructure against threats associated with the physical environment.

University physical and environmental security focus involves rooms where servers are housed, and data centers. All of the security controls that apply to server rooms also apply to data centers. Data centers have additional security controls, since they contain most of the University critical servers. This section of the document outlines the controls that apply to server rooms. The additional controls that are appropriate for data centers can be found in Appendix L.

3.11.1 Physical Access to Offices and Buildings

Managers should ensure that all protected information within their area of responsibility is locked away at the end of each day. Documents that contain protected information and are no longer required must be shredded. If documents that contain protected information cannot be shredded at that time, they should be locked away in secure storage spaces or bins until they can be shredded. If the volume of protected information to be shredded becomes too great, locked shredder bins are an option to store protected information until it can be shredded in bulk.

Managers should request reports from Public Safety on a yearly basis which detail key and card access listings for each of their employees, and access reports by doors and buildings. Managers should take immediate action to revoke unnecessary access. If keys and/or access cards to areas
containing protected information or critical resources are lost, the access cards should be
disabled immediately, and/or the lock should be re-keyed and new keys issued.

3.11.2 Physical Access in Server Rooms

1) The Server Room: Server rooms must be locked, and accessible only by authorized key
access. Visitors (such as service personnel or contractors) should be escorted at all times. Server
rooms should not be used for functions that require uncontrolled access (such as storing office
supplies).

2) Doors: Doors must be locked. If key card access is used, there should be a manual key access
as backup. Doors should be constructed using material with a one hour fire rating, and be
resistant to being forced open. During a power interruption, the doors should fail-safe; requiring
key access for entry and allowing any exit. Doors should be self-closing, with no hold-open
feature. With card access, an alarm, monitoring should trigger if a door is forcibly opened or held
open for an extended period of time.

3) Windows: Ideally, a server room should not contain windows. If windows are present, they
should be small enough to prevent access into the server room. Blinds or reflective film should
be used to limit visibility into the server room. Depending on the server room contents, the
windows should have additional bars to prevent theft of critical equipment or protected
information.

3.11.3 Fire Safety

Fires have the potential for the complete destruction for all systems housed within a given
building. IT management should ensure that controls exist to properly manage the sources and
factors that can lead to fires.

Typical ignition sources include faulty electric devices and wiring, and unattended heating
devices. IT managers should ensure that no heating devices are used in the server room, and that
combustible materials (such as chemicals and liquids) are not stored in the server room.

IT managers should ensure that fire extinguishment systems are located in the server room. Fire
extinguishment systems, can range from hand held portable devices, to large scale automatic
discharge systems. IT managers should ensure that the correct type of extinguisher is housed in
the appropriate location.

3.11.4 Electrical Systems

Electrical power is particularly critical in terms of both quality and quantity. IT managers should
ensure appropriate precautions to control the availability and supply of electrical power. These
precautions may include:
- Using configurable Uninterruptible Power Supplies (UPS) for both power supply conditioning and redundancy
- Monitoring the amount of power being drawn if multiple machines are being plugged into a single power strip
- Using anti-static carpeting to protect against static electricity
- Using line conditioners or surge protectors to protect desktop systems
- Ensuring there is a readily available Emergency Power Off switch to shut down the power quickly if required; preferably one switch for all systems, which is near an exit, and covered to protect against accidental activation
- Ensuring automatic generator backup.

IT managers should request a review of power use and electrical system controls by Physical Plant when there are significant changes in the equipment used.

### 3.11.5 Plumbing and Cooling System (HVAC) Leaks

IT management should consider all options when deciding on the placement of facilities. For instance, critical servers should never be placed directly below water pipe lines, or air conditioner condensers, in case of leaks.

IT management should ensure that IT support staff know the location of all relevant shutoff valves, and understand the procedure that should be followed in the event of a water line failure.

IT managers should request a review of plumbing and cooling system use and controls by Physical Plant, when there are significant changes in the building architecture.

### 3.11.6 Temperature and Humidity ranges

Often a system will crash or shut down due to high temperatures and/or excessively low humidity levels. IT managers should ensure that temperature and humidity ranges are within acceptable levels and monitored. An automated alert system should be configured to notify the IT manager when temperature and humidity ranges are outside acceptable levels for all critical systems.

### 3.12 Residential Halls

*This section of the VMP explains the procedures used by Residential Halls to connect student computers to the network, addresses Acceptable Use Policy violations incidents and unauthorized network devices.*

Residents moving into residential halls will work with their RezCon Assistant (RCA) in order to gain access to the residential halls network and Internet. Before access is granted, all operating system patches, anti-virus and anti-spyware definitions need to be updated. Additionally, residents will need to read and accept the RezCon Acceptable Use Policy (AUP). Once access
has been granted, residents will use a combination of their RedID and a unique registration code to authenticate. Failure to adhere to the AUP will result in residential halls network and Internet access being disconnected.

### 3.13 Visitor Security

*This section of the VMP addresses proper processes and protections from risk of non-CSU equipment accessing the campus networks, systems and information.*

#### 3.13.1 Vendors/Consultants

SDSU is not liable for vendor property (such as personal or company laptops). Vendors should take precautions to protect their property (such as using lockable laptop cables).

All SDSU software and information must be removed from vendor computers at contract termination. Vendor computers should never contain CSU protected information, without proper encryption.

The reporting IT manager is responsible for ensuring that the vendor has appropriate account access. The establishment of accounts should be controlled on a need-to-know basis. Accounts should be limited to work hour access, and from authorized sources, such only from SDSU assigned computers or other specified computers. Accounts should be set to expire at contract end or every six months (whichever is less) unless renewed by the reporting IT manager.

The reporting IT manager is responsible for ensuring that all information security requirements pertaining to desktop/laptop security, application security and account management outlined in this document are adhered to by vendors. Questions involving information and accounts should be addressed to the ISO.

All vendors accessing CSU information should sign a confidentiality agreement, a non-disclosure agreement, and agree to abide by all federal and state laws; including notification of vendor owned computer security breaches containing personal protected information, in coordination with the ISO.

Retention of information by vendors must be authorized by the reporting IT manager. The retention period should only be as long as necessary, and adhere to the appropriate data authority guidelines.

The reporting IT manager is responsible for checking with Key Issue to confirm that all card access/keys are turned in at the end of the contract.

#### 3.13.2 Visiting CSU Staff/Faculty

Visiting staff/faculty will be held to the same standards as SDSU staff/faculty.
3.14 Departmental Assessments

IT management is responsible for ensuring that they and the IT support staff are familiar with the principles outlined in this Information Security Plan, and that the controls detailed within the program are appropriately implemented within their operation.

IT management is responsible for completing and signing the Departmental Assessment Form on the next page each quarter or semester. Additionally, IT managers should attach a written plan of improvements they intend to make in areas of their operation where security controls are weak to the assessment form.

The Departmental Assessment Form is intended to be a tool for the use of the IT managers. It is not intended to be reported to the IT Security Office. Completion of the assessment form ensures that a periodic and minimal assessment of security practices is performed by IT managers.
### 3.14.1 Departmental Assessment Form

**DEPARTMENTAL ASSESSMENT FORM - Page 1**

<table>
<thead>
<tr>
<th>Desktop/Laptop/Mobile Device Security</th>
<th>Y/N</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The Information Classification Standard has been read/understood</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. There is a written patch management plan</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 3. Using a 10% sample of systems:  
  * Patch management clients are configured/functioning properly  
  * Anti-virus/spyware clients are configured/functioning properly  
  * Anti-virus/spyware clients have active protection turned on  
  * Anti-virus/spyware clients search for updates at least twice a day |       |          |
| 4. Security patches are installed within 1 week of release |       |          |
| 5. There is a weekly report of systems not reporting 100% patched |       |          |
| 6. There is a daily report of infections found in the last 24 hours |       |          |
| 7. Standard builds are used to install desktop software, are secured in a central repository & use authorized software |       |          |
| 8. There is a list of authorized software |       |          |
| 9. Laptops are configured with full disk encryption |       |          |
| 10. Protected information is encrypted on file servers |       |          |

**Server Security**

<table>
<thead>
<tr>
<th>Y/N</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Servers utilize RAID, dual powers supplies and UPS</td>
<td></td>
</tr>
<tr>
<td>2. Each server has a pre-arranged patch management schedule</td>
<td></td>
</tr>
<tr>
<td>3. Each server has a pre-arranged anti-virus update schedule</td>
<td></td>
</tr>
<tr>
<td>4. Each server has a pre-arranged anti-spyware update schedule</td>
<td></td>
</tr>
<tr>
<td>5. Each server has logging turned on or enabled</td>
<td></td>
</tr>
</tbody>
</table>

**Configuration Management**

<table>
<thead>
<tr>
<th>Y/N</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. There is a process to identify/manage controlled documentation</td>
<td></td>
</tr>
<tr>
<td>2. There is a process to identify/manage controlled systems</td>
<td></td>
</tr>
</tbody>
</table>

---

44 An electronic copy of this form can be found at [http://security.sdsu.edu/policy/Departmental_Assessment-4.1.xls](http://security.sdsu.edu/policy/Departmental_Assessment-4.1.xls)
<table>
<thead>
<tr>
<th>DEPARTMENTAL ASSESSMENT FORM - Page 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Account Management</strong></td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td><strong>Information Security</strong></td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>7</td>
</tr>
<tr>
<td>8</td>
</tr>
<tr>
<td><strong>Application Security</strong></td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td><strong>Network Security</strong></td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td><strong>Physical and Environmental Security</strong></td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td><strong>Manager Signature</strong></td>
</tr>
</tbody>
</table>
### 3.15 IT Security Office Assessments

The purpose of the Vulnerability Management Program is to assist the IT Security Office in creating an awareness of the type of threats and vulnerabilities that SDSU faces on a daily basis and to provide remediation of these dangers.

The IT Security Office has several roles. The IT Security Office is responsible for ensuring the information technology security of campus systems and information. In consultation with management as appropriate, the IT Security Office may take steps in order to remediate security vulnerabilities that are out of compliance with SDSU security standards. Additionally, the IT Security Office will assist and advise IT management and support staff in the implementation of the principles outlined in this program.

IT Security Office will work with IT management and IT support staff to review the results of the departmental assessments.

Additionally, as part of its University responsibilities, the IT Security Office will conduct security assessments of departmental operations, which may include, but are not limited to review of:

- Departmental assessment results
- Data center security
- Network security
- Desktop security
- Information security
- Protected information retention and disposal
- Surplus Security
- Departmental assumed risks and exceptions
- Escalation criteria and activations

Some assessments may be unannounced, other may involve pre-scheduled coordination with appropriate IT management or IT support staff. Pre-scheduled assessments that involve coordination will be conducted so as not to seriously impact the schedules of IT management or IT support staff.

All vulnerabilities identified during the assessment will be documented by the IT Security Office for review with the applicable IT manager and IT support staff. Vulnerabilities will be classified as critical, serious, moderate or low (see Glossary in Appendix B for explanations of these classifications).
IT managers will be responsible for:

- Remediating any critical vulnerabilities immediately
- Creating mitigation plans and estimated completion dates for all serious vulnerabilities within two weeks of the review meeting.
- Indicating “assumed risk” for vulnerabilities which cannot be mitigated, but must remain in production.
- Notifying “users” when there is a security conflict with the system use.
4.0 Introduction to the Security Awareness and Training Program

The Security Awareness and Training Program (SA&T) will outline the minimal and optional training and awareness to be provided for faculty, staff, students, and consultants in information security.

This SA&T Program will provide details for the following:

- Security awareness training for faculty, staff and consultants
- Protected information security awareness for faculty, staff and consultants
- Security awareness for residence students
- Security training for technical support staff and IT management
- Optional security events for faculty, staff and students

The IT Security Office will be responsible for understanding campus security needs, and recommending or presenting appropriate materials in a variety of learning settings, including the following:

- Handouts (copies of articles or slide shows, and links to web sites)
- Staff and faculty communications (new hire letters, payroll letters, etc)
- Meetings (IT Security meeting, department meeting, etc.)
- Presentations (video, DVD, web-based, instructor led, etc.)
- University publications (staff/faculty handbooks, SDSUniverse, etc.)
- University distribution outlets (portal, kiosk, booklet information, etc.)
- Electronic distribution (memos, Wiki/Blackboard, direct emails, mailing lists, etc.)
- Reinforcement “freebies” (placards, mouse pads, etc)
- External vendor and association meetings (local chapter meetings, conferences, etc.)

IT managers will be responsible for preparing and presenting training budget requests, and setting aside time for security awareness and training and for ensuring the training is implemented.

4.1 Security Awareness Training

This course will be provided by the California State University (CSU) system. The course will be web-based, consisting of approximately thirty minutes of information and user interaction.

The initial course will be delivered at the end of the 2007 academic year, and refreshed thereafter. All faculty and staff, including auxiliary staff and student employees, must complete the initial awareness training and each subsequent refresh of the course.

The awareness training will describe CSU and campus information security policies and procedures, focusing on teaching employees, who come into contact with CSU assets and systems, the risks associated with insecure activities and of their responsibilities to comply with CSU policies and procedures. All employees must understand their respective information
security responsibilities, and properly use and protect the information and resources entrusted to them.

Announcements of the awareness training may be delivered to the campus through email, payroll letters, new hire letters, the faculty handbook, and SDSUniverse.

### 4.2 Protected Information Security Awareness

This course will be developed by SDSU, and will consist of material that is supplemental to the CSU Security Awareness Training. The Protected Information Security Awareness course will be specifically designed for employees who have access to large amounts of protected information (such as SSN, driver’s license, credit cards, student records, medical records, etc.).

The course will be delivered each year and the content will consist of specialized practices and controls for protected information in accordance with the SDSU Security Plan, incident trends, and new policies and procedures regarding protected information.

Delivery methods for this program may include meetings, web-based presentations, slide presentations, memos, emails, newsletters, web casts and Wiki/Blackboard presentations.

Announcements of the course may be delivered through email, department meetings, payroll letters, SDSUniverse, and portal announcements.

### 4.3 Residential Student Security Course

This course will be tailored to meet the requirements of SDSU residence students. The computing environment for residence students is different from other SDSU users in that the campus is their home, and their use of the network is for both study and personal use.

The Residential Student Security Course is provided each fall semester for all incoming residential students. The course is provided prior to granting general network connectivity. The content includes policies and procedures pertaining to the Residence Halls environment, copyright infringement, and an explanation of the minimum computer security standards that they will be required to maintain. The emphasis of the awareness is to teach the residential students prevention of incidents and consideration of the shared computing environment.

Delivery methods for this program may include lectures, web-based presentations, video or DVD presentations, slide presentations, or kiosk and booklet information.

Announcements of the course may be delivered through email, during student orientations, or when the residence student signs their lease.
4.4 Security Training for IT Management and Technical Support

This security training will be provided or recommended on an ongoing basis by SDSU, and consists of material supplemental to the CSU Security Awareness Training. The training is designed for technical and managerial faculty and staff and the content will consist of technical training in security trends, technologies, and procedures. Table 4-1 illustrates the different types of training needed depending on responsibilities. The target audience for individual security trainings events will vary depending on the duties and responsibilities of the faculty or staff.

4.4.1 Strategic Managers

Strategic managers provide high level governance of information and technology functions and dictate the priorities and resources for implementing information security at SDSU. Examples of strategic managers are the University President, Vice Presidents, Associate Vice Presidents, College Deans, Auxiliary Directors, Principal Investigators on projects, and other Directors with operational manager reports.

Strategic managers need understanding of conceptual security risks, controls, incidents, and trends. The strategic manager may not have an IT or information security background, but is responsible for staffing, budgeting, and prioritizing information security for their division, college, auxiliary, or project.

In addition to the CSU Security Awareness Training, strategic manager training can include security leadership workshops and seminars, security articles contained in executive publications, campus security articles, and security discussions with reporting operational managers or campus security officers. Strategic managers should also request and review departmental security assessments periodically from operational managers, to ensure appropriate priority, resources, and training is directed for items out of compliance.

4.4.2 IT Security Officers

The IT Security Office is responsible for a wide range of computing security services to the campus community including:

- Incident response and a primary contact point for SDSU computing security issues
- Firewall management services
- Network and host-based security auditing and consulting
- Intrusion detection services (IDS)
- Secure remote access services (VPN)
- Security awareness and training
- Security assessments
- Coordination of the SDSU IT Security Plan

IT Security Officers are expected to have expert level knowledge on security services provided for, and security issues that affect the University. In addition to the CSU Security Awareness
<table>
<thead>
<tr>
<th>Description</th>
<th>Strategic Managers</th>
<th>IT Security Officers</th>
<th>Operational Managers</th>
<th>Technical Support</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Faculty/managers who provide high level governance that drive priorities and budget for Security</strong></td>
<td>Faculty/managers who provide strategic and operational direction to the University</td>
<td>Campus Information Security Officers who provide primary technical support of information resources</td>
<td>Faculty/managers with direct technical support staff reports, or who provide primary technical support of information resources</td>
<td>Faculty/managers/staff that administer technology, including security practitioners</td>
</tr>
<tr>
<td><strong>Examples</strong></td>
<td>President, VPs, AVPs, Deans, Auxiliary Directors, Principle Investigators, and Directors with Operational Manager reportees</td>
<td>Information Security Officer (ISO), Technical Security Officer (TSO)</td>
<td>Associate Deans Data Center Managers Managers of Technical Support staff Network Managers Help Desk Managers Desktop Managers</td>
<td>Database Administrators, Information Security Professionals, Security Analysts, Webmasters, Programmers, Data Center Operators, Desktop and Server Administrators, Security Administrators, Network Technicians</td>
</tr>
<tr>
<td><strong>Training Needs</strong></td>
<td>Conceptual understanding of security risks, controls, incidents, and trends</td>
<td>Detailed understanding of security risks, controls, trends, assessments, incident management scoped to areas of responsibility, broad understanding of security areas outside of responsibility</td>
<td>Detailed understanding of security risks, controls, trends, and implementations scoped to area of responsibility</td>
<td>Detailed understanding of security implementations, incidents, and trends scoped to areas of responsibility</td>
</tr>
<tr>
<td><strong>Training Examples</strong></td>
<td>CSU Security Awareness Training Security leadership type workshop Security Discussions with Operational Managers Security Articles</td>
<td>CSU Security Awareness Training Security conferences, workshops and/or webcasts Security publications Security mailing lists</td>
<td>CSU Security Awareness Training Strategic Manager Meetings Security conferences, workshops and/or webcasts (general and technology specific) Security Articles IT Manager's meeting Senate IIT meeting Security Officer discussions SDSU IT Security mailing list</td>
<td>CSU Security Awareness Training IT Security meeting SDSU IT Security mailing list Security Articles Operation Manager meetings Security publications Security conferences, workshops and/or webcasts scoped to areas of responsibility</td>
</tr>
</tbody>
</table>

**Table 4-1: IT Managers and Technical Support Training Needs**
Training, typical security training for security officers will encompass general and specialized understanding of security trends and emerging threats, in security technologies, and strategic training focused on the implementation of security policies and procedures at both the CSU and SDSU level.

Typical sources for IT security officer training are local security organizations, CSU Information Security Advisory Committee (ISAC) meetings, security conferences, security seminars, security workshops and/or Webcasts, security mailing lists, and security publications.

The IT Security Office is responsible for recommending appropriate training for the campus and auxiliary faculty and staff. Examples of security awareness and training venues can be found in Appendix M.

### 4.4.3 Operational Managers

Operational managers have direct oversight of daily information and technology. Examples of operational managers are College Associate Deans, Data Center Managers, Network Managers, Help Desk Managers, Desktop Managers and other campus/project/auxiliary faculty and staff responsible for direct management of technical support staff and systems.

A detailed understanding of security risks, controls, trends, and implementations scoped to their area(s) of responsibility is needed in order for operational managers to provide appropriately for secure account management, application security, access control, server and desktop security, change management, physical security, and business continuity and disaster recovery.

Examples of operational management security awareness and training:

- Ensure all reporting employees (faculty, students, and staff) and consultants have completed CSU Security Awareness Training
- Ensure reporting technical support staff are also members of the SDSU IT Security mailing list
- Escalate and report department/college progress of security issues and requirements to strategic management for planning and prioritizing
- Plan for security training when systems are refreshed with new operating systems, hardware, or major applications
- Attend regular IT Security and Academic Affairs IT Coordinator meetings
- Review monthly IT Security/AA IT Coordinator meeting content with staff
- Review IT Manager/Senate IIT meeting with designated attendee (or provide status to peers and strategic manager if acting as designee)

---

45 May decide to send multiple employees to operational training, but one representative to security training
46 For Associate Dean operational managers
Review security assessment(s), approve plan(s) to close security gaps, and identify additional security training or consultation needed

Peruse trade magazines (Educause, CSO, Network Security, etc. as applies to position) for security articles

Follow up on SDSU IT Security mailing list postings of systems infected/vulnerable, security training or implementations

Report applicable security policy or procedural changes from areas of expertise to IT Managers/Senate IIT/AA IT Coordinator or IT Security Office directly (IRB, Financial protections, NTA, WACUBO, etc.)

Attend general and topic specific security conferences/workshops/Webcasts training courses

Subsequent to employees participating in training or reading training materials, the operational manager needs to ensure the training is applied by having the employee present a report or presentation either one-on-one with the operational manager, or with other employees to provide cross-training and initiate team discussions and planning of applicable security implementations. The operational manager should evaluate the training report, and provide feedback at IT Manager’s meeting or to the IT Security Office so that other departments on campus benefit from avoiding or participating in similar training.

The operational manager should evaluate and budget what training needs to be integrated into their area of responsibility (changes to procedures, consideration of tools, or further training). Most importantly, the operational manager needs to ensure that other technical support staff are appropriately cross trained in the materials or are scheduled for attending the course in the future. Depending on the course content, skill level of the individual, and/or the complexity of the material, employees might attend the same training several times in successive years, or get an update less often.

In addition to SDSU security training and awareness, operational managers may also be liaisons to CSU or other collaborative groups which provide security implementation and information. It is important that operational managers disseminate appropriate information from these meetings to reporting staff and peers on campus.

4.4.4 Technical Support

Technical support staff are responsible for administering information technology. Examples of technical support staff are Database Administrators, Programmers, Data Center Operators, Desktop and Server administrators, Security Analysts and Administrators, and Network Technicians. In addition to the CSU Security Awareness Training, technical support staff need detailed understanding of security implementations, incidents, and trends scoped to their area of responsibility.

---

47 These duties and the training may apply to faculty, staff, or student employees
SDSU provides for technical support training in a number of ways:

- Attendance at/review of monthly IT Security meetings
- SDSU IT Security mailing list articles, incident information, and training courses
- Security articles
- Meetings with operational manager regarding implementation, planning, and trends
- Security conferences/workshops/Webcasts scoped to area of responsibility
- Security publications scoped to area of responsibility

Security training can be expensive not only in cost of the course, but also time missed performing other duties. Technical support selected for security training need to report the results of the training with their operational managers and department/college peers to maximize the value of the training. Any deficiencies or issues with the training should be reported to the IT Security Office directly or through the operational manager to assist with identification of effective training venues.

As with operational managers, technical support may also be liaisons to CSU or other collaborative groups which provide security implementation and information. It is important that technical support disseminate information from these meetings to reporting managers and peers on campus through their operational manager and IT security meetings.

### 4.5 Additional Security Activities

These are events that may be included from time to time, and would highlight security trends (such as an increase in types and number of incidents, or incidents involving new technologies), and promote special security actions (such as Security Awareness month, and new legislative security laws or CSU directives). The events may be provided on an ad hoc basis.

Additional security events may include lectures, web casts, web-based presentations, class announcements, student newspapers and portal, walkway events, handouts (CDs, booklets, etc), panels and forums, demonstrations, seminars, questionnaires, games (such as jigsaw puzzles, word searches, scavenger hunts, and so on), campus TV and/or radio, Wiki/Blackboard and kiosk presentations, and campus wide promotions of Homeland Security Awareness month.

Announcements of the special events may be delivered through the web portal, class announcements, posters, SDSUniverse, The Daily Aztec, SDSU events calendar, and campus email.

---

48 Each department/college sends at least one liaison to the monthly IT Security meetings
## Appendix A: Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AA IT Coordinator</td>
<td>Academic Affairs IT Coordinator</td>
</tr>
<tr>
<td>ACH</td>
<td>Automated Clearing House</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption System</td>
</tr>
<tr>
<td>AFP</td>
<td>Apple Filing Protocol</td>
</tr>
<tr>
<td>ANSI</td>
<td>American National Standards Institute</td>
</tr>
<tr>
<td>AS</td>
<td>Anti-spyware</td>
</tr>
<tr>
<td>ATA</td>
<td>Advanced Technology Attachment</td>
</tr>
<tr>
<td>AUP</td>
<td>Acceptable Use Policy</td>
</tr>
<tr>
<td>AV</td>
<td>Anti-virus</td>
</tr>
<tr>
<td>BFA</td>
<td>Business and Financial Affairs</td>
</tr>
<tr>
<td>CCC</td>
<td>California Civil Code</td>
</tr>
<tr>
<td>CD</td>
<td>Compact disk</td>
</tr>
<tr>
<td>CD-R</td>
<td>Compact Disc Recordable</td>
</tr>
<tr>
<td>CD-ROM</td>
<td>Compact disk read only memory</td>
</tr>
<tr>
<td>CD-RW</td>
<td>Compact disk read write</td>
</tr>
<tr>
<td>CHR</td>
<td>Center for Human Resources</td>
</tr>
<tr>
<td>CIO</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>COTS</td>
<td>Commercial-off-the-shelf</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>CSU</td>
<td>California State Universities</td>
</tr>
<tr>
<td>CVS</td>
<td>Concurrent Versions System</td>
</tr>
<tr>
<td>DAT</td>
<td>Data File</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic host configuration protocol</td>
</tr>
<tr>
<td>DMV</td>
<td>Department of Motor Vehicles</td>
</tr>
<tr>
<td>DOB</td>
<td>Date of birth</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of service</td>
</tr>
<tr>
<td>DSA</td>
<td>Digital Signature Algorithm</td>
</tr>
<tr>
<td>DVD</td>
<td>Digital Video Disc</td>
</tr>
<tr>
<td>ECDSA</td>
<td>Elliptic Curve Digital Signature Algorithm</td>
</tr>
<tr>
<td>Email</td>
<td>Electronic mail</td>
</tr>
<tr>
<td>ePO</td>
<td>ePolicy Orchestrator</td>
</tr>
<tr>
<td>Email</td>
<td>Electronic mail</td>
</tr>
<tr>
<td>FERPA</td>
<td>Family Education Rights and Privacy Act</td>
</tr>
<tr>
<td>FIPS</td>
<td>Federal Information Processing Standards</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>GA</td>
<td>Graduate Assistant</td>
</tr>
<tr>
<td>HRLO</td>
<td>Housing and Residential Life Office</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol over SSL</td>
</tr>
<tr>
<td>HVAC</td>
<td>Heating Ventilating Air Conditioning</td>
</tr>
<tr>
<td>IACC</td>
<td>Instructional Academic Computing Committee</td>
</tr>
<tr>
<td>IDP</td>
<td>Intrusion Detection Protection</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>IM</td>
<td>Instant Messaging</td>
</tr>
<tr>
<td>IMAPS</td>
<td>Internet Message Access Protocol over SSL</td>
</tr>
<tr>
<td>IP</td>
<td>Internet protocol</td>
</tr>
<tr>
<td>IRB</td>
<td>Institutional Review Board</td>
</tr>
<tr>
<td>ISA</td>
<td>Intern Student Assistant</td>
</tr>
<tr>
<td>ISAC</td>
<td>Information Security Advisory Committee</td>
</tr>
<tr>
<td>ISO</td>
<td>Information Security Officer</td>
</tr>
<tr>
<td>ISSA</td>
<td>Information Systems Security Association</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>ITSO</td>
<td>Information Technology Security Office</td>
</tr>
<tr>
<td>MWSSLS</td>
<td>Minimum Workstation Specification and Site License Software</td>
</tr>
<tr>
<td>NetBIOS</td>
<td>Network basic input/output system</td>
</tr>
<tr>
<td>NIC</td>
<td>Network interface card</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>OU</td>
<td>Organizational Unit</td>
</tr>
<tr>
<td>OWASP</td>
<td>Open Web Application Security Project</td>
</tr>
<tr>
<td>PDA</td>
<td>Personal Digital Assistant</td>
</tr>
<tr>
<td>PHP</td>
<td>PHP Hypertext Preprocessor</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>POPS</td>
<td>Post Office Protocol over SSL</td>
</tr>
<tr>
<td>RAID</td>
<td>Redundant Array of Independent Disks</td>
</tr>
<tr>
<td>RAM</td>
<td>Random Access Memory</td>
</tr>
<tr>
<td>RCA</td>
<td>RezCon Assistant</td>
</tr>
<tr>
<td>RDP</td>
<td>Remote Desktop Protocol</td>
</tr>
<tr>
<td>RedID</td>
<td>SDSU Identification Number</td>
</tr>
<tr>
<td>RPC</td>
<td>Remote Procedure Call</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest Shamir Adleman</td>
</tr>
<tr>
<td>SA&amp;T</td>
<td>Security and Awareness Training</td>
</tr>
<tr>
<td>SDSU</td>
<td>San Diego State University</td>
</tr>
<tr>
<td>Senate IIT</td>
<td>Senate Instructional and Informational Technology</td>
</tr>
<tr>
<td>SFTP</td>
<td>Secure FTP</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hash Algorithm</td>
</tr>
<tr>
<td>SHS</td>
<td>Student Health Services</td>
</tr>
<tr>
<td>SIMS/R</td>
<td>Student Information Management Systems/Relational</td>
</tr>
<tr>
<td>SIRP</td>
<td>Security Incident Response Program</td>
</tr>
<tr>
<td>SIRT</td>
<td>Security Incident Response Team</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>SSN</td>
<td>Social Security number</td>
</tr>
<tr>
<td>TA</td>
<td>Teacher Assistant</td>
</tr>
<tr>
<td>Tax ID</td>
<td>Tax Identification Number</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TNS</td>
<td>Telecommunications and Network Services</td>
</tr>
<tr>
<td>TSO</td>
<td>Technology Security Officer</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>UCO</td>
<td>University Computing Operations</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>UPS</td>
<td>Uninterruptible Power Supplies</td>
</tr>
<tr>
<td>USB</td>
<td>Universal serial bus</td>
</tr>
<tr>
<td>VMP</td>
<td>Vulnerability Management Program</td>
</tr>
<tr>
<td>VNC</td>
<td>Virtual Network Computing</td>
</tr>
<tr>
<td>VP</td>
<td>Vice President</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
</tbody>
</table>
**Appendix B: Glossary**

**Active Protection**
Active Protection is a service that runs on a designated system and can monitor both for attempts to change specific security configuration settings and for attempts to install spyware. If it detects a change it responds by immediately changing the setting back to the original value, protecting the machine from the effects of the spyware. The Active Protection service also enables the system to automatically perform scans and remediation on a continuous or scheduled basis.

**Aggregate Data**
Several instances of the same information, example might be transmitting one name and email address of an employee, versus transmitting names/email addresses of all employees. The second would require an approval.

**Attended FAX**
Someone physically present at both ends of the FAX machine waiting to send and remove the FAX upon completion.

**Computer Account**
The combination of a user number, username, or user ID and a password that allows an individual access to a computer or network.

**Computer Forensics**
Computer forensics is the analysis of data processing equipment-- typically a home computer, laptop, server, or office workstation-- to determine if the equipment has been used for illegal, unauthorized, or unusual activities. It can also include monitoring a network for the same purpose.

**Computer Resources**
In the context of these guidelines, this phrase refers to the computers, network, software and hardware that makes electronic data or information available to users.

**Container**
Box, envelope, folder, or other object that holds objects. Does not include electronic mobile devices such as cell phones, flash drives, and so on.

**Data, Confidential**
Data requiring high level of protection due to the risk and magnitude of loss or harm that could result from disclosure, alteration or destruction of the data. This includes information whose improper use or disclosure could adversely affect the ability of the University to accomplish its mission as well as records about individuals requiring protection.

**Data, Public**
Information which can be made generally available both within and beyond the University.
Data, Sensitive
Information that requires some level of protection because its unauthorized disclosure, alteration, or destruction will cause perceivable damage to the University.

Data Owner
The individual or department that can authorize accesses to information, data, or software and that is responsible for the integrity and accuracy of that information, data, or software. The data owner can be the author of the information, data, or software or can be the individual or department that has negotiated a license for the University's use of the information, data, or software.

Denial of Service
Action(s) that prevent any part of an information system from functioning in accordance with its intended purpose. Usually flooding a system to prevent it from servicing normal and legitimate requests.

Dialup
A temporary connection between machines established with modems over a standard phone line.

Discussed verbally
Includes sign language as well as spoken in any language.

Firewall
Standard security measure composed of a system or combination of systems that enforce borders between two or more networks. A firewall regulates access between these networks based on security policies. To enable information to travel in and out of a protected network, holes or "ports" must be opened in the firewall.

Forensic Image
If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an “original”.

Hacker
1) According to The New Hacker's Dictionary a hacker is a clever computer programmer, who does not necessarily engage in illegal activities. 2) In the media, a Hacker refers to a person who illegally break in or attempts to break into a computer system.

IT Manager
Although this term includes positions such as Executive Vice Presidents, Vice Presidents, Assistant Vice Presidents, Divisional Managers and Departmental Managers; an IT manager is not necessarily a member of the Management Personnel Plan. Some IT managers have oversight over campus servers, network infrastructure, and datacenters (mail server, calendar server, campus portal, telecommunications, etc.). Other IT managers are faculty responsible for classroom labs, applications, and systems for teaching coursework or performing research. Still other IT managers are responsible for technology tools (desktops, printers, faxes, PDA’s, etc.).
At times the roles of IT manager and IT support staff may be one and the same (the same person who manages a system is responsible for applying the appropriate security controls). All IT managers are responsible for ensuring that IT support staff apply the minimum protections described in the SDSU Information Security Plan, and for ensuring that the minimum procedures for protecting information are followed.

**IT Support Staff**
Includes Analyst/Programmers, Equipment System Specialists, Information Technology Consultants, Instructional Support Assistants and Technicians, Network Analysts, Operations Specialists and Operating System Analysts. Primary responsibilities include the installation, configuration and maintenance of computerized systems and network devices.

**Key Encryption**
A private (or secret) key is an encryption/decryption key known only to the party or parties that exchange secret messages. In traditional secret key cryptography, a key would be shared by the communicators so that each could encrypt and decrypt messages. The risk in this system is that if either party loses the key or it is stolen, the system is broken.

A public key is a value provided by some designated authority as an encryption key that, combined with a private key derived from the public key, can be used to effectively encrypt messages and digital signatures. In public key encryption, a message encrypted with a recipient's public key cannot be decrypted by anyone except the recipient possessing the corresponding private key. This is used to ensure confidentiality.

Asymmetric (or public key) encryption is a form of cryptography in which a user has a pair of cryptographic keys; a public key and a private key. The private key is kept secret, while the public key may be widely distributed. The keys are related mathematically, but the private key cannot be practically derived from the public key. A message encrypted with the public key can be decrypted only with the corresponding private key.

Symmetric (or secret key) encryption uses a single private or secret key for both encryption and decryption.

**Key Logger**
A program that runs invisibly in the background, recording all the keystrokes, usually saving the results to a log file.

**Network**
A group of computers and peripherals that share information electronically, typically connected with each other by either cable, modem, or wireless.

**Normal Resource Limits**
The amount of disk space, memory, printing, and so forth, allocated to your computer account by that computer's system administrator.
**Password Protected Voice Messaging**
Requires a unique password to access voice messages.

**Pharming**
Similar in nature to e-mail phishing, pharming seeks to obtain personal or private (usually financial related) information through domain spoofing. Rather than being spammed with malicious and mischievous e-mail requests for you to visit spoof Web sites which appear legitimate, pharming ‘poisons' a DNS server by infusing false information into the DNS server, resulting in a user's request being redirected elsewhere. Your browser, however will show you are at the correct Web site, which makes pharming a bit more serious and more difficult to detect. Phishing attempts to scam people one at a time with an e-mail while pharming allows the scammers to target large groups of people at one time through domain spoofing.

**Phishing**
The act of sending e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user’s information.

**Physically Secured**
Requiring a key or combination to access (can be locking built-in overheads, a file cabinet, heavy bin, or a vault).

**Port Scanning**
Sending queries to servers on the Internet in order to obtain information about their services and level of security. On Internet hosts (TCP/IP hosts), there are standard port numbers for each type of service. Port scanning is also widely used to find out if a network can be compromised.

**Private Area**
This is an area within the working environment in which reasonable safeguards have been taken to keep verbal discussions of protected information from being overhead by unauthorized individuals. This may include cordoned off areas in an open space, or an enclosed office. Public areas such as stairwells, elevators, restrooms are not considered private.

**Protected Information**
Protected level 1 information is information primarily protected by statutes, regulation, other legal obligation or mandate. The CSU has identified specific guidelines regarding the disclosure of this information to parties outside the University and controls needed to protect the unauthorized access, modification, transmission, storage or other use.

Protected level 2 information is information that must be guarded due to proprietary, ethical or privacy considerations. Campus guidelines will indicate the controls needed to protect the unauthorized access, modification, transmission, storage or other use.
Protected level 3 information is information that is regarded as publicly available. These information values are either explicitly defined as public information (such as state employee salary ranges), intended to be available to individuals both on-campus and off-campus (such as an employee’s work email addresses), or not specifically classified elsewhere in the protected information classification standard. Publicly available information may still subject to appropriate SDSU campus review or disclosure procedures to mitigate potential risks of inappropriate disclosure.

**Root Kit**
A collection of tools that allows a hacker to provide a backdoor into a system, collect information on other systems on the network, capture passwords and message traffic to and from a computer, mask the fact that the system is compromised, etc.

**Security Level Tagging**
Involves applying descriptor or tag to an documentation item which explains the relative level of security that should be applied to that item. For instance, protected level 1, protected level 2, and protected level 3 are descriptors or tags used in this document to describe the relative level of security given to protected information.

**Server**
A server is defined as an application or device that has the ability to perform services for more than one connected client as part of a client-server architecture.

**Shred**
Should be an electronic cross-cut shredding machine.

**Spam**
Unsolicited (usually commercial) e-mail sent to a large number of addresses.

**Spear Phishing**
A type of phishing attack that focuses on a single user or department within an organization, addressed from someone within the company in a position of trust and requesting information such as login IDs and passwords. Spear phishing scams will often appear to be from a company's own human resources or technical support divisions and may ask employees to update their username and passwords. Once hackers get this data they can gain entry into secured networks. Another type of spear phishing attack will ask users to click on a link, which deploys spyware that can thieve data.

**Spyware**
On the Internet, "spyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties." As such, spyware is cause for public concern about privacy on the Internet.
Sync
Synchronization. Two devices are said to be in sync when they are locked together with respect to time, so that the events generated by each of them will always fall into predictable time relationships.

Trojan Horse
A malicious program that disguises itself as a beneficial or entertaining program but that actually damages a computer or installs code that can counteract security measures (perhaps by collecting passwords) or perform other tasks (such as launching a distributed denial of service attack). Unlike a computer virus, a Trojan horse does not replicate itself.

Unattended in Work Area
Someone with authorization to the information is not present to physically prevent unauthorized access.

University
This term is used not only to apply to the SDSU campus, but also to include all other locations such as campus offsite locations, auxiliaries, and research stations.

Virtual Private Network (VPN)
A VPN is a way to provide remote access to an organization's network via the Internet. VPNs send data over the public Internet through secure "tunnels".

Virus
A small, self-replicating, malicious program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive. A file virus executes when an infected file is accessed. A macro virus infects the executable code embedded in Microsoft® Office® programs that allows users to generate macros.

Vulnerabilities
Critical level vulnerabilities are those which need to be escalated to the IT manager for immediate remediation:
- Serious level vulnerabilities are those which need to have a target remediation completion date of one week or less, but on which remediation action needs to begin immediately
- Moderate level vulnerabilities are those which need to have a target remediation completion date of one month or less
- Low level vulnerabilities are those for which remediation may be discretionary based on risk, but which need to be reported to the IT security office regardless.

Worm
A computer program that replicates itself and is self-propagating. Worms, as opposed to viruses, are meant to spawn in network environments.
Appendix C: Final Authorities

The data authorities responsible for creating and implementing campus retention schedules and procedures include:

- The Registrar for Educational Student Records
- The Associate Vice President for Administration
- The Associate Vice President for Faculty Affairs
- The Campus Privacy Officer for Medical Information
- The Controller for Financial Information
- The Associate Director for Associated Students
- The Chief Executive Officer for the Research Foundation
- The Chief Executive Officer for Aztec Shops
- The Chief Executive Officer & Chief Information Officer for the Campanile Foundation
Appendix D: Determining Access to Protected Information

When considering a new account for an employee it is important that the manager weigh the risks of providing and maintaining the account against the critical need for the employee to have the account to complete their day to day work.

The risks for confidential information accounts are many:

1) Firewall rules need be opened to allow access to the secure data by the employee. Every opened firewall rule decreases the security of all the computers protected by the firewall, not just the particular computer the employee needs to access.

2) If the employee’s desktop were to be compromised, the firewall will not block access to an intruder attempting to compromise the confidential data. Desktop compromises occur regularly on the SDSU network due to the openness of our network, software susceptible to human error - such as malicious email attachments or web links, poor desktop security, and compromised malicious web sites visited by employees.

3) Computer compromises can also originate from employees. Statistically insider threats can be equal if not greater than outsider threats. The more employees with access; the greater the chance of an insider compromise. Although auditing should be in place at the network and desktop level to monitor malicious employee activities, auditing does not stop the compromise, but detect it after it has occurred.

4) Confidential data compromises not only cost the University time and money in managing the incident and securing the data, presents a risk to our users personal data if accessed for the purposes of identity theft or fraud, but with the California Database Notification Act, can also cost thousands of dollars in notification costs whether the data is misused or not. Each Department must pay for all costs incurred as a result of a computer compromise.

Before requesting an account with access to confidential data, managers need to ask themselves, “Is there another way the work can be completed without this employee having a new account”? Security needs should be compared to operational needs. If access to confidential data is needed infrequently (i.e. student records are looked up by the employee a few times a week), then it is best to enlist another employee, who already accesses student record data more frequently, to provide the service, rather than request an additional employee account.

All confidential accounts should be approved by a Data Custodian, a manager responsible for securing the data and limiting access. When in doubt of the need for an account, managers should contact the Data Custodian and discuss alternatives. Exercising discernment and limiting confidential data access is the most cost effective and operationally simple means of infusing security for all University management.
Appendix E: Patch Management Plan Examples

DISCLAIMER: Sample documentation provided in this section is for example only. Each department should develop their own documentation based on processes, requirements and risks which are unique to them.

Figure 1: Example of a Patch Management Plan demonstrates a document which outlines the essential elements required for a patch management plan. This document is intended to be a high level presentation of the patch management plan, and is not intended to provide plan details. However, it should include:

- Scope of the plan
- Description of inventory
- Tier testing structure
- Time lines for automated patching
- Priority ratings for systems
- Description of deployment procedure.

Other information that might be included in the patch management plan may include contact information for managers and IT support staff (if required).

Figure 2: Example of a Computer Systems Inventory provides additional information about the computer systems included in the patch management plan. Information includes:

- Computer name
- Department
- System type
- Operating system
- Computer assignee
- Physical location
- Current usage

The inventory should reflect the appropriate amount of information for the purposes of the division. However, additional information may include:

- Computer asset tag
- Operating system version
- Software installed (with version information)
- IP address
- MAC address
- Domain or Workgroup information
- System information (such as system speed, disk size, and available space)
- Manufacturer information
As part of the multi-tier deployment, IT support staff need to have a mechanism to notify IT management and other affected staff of the impending deployment of a patch.

**Figure 3: Example of text used for a patch advisory** demonstrates that the details required for a patch deployment notification should include:

- Date of deployment
- Patch name(s)
- Source of patch
- Priority of patch
- System(s) affected
- Impact of vulnerability
- Time line for deployment

After patch testing has been completed and the patches are ready for deployment, all affected systems should be patched within seven days. Extending this interval has the potential of exposing the University computing resources to additional risk.

IT support staff are responsible for compiling patch management plan reports for IT management. These should include:

- A listing of patches deployed with installation reporting
- A listing by computer of uninstalled patches
- Documentation of issues or concerns
- Patch exceptions

IT management will use reports to assess the effectiveness of their patch management plan. Patch management progress should be reviewed, and obstacles resolved and updates charted on a continuous basis. **Figures 4 through Figure 7** show how different vulnerabilities may be tracked and reported.
DIVISIONAL PATCH MANAGEMENT PLAN
(as of 2007)

Mission: To provide routine, automated patching to divisional workstations only (not servers) on the SDSU network.

Divisional System Information Necessary:
An inventory of all divisional workstations that includes for each system an identifier, such as property ID tag, the operating system, the IP or DHCP, owner of the asset and physical location.

An ongoing and updated reference as to whether an inventoried system is off the network and/or non-bootable to the network.

Inventoried systems are identified as members of groups or Tiers for patch deployment purposes. Deployment occurs in stages to divisional workstations. For example, members of Tier I are IT support and test systems, Tier II is a collection of systems used by IT representatives in each department (DAREs) and Tier III is the remainder of the division’s workstations.

Timeline for Automated Patching:
Check daily, weekly and/or monthly for notifications of critical vulnerabilities applicable to the system environment;
Use the patch management software to receive notifications of critical operating system and application patches;
Confirm the updates that apply to the system environment which should be deployed;
Notify appropriate managers of pending updates to be deployed and advise of planned deployment dates to each Tier (staged process);
Upon approval to deploy updates, send notification to IT representatives in the Division departments;
Notification includes all update references (patch #) and dates of deployment to each Tier.

For emergency deployment of a critical patch if necessary a deployment of the patch would be done to all Tiers at once.

System criteria for patching is:
Workstations with Windows 2000, XP operating systems;
Workstations must be bootable on the network

Automated Deployment consists of:
A centralized server running a patch management application;
A workstation client as a patch agent on each workstation;
A database of all detected network workstations to provide dynamic information as to system status;
Central reporting output of all divisional system’s status on a weekly basis;
Weekly review of the number of systems with outstanding patches that remain vulnerable.

Figure 1: Example of a patch management plan
<table>
<thead>
<tr>
<th>System Items</th>
<th>System Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>State ID</strong></td>
<td><strong>June</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>2007</strong></th>
<th><strong>Dept</strong></th>
<th><strong>EquipType</strong></th>
<th><strong>Op Sys</strong></th>
<th><strong>Win,Mac,Unix</strong></th>
<th><strong>Last Name</strong></th>
<th><strong>Bld</strong></th>
<th><strong>Room</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer1746</td>
<td>ENG</td>
<td>PC</td>
<td>Windows 2000</td>
<td>Smith</td>
<td>Building1</td>
<td>320</td>
<td>Off network</td>
</tr>
<tr>
<td>Computer1767</td>
<td>ENG</td>
<td>PC</td>
<td>Windows 2000</td>
<td>Johnson</td>
<td>Building1</td>
<td>320</td>
<td>Off network</td>
</tr>
<tr>
<td>Computer1769</td>
<td>SALES</td>
<td>PC</td>
<td>Windows 2000</td>
<td>Jenkins</td>
<td>Building1</td>
<td>200</td>
<td>On network/In use</td>
</tr>
<tr>
<td>Computer1836</td>
<td>HR</td>
<td>Server</td>
<td>Windows</td>
<td>Email Server</td>
<td>Building1</td>
<td>116</td>
<td>On network/In use</td>
</tr>
<tr>
<td>Computer1837</td>
<td>SALES</td>
<td>PC</td>
<td>Windows XP</td>
<td>Jonston</td>
<td>Building1</td>
<td>200</td>
<td>On network/In use</td>
</tr>
<tr>
<td>Computer1840</td>
<td>SALES</td>
<td>PC</td>
<td>Windows XP</td>
<td>Jones</td>
<td>Building1</td>
<td>200</td>
<td>Off network</td>
</tr>
<tr>
<td>Computer1846</td>
<td>SALES</td>
<td>PC</td>
<td>Windows XP</td>
<td>Padilla</td>
<td>Building1</td>
<td>200</td>
<td>On network/In use</td>
</tr>
<tr>
<td>Computer1850</td>
<td>HR</td>
<td>Server</td>
<td>Windows</td>
<td>Print Server</td>
<td>Building1</td>
<td>116</td>
<td></td>
</tr>
<tr>
<td>Computer1934</td>
<td>SALES</td>
<td>Server</td>
<td>No Selection</td>
<td>File Server</td>
<td>Building1</td>
<td>210</td>
<td>Spare</td>
</tr>
<tr>
<td>Computer1946</td>
<td>SALES</td>
<td>PC</td>
<td>Windows XP</td>
<td>Brown</td>
<td>Building1</td>
<td>200</td>
<td>On network/In use</td>
</tr>
<tr>
<td>Computer1991</td>
<td>SALES</td>
<td>PC</td>
<td>Windows 2000</td>
<td>Haddin</td>
<td>Building1</td>
<td>200</td>
<td>On network/In use</td>
</tr>
<tr>
<td>Computer1992</td>
<td>BIS</td>
<td>PC</td>
<td>Windows 2000</td>
<td>Petros</td>
<td>Building1</td>
<td>331</td>
<td>Off network</td>
</tr>
<tr>
<td>Computer1993</td>
<td>IT</td>
<td>PC</td>
<td>Windows 2000</td>
<td>Test1</td>
<td>Building1</td>
<td>Lab1</td>
<td>On network/In use</td>
</tr>
<tr>
<td>Computer1994</td>
<td>IT</td>
<td>PC</td>
<td>Windows 2000</td>
<td>Test2</td>
<td>Building1</td>
<td>Lab1</td>
<td></td>
</tr>
<tr>
<td>Computer1995</td>
<td>IT</td>
<td>PC</td>
<td>Windows 2000</td>
<td>Test3</td>
<td>Building1</td>
<td>Lab1</td>
<td></td>
</tr>
<tr>
<td>Computer1997</td>
<td>IT</td>
<td>PC</td>
<td>Windows 2000</td>
<td>Test4</td>
<td>Building4</td>
<td>Lab1</td>
<td></td>
</tr>
<tr>
<td>Computer1998</td>
<td>IT</td>
<td>PC</td>
<td>Windows 2000</td>
<td>Test5</td>
<td>Building3</td>
<td>Lab1</td>
<td></td>
</tr>
<tr>
<td>Computer1999</td>
<td>IT</td>
<td>PC</td>
<td>Windows 2000</td>
<td>Test6</td>
<td>Building4</td>
<td>Lab1</td>
<td></td>
</tr>
<tr>
<td>Computer2000</td>
<td>ENG</td>
<td>PC</td>
<td>Windows 2000</td>
<td>Kimmet</td>
<td>Building1</td>
<td>320</td>
<td>On network/In use</td>
</tr>
<tr>
<td>Computer2001</td>
<td>IT</td>
<td>PC</td>
<td>Windows 2000</td>
<td>Sanders</td>
<td>Building3</td>
<td>420</td>
<td>Spare</td>
</tr>
<tr>
<td>Computer2002</td>
<td>IT</td>
<td>PC</td>
<td>Windows XP</td>
<td>Portello</td>
<td>Building3</td>
<td>409</td>
<td>On network/In use</td>
</tr>
<tr>
<td>Computer2003</td>
<td>IT</td>
<td>PC</td>
<td>Windows 2000</td>
<td>Little</td>
<td>Building4</td>
<td>105</td>
<td>On network/In use</td>
</tr>
<tr>
<td>Computer2004</td>
<td>IT</td>
<td>PC</td>
<td>Windows 2000</td>
<td>Evans</td>
<td>Building4</td>
<td>105</td>
<td></td>
</tr>
<tr>
<td>Computer2005</td>
<td>HR</td>
<td>PC</td>
<td>Windows</td>
<td>Brighton</td>
<td>Building1</td>
<td>116</td>
<td>On network/In use</td>
</tr>
<tr>
<td>Computer2008</td>
<td>HQ</td>
<td>PC</td>
<td>Windows 2000</td>
<td>Tarquin</td>
<td>Building2</td>
<td>104</td>
<td></td>
</tr>
<tr>
<td>Computer2009</td>
<td>HQ</td>
<td>PC</td>
<td>Windows 2000</td>
<td>LAB1</td>
<td>Building2</td>
<td>104</td>
<td></td>
</tr>
<tr>
<td>Computer2010</td>
<td>HQ</td>
<td>PC</td>
<td>Windows 2000</td>
<td>LAB2</td>
<td>Building2</td>
<td>104</td>
<td></td>
</tr>
<tr>
<td>Computer2011</td>
<td>HQ</td>
<td>PC</td>
<td>Windows 2000</td>
<td>LAB3</td>
<td>Building2</td>
<td>230</td>
<td></td>
</tr>
<tr>
<td>Computer2012</td>
<td>HQ</td>
<td>PC</td>
<td>Windows 2000</td>
<td>LAB4</td>
<td>Building2</td>
<td>104</td>
<td></td>
</tr>
<tr>
<td>Computer2013</td>
<td>HQ</td>
<td>PC</td>
<td>Windows 2000</td>
<td>LAB5</td>
<td>Building2</td>
<td>104</td>
<td></td>
</tr>
<tr>
<td>Computer2014</td>
<td>HQ</td>
<td>PC</td>
<td>Windows 2000</td>
<td>LAB6</td>
<td>Building2</td>
<td>104</td>
<td></td>
</tr>
<tr>
<td>Computer2015</td>
<td>HQ</td>
<td>PC</td>
<td>Windows 2000</td>
<td>LAB7</td>
<td>Building2</td>
<td>104</td>
<td></td>
</tr>
<tr>
<td>Computer2016</td>
<td>HQ</td>
<td>PC</td>
<td>Windows 2000</td>
<td>LAB8</td>
<td>Building2</td>
<td>104</td>
<td></td>
</tr>
<tr>
<td>Computer2017</td>
<td>HQ</td>
<td>PC</td>
<td>Windows 2000</td>
<td>LAB9</td>
<td>Building1</td>
<td>233</td>
<td></td>
</tr>
<tr>
<td>Computer2018</td>
<td>HQ</td>
<td>PC</td>
<td>Windows 2000</td>
<td>LAB10</td>
<td>Building1</td>
<td>233</td>
<td></td>
</tr>
<tr>
<td>Computer2020</td>
<td>IT</td>
<td>PC</td>
<td>Windows 2000</td>
<td>Edrige</td>
<td>Building1</td>
<td>220</td>
<td>On network/In use</td>
</tr>
<tr>
<td>Computer2021</td>
<td>IT</td>
<td>PC</td>
<td>Windows 2000</td>
<td>Simson</td>
<td>Building1</td>
<td>220</td>
<td></td>
</tr>
<tr>
<td>Computer2029</td>
<td>SALES</td>
<td>PC</td>
<td>Windows XP</td>
<td>Pascal</td>
<td>Building1</td>
<td>200</td>
<td>On network/In use</td>
</tr>
<tr>
<td>Computer2030</td>
<td>IT</td>
<td>PC</td>
<td>Windows 2000</td>
<td>Hadley</td>
<td>Building1</td>
<td>220</td>
<td>Off network</td>
</tr>
</tbody>
</table>

**Figure 2: Example of a Computer Systems Inventory**
**Division Patch Advisory**

**Advisory Date:** June 14, 2007

**MS Patch or SP #:** MS07-030, MS07-031, MS07-032, MS07-033, MS07-034, MS07-035

**Date Issued by Microsoft – June 12, 2007**

**Priority Assigned = Moderate, Important, Critical:** Critical

**Desktop System Platform(s) affected:**

- Windows XP SP2,
- Windows XP SP1,
- Windows 2000 SP4,
- Windows Vista

**Impact of Vulnerability:** - Remote Code Execution

**Description of Patch/SP:**

[Link to Microsoft patch bulletin](http://www.microsoft.com/protect/computer/updates/bulletins/200706.mspx)

**Division Deployment**

**Effective Date to Depts:** June 14 - 19

**Deploy Dates to Division System Tiers:**

- Tier 1 - June 14
- Tier 2 - June 15 - 18 (Dares, TNSHelpDesk)
- Tier 3 - June 19

**Implementer:** Division IT Support

*Figure 3: Example of text used for a patch advisory*
### Figure 4: Example of Tracking Microsoft Patches

The report shown in Figure 4 is a very useful mechanism for tracking the deployment of patches. The numbers in the columns AF to BF show the number of systems which are reporting as unpatched between the dates 12/20/2006 and 6/20/2007. In theory, the number of system reporting unpatched should become zero over time, but in practice this is not so easy.

For instance, on line 30; zero systems are reporting as unpatched from 12/20/2006 to 5/2/2007 (nearly 5.5 months), until on 5/9/2007, 1 system reports as unpatched. This single system may have been a desktop system that was turned off until this time, or perhaps a laptop system that was not in use on the University network for these months. Either way, the responsible IT manager will need to assess the potential risk and decide whether to commit resources to tracking down/patching this single system, or focus on the deployment of other patches.

Assessing the potential risk of an unpatched system involves understanding what the patch does. For instance, on line 62, the highlighting and an “R” are used to indicate that this is a reissued patch, and is not a security patch. This type of information assists the IT manager in deciding on a course of action in setting the priority for ensuring the deployment of this patch.
Decisions about exceptions that the IT manager makes can be noted on this report (as they are in lines 155 and 156).

The most important trend that the IT manager should be able to see on this report is progress. For instance, on line 122; 196 systems report unpatched on 2/21/2007. By 2/28/2007, the number of systems reporting unpatched has dropped to 106 (a 54% reduction in one week), to 61 the next week (a 57% reduction), to 41 the next week and so on.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe Reader 8.0</td>
<td>12/1/2006</td>
<td>467</td>
<td>234</td>
<td>200</td>
<td>192</td>
<td>172</td>
<td>153</td>
<td>141</td>
<td>137</td>
<td>135</td>
<td>134</td>
<td>132</td>
<td>125</td>
<td>123</td>
<td>99</td>
<td>97</td>
</tr>
<tr>
<td>KB-931836-cumulative time zone update for Microsoft Windows operating systems</td>
<td>2/7/2007</td>
<td>7</td>
<td>7</td>
<td>5</td>
<td>5</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>KB931667-Addressing the daylight saving time changes in 2007 using the Outlook Time Zone Data Update Tool</td>
<td>1/30/2007</td>
<td>11</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>5</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Google Internet Tool Bar</td>
<td>1/1/2007</td>
<td>26</td>
<td>26</td>
<td>35</td>
<td>36</td>
<td>29</td>
<td>18</td>
<td>16</td>
<td>4</td>
<td>6</td>
<td>5</td>
<td>7</td>
<td>11</td>
<td>10</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

**Figure 5: Example of Tracking 3rd Party Software Patches**

The IT manager also needs to be able to track patch management progress for non-security or 3rd party software as well. The report in Figure 5 demonstrates a way to do this.

Again, the numbers in the columns from 3/7 to 6/20 are systems that are reporting back as unpatched.
### Figure 6: Tracking Microsoft Vulnerabilities by Computer

To get a high level view of patch management plan progress by individual computer, the IT manager might use a report similar to the one shown in Figure 6. Here, the IT manager can not only see the relative state of compliance of each computer (given by %), but also the number of vulnerabilities that remain on each system.

In this report, a system with the name “Computer1066” suddenly appears on 13\(^{th}\) June 2007. Looking at previous weeks, the IT manager can see that this system does not appear before this date. Further investigation shows it to be a new system that was not full patched. In this case, there are less complications to update the patches on this new system. By the following week, the system no longer appears on the list of systems with vulnerabilities.
Finally, sometimes the IT manager may want to be able to track the patch management plan progress by a specific vulnerability.

In Figure 7, the report being used gives information about location, assigned user and usage. Such information is valuable to the IT manager when setting priorities for ensuring the Google Tool Bar is removed.

In this case, by 6/13/2007, it was decided that priorities should be the human resources department, all managers, and the information technology department (with the exception of one test machine to further research the vulnerability).

The next set of priorities included all user systems that were not used for testing. This was achieved by 6/20/2007, however, by then two more users had downloaded and installed the vulnerability.
Appendix F: Acquiring Anti-Virus Software for Home Use

SDSU has a site license for McAfee anti-virus (AV) and a site license for McAfee ePolicy Orchestrator (ePO) console.

University staff, faculty and students may acquire a free copy of anti-virus software from the Student Computer Services Help Desk or the TNS Help Desk in Love Library.

All users with Rohan email accounts (faculty, staff and students) should go to the Student Computer Services Help Desk.

All faculty and staff with campus email server accounts should go to the TNS Help Desk.

Both Help Desks use the same form which University staff, faculty and students will need to fill out and sign.

University staff, faculty and students will need to show SDSU identification for email account confirmation.

University staff, faculty and students will need to provide a blank CD onto which the anti-virus software will be burnt.

Any questions regarding installation and licensing of the anti-virus software should be addressed to the appropriate help desk, and not to the IT Security Office.
Appendix G: Windows XP Workstation Standard Build Sample

DISCLAIMER: Sample documentation provided in this section is for example only. Each department should develop their own documentation based on processes, requirements and risks that are unique to them.

The following is an example of a Windows XP Pro Standard Workstation Configuration. In this example, software and user profiles are stored on a server called “Server1”, and the standard applications include McAfee anti-virus, Acrobat Reader, Eudora, WinZip, Spybot, Meeting Maker, Office 2003 and Altiris. Also, an Active Directory domain is used.

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>STEP</strong></td>
<td><strong>PROCESS</strong></td>
</tr>
<tr>
<td><strong>Consolidate &amp; Backup User’s Data</strong></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>User Prep</td>
</tr>
<tr>
<td>2</td>
<td>Update Inventory</td>
</tr>
<tr>
<td>3</td>
<td>Vendor Image</td>
</tr>
<tr>
<td>4</td>
<td>Local Account Profiles</td>
</tr>
<tr>
<td>5</td>
<td>Active Directory Profiles</td>
</tr>
<tr>
<td>6</td>
<td>Consolidate/Backup Data</td>
</tr>
<tr>
<td><strong>Install and Configure Win XP</strong></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Notify AD Admin</td>
</tr>
<tr>
<td>2</td>
<td>Create a fresh installation</td>
</tr>
<tr>
<td>3</td>
<td>Begin process</td>
</tr>
<tr>
<td>4</td>
<td>License agreement</td>
</tr>
<tr>
<td>5</td>
<td>Select installation</td>
</tr>
<tr>
<td>6</td>
<td>Delete old partitions</td>
</tr>
<tr>
<td>7</td>
<td>Delete system partition</td>
</tr>
</tbody>
</table>
8. **Confirm partition deletion**
   To delete this partition, press `<L>`.

9. **Select unpartitioned space**
   To set up Windows XP on the selected item, press `<ENTER>`.

10. **Format unpartitioned space**
    Select, "Format the partition using the NTFS file system" then press `<ENTER>`.

11. **Format process begins**
    C: Partition1 [New (Raw)] 76285 MB (76285 MB free)... Setup is formatting...

12. **Files copied to installation folder**
    "Please wait while Setup copies files to the Windows installation folders..."

13. **System re-boots**
    Leave the installation CD in the CD-ROM Drive. Ignore the prompt, "Press any key to boot from CD." The system boots from the hard drive.

14. **Installing devices begins**
    No action required.

15. **Set regional/language settings**
    Press `<Next>`.

16. **Personalize software**
    Enter `<SDSU>` for Name and `<DeptName>` for Organization, then press `<Next>`.

17. **Product Key**
    Enter the Windows Product Key (if necessary).

18. **Set computer name & admin password**
    Enter the State-ID for Computer name. Enter the standard local administrator's password for Administrator password, then press `<Next>`.

19. **Set date & time**
    Verify the current Date and Time. Time Zone should be set to "(GMT-08:00) Pacific Time (US & Canada); Tijuana" and the daylight savings check box selected. Press `<Next>`.

20. **Install components**
    Messages display as Setup installs the Network and Start Menu Items, registers components, saves settings, and removes temporary files. No action is required.

21. **Network Settings**
    `<Select>` (click-on) radio button "Typical" then press `<Next>`.

22. **Workgroup or Domain**
    `<Select>` (click-on) radio button "no", leave as WORKGROUP then press `<Next>`.

23. **Install components**
    Messages display as Setup installs the Network and Start Menu Items, registers components, saves settings, and removes temporary files. No action is required.

24. **Finalize installation**
    The system restarts. Again, ignore the prompt, "Press any key to boot from CD." The system boots from the hard drive.

25. **Configure display**
    When prompted, "To improve the appearance of visual elements...", the display resolution settings are optimized, press `<OK>` | `<OK>` to accept the new settings.

26. **Welcome to Windows**
    Press `<Next>`.

27. **Help Protect your PC**
    `<Select>` (click-on) the radio button, "Not right now" to turn off automatic updates, then press `<Next>`.

* The next two steps may or may not appear during set up of Windows XP

28. **How will computer connect to the Internet**
    `<Select>` (click-on) the radio button, "Local Area Network (LAN)", then press `<Next>`.

29. **Setting up Connection**
    `<Select>` (click-on) the radio button "Obtain IP automatically" and configure DNS for IPs 16.81, 16.85, 1.1 and 200.1. IF the IPs cannot be entered then `<Select>` "Obtain DNS automatically" then press `<Next>`.

30. **Ready to register with Microsoft?**
    `<Select>` (click-on) the radio button, "Not at this time", then press `<Next>`.

31. **Set primary user account "Who will be using this computer?"**
    Enter a temporary user account "admin2" then press `<Next>`. No local accounts are to be made available for department users. Note: the account is created without a password. Additionally the account is added to the Administrator group. Later, we’ll remove the account from the system.

32. **Setup completes**
    At the "Thank you!" prompt, press `<Finish>`.

33. **Welcome to Windows**
    The computer logs in under your user account to the desktop.

34. **Prep for Admin log in**
    Launch Control Panel, `<Select>` User Accounts, `<Select>` "Change the way users log on or off" `<De-select>` (uncheck) "Use the Welcome screen" | `<Apply Options>` | `<close>`. Log Off Machine. Note: disabling Win XP's welcome screen forces Windows Classic logon: `<Ctrl>` + `<Alt>` + `<Delete>` | enter `<account>` | enter `<password>`.

35. **Log in as Administrator**
    Log in using user name: administrator

36. **Win XP desktop**
    Launch Control Panel to set the desktop, taskbar, and folder options to Windows Classic view.
36 Control Panel  
Click on <Switch to Classic View>

37 Folder Options, General Tab  
Double-click on <Folder Options>. The Folder Options dialog box displays. Under the "General" tab, <Select> (click-on) on the following radio buttons, "Use Windows classic folders", "Open each folder in the same window", and "Double-click to open an item (single-click to select)". Then press <Apply>.

38 Change Folders to List View  
Click on the <View> tab. Under the heading, "Advanced settings" make the following changes: <Select> (check) the following boxes: "Display the contents of system folders", "Display the full path in the title bar", and "Show hidden files and folders". <De-select> (uncheck) the following boxes: "Hide extensions for known file types", "Hide protected operating system files (Recommended)" press <Yes>, "Show pop-up description for folder and desktop items" and "Use simple file sharing (Recommended)". Then press <Apply> then press <OK>.

39 Taskbar and Start Menu Properties  
Select the <Start Menu> tab and <Select> (click-on) the radio button, "Classic Start menu", then press <Customize>. From the scrolled region, under the heading, "Advanced Start menu options". <Select> (check) "Display Favorites", <Select> (check) "Show Small Icons in Start menu" and <De-select> (uncheck) "Use Personalized Menus", then press <Apply>.

40 Start Menu Tab  
Double click <Add or Remove Programs> | <Add/Remove Windows Components>. Under the heading "Components", from the scroll-down menu, select <Accessories and Utilities> | <Details> | <De-select> (uncheck) <Games> | <OK>.

41 Windows Components, continued  
Scroll down the components list and <De-select> (uncheck) the following: "MSN Explorer", "Networking Services", "Outlook Express", and "Windows Messenger", then press <Next>, and <Finish>. Press <Yes> to restart your computer.

42 Bios Boot Sequence  
On restart enter the computer BIOS. Reset the boot sequence to (1) hard drive, (2) CD-ROM, and (3) Floppy Drive.

43 Log On to Windows  
Logon as administrator.

44 Set the Desktop to Win Classic  
Right-click on the desktop, then select <Properties>. Under the "Themes" tab, select <Windows Classic> from the Theme pull-down menu. Click on the <Desktop> tab. Press <Customize Desktop>. Under the heading Desktop icons, de-select (uncheck) <Internet Explorer>. Under the heading, "Desktop cleanup" <De-select> (uncheck) "Run Desktop Cleanup Wizard every 60 days", then press <OK>.

45 Screen Saver  
Click on the <Screen Saver> tab. From the Screen Saver pull-down menu, select <Windows XP>. Set the wait time to 15 minutes and <Select> (check) "On resume, password protect". Then press <Apply>.

46 Display Power Settings  
On the Screen Saver tab, click on POWER button. Set the wait time to power off monitor to 20 minutes and select NONE for turn off hard disks. Then press <Apply>, it may be the default setting so only <OK> may need to be selected.

47 Appearance  
Click the <Appearance> tab. From the "Windows and buttons" pull-down menu, select <Windows Classic style>. From the "Color scheme" pull-down menu, select <Windows Standard>. Then press <Apply>, it may be the default setting, if so then go to step #48. Do not press <OK>.

48 Settings  
Click the <Settings> tab. Set the screen resolution to <1024 X 768> for CRT displays, or <1280 X 1024> for LCD displays. Set color quality to <Highest>, then press <Apply>, <Yes> to accept the settings, then <OK>.

49 Set Refresh Rate  
In the Settings tab click on <Advanced> button. Click on the <Monitor> tab. Refresh frequency should be set to 75 Hertz or higher.
<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>50</td>
<td><strong>Search for files and folders</strong>&lt;br&gt;Click on <code>&lt;Start&gt;</code></td>
</tr>
<tr>
<td>51</td>
<td><strong>Desktop Icons</strong>&lt;br&gt;Rename 'My Network Places' to 'Network'. Rename 'My Computer' to 'Computer'.</td>
</tr>
<tr>
<td>52</td>
<td><strong>Load Drivers</strong>&lt;br&gt;Remove the Win XP installation disk from the CD-ROM drive and insert the vendor’s &quot;Drivers and Utilities&quot; CD to install drivers for onboard components such as: NIC, Video, and sound adapters.</td>
</tr>
<tr>
<td>53</td>
<td><strong>Connect network cable</strong>&lt;br&gt;Connect network cable to the computer</td>
</tr>
<tr>
<td>54</td>
<td><strong>Map Network Drive</strong>&lt;br&gt;<code>\server1\DeptName</code>. Connect with user name and password.&lt;br&gt;Open &quot;Install Shortcuts&quot; folder.</td>
</tr>
<tr>
<td>55</td>
<td><strong>Install McAfee from Server</strong>&lt;br&gt;Double-Click on McAfee 8.0i icon and install McAfee. For license expiry type select &quot;perpetual&quot;. On next screen select &quot;typical&quot; setup. When complete uncheck Run On-Demand Scan. press <code>&lt;Finish&gt;</code> McAfee updates and then click <code>&lt;OK&gt;</code> and restart computer.</td>
</tr>
<tr>
<td>56</td>
<td><strong>Log On to Windows</strong>&lt;br&gt;Log on as administrator.</td>
</tr>
<tr>
<td>57</td>
<td><strong>Install Microsoft Update</strong>&lt;br&gt;Start Internet Explorer, (click on) <code>&lt;Tools&gt;</code></td>
</tr>
<tr>
<td>58</td>
<td><strong>Change Automatic Updates</strong>&lt;br&gt;Leave off and <code>&lt;Select&gt;</code> Check for updates. <code>&lt;Select&gt;</code> custom. Select all available updates. Continue the updates (sometimes restarting computer) until all updates are completed.</td>
</tr>
<tr>
<td>59</td>
<td><strong>Delete Windows Update</strong>&lt;br&gt;From desktop click <code>&lt;Start&gt;</code> and right click on windows update and delete, click <code>&lt;Yes&gt;</code>&lt;br&gt;&lt;br&gt;<strong>Install Standard BFA Desktop Applications</strong>&lt;br&gt;Map a drive to <code>\server1\DeptName\Install Shortcuts</code>, then install applications from network by launching each of the following shortcuts</td>
</tr>
<tr>
<td>60</td>
<td><strong>Install Shortcuts</strong>&lt;br&gt;Double Click &quot;AcrobatReader708.exe&quot; <code>&lt;next&gt;</code></td>
</tr>
<tr>
<td>61</td>
<td><strong>Acrobat Reader 7.0</strong>&lt;br&gt;Double Click &quot;AcrobatReader708.exe&quot; <code>&lt;next&gt;</code></td>
</tr>
<tr>
<td>62</td>
<td><strong>Eudora Installation</strong>&lt;br&gt;Eudora 7.0.1. Do not select <code>&lt;deselect&gt;</code> pure voice or Importers. Grant Full Control to Users via security tab for the Qualcomm directory. This will have to be done after user logs in with domain account first time. Restore User's configuration settings from the backup copy, from the Consolidate/Backup User's procedure. Files to restore are: Mailboxes, tocs, NNdbase.txt &amp; .toc, and descmap.pce. Also include attachments, embedded, Filters, Sigs, Stationery, Nickname &amp; any user-created mailbox folder.</td>
</tr>
<tr>
<td>63</td>
<td><strong>DEPT W2K-XP Changes.reg</strong>&lt;br&gt;Double-click DEPT W2K-XP Changes.reg. <code>&lt;select&gt;</code> 'yes' and &quot;ok&quot;</td>
</tr>
<tr>
<td>64</td>
<td><strong>Winzip</strong>&lt;br&gt;Double Click &quot;Winzip (Run this 1st!)&quot; <code>&lt;ok&gt;</code></td>
</tr>
<tr>
<td>65</td>
<td><strong>FTP</strong>&lt;br&gt;Double Click &quot;WS_FTP32&quot;. <code>&lt;Continue&gt;</code> and then <code>&lt;select&gt;</code> &quot;A student, faculty member or staff of an educational institution.&quot; <code>&lt;next&gt;</code></td>
</tr>
<tr>
<td>66</td>
<td><strong>SpyBot</strong>&lt;br&gt;See SpyBot documentation for install</td>
</tr>
</tbody>
</table>
67 Meeting Maker 8.5
Double-Click "Meeting Maker 8.5" <next>|<next>|<next>... Select yes for "default calendar application. <finish> Meeting Maker will run. For server <select> to configure. Protocol is SSL and select proper server. From start menu move the MeetingMaker icon from C:|documents and settings|administrator|start menu|programs to C:|documents and settings\all users\start menu|programs. Next right click on the icon and select properties and the security tab. Click add and type users. Allow users full control and <select> "Apply". <select> advanced. Under "permission properties" highlight users and then check both boxes on bottom of window. Click <apply>|<yes>|<ok>|<ok>. Go to C:|program files and right-click on the Meeting Maker folder. <select> properties and then the security tab. Click on users and allow full control. <select> advanced and check the box that states "Replace permission entries..." <apply> | <yes> - close the windows, install complete.

68 Office 2003
Double-Click Office2003 to install.

69 Disconnect Network Drives
Disconnect \Server1\DeptName as a mapped drive.

70 Shortcuts
set up shortcuts in Quick Launch bar for applications Meeting Maker, Eudora, Excel, Word and others that user may want.

71 ***
Next step for single install. If set up is for deployment by image this step should be done on each separate computer after deployment.

72 Altiris
Double-click "Altiris agent download" Allow Install the active X control. <select> "install" and click on "click here to begin the download and install." Close Internet Explorer.

73 Install A-Client & SIDGEN
On \Server1\PCApps\Altiris\Aclient double click on Aclient.exe to install Aclient. In first window <next>|<next> check the box that says "Enable changing of security ID (Windows NT only)" then click "advanced" and enter host name: 130.191.16.87. Click <ok>|<next>|<next>|<finish>

74 Join computer to DEPT Domain
Join the computer to the DEPT domain. Right Click <Computer> Select "custom" and install updates for Office Programs and other updates that were missed. Continue to check for updates until none are available.

75 Login using admin2 account
Login into Windows under the admin2 account. From start menu go to control panel, click on <Switch to Classic View> and then double-click Folder Options. Click on the view tab and then under advanced settings make sure that "Show hidden files and folders" is selected. Click <Apply> if necessary and then <OK>. (Don't close control panel)

76 Check LAG & LPUG
Check that domain GPO has taken effect; go to Computer/Manage/Local Groups and under Administrators confirm that LAG-(dept name) appears. Under Power Users confirm that LPUG-(dept name) appears. Examples: LAG-EHS; LPUG-EHS

77 Set a default user profile
In control panel double click <System> and click <Advanced> tab and click <Settings> under the User Profiles menu. Under user profiles select the user profile for the jsmith account.

APPENDIX G
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>77</td>
<td>Set a default user profile&lt;br&gt;In control panel double click <code>&lt;System&gt;</code> and click <code>&lt;Advanced&gt;</code> tab and click <code>&lt;Settings&gt;</code> under the User Profiles menu. Under user profiles select the user profile for the jsmith account.&lt;br&gt;Select <code>&lt;Copy To&gt;</code> and browse/navigate to &quot;C:\Documents and Settings\Default User&quot;, click <code>&lt;OK&gt;</code>. In the Permitted to use field click <code>&lt;Change&gt;</code> and type &quot;EVERYONE&quot; Click <code>&lt;OK&gt;</code>. You will then need to log in using your domain login account. Click <code>&lt;OK&gt;</code></td>
</tr>
<tr>
<td>78</td>
<td>Login using claub account&lt;br&gt;From desktop, right click <code>&lt;Computer&gt;</code> select properties. Click <code>&lt;Advanced&gt;</code> tab and click <code>&lt;Settings&gt;</code> under the User Profiles menu. Under user profiles select the user profile for the admin2 account. Click <code>&lt;Delete&gt;</code>, delete the admin2 user profile. Confirm click <code>&lt;Yes&gt;</code>.&lt;br&gt;Login using claub account</td>
</tr>
<tr>
<td>78</td>
<td>remove admin2 account&lt;br&gt;Launch Control Panel to delete the admin2 account set up in step 30. <code>&lt;Control Panel&gt;</code></td>
</tr>
<tr>
<td>79</td>
<td>Configure Network Settings&lt;br&gt;Right-click on the &quot;Network&quot; icon from the desktop <code>&lt;select&gt;</code> &quot;properties&quot;. Right-click on the &quot;Local Area Connection&quot; and <code>&lt;select&gt;</code> &quot;properties.&quot; Left-click on &quot;Internet Protocol (TCP/IP)&quot; and <code>&lt;select&gt;</code> &quot;Properties.&quot; If the department specified a static IP Address, configure it now. If a static IP Address is not available, then configure DHCP connectivity. Note: the department must request a new IP Address assignment from TNS.</td>
</tr>
<tr>
<td>80</td>
<td>Configure DNS Servers (if unable to do so at Step 28)&lt;br&gt;<code>Click</code> &quot;Use the following DNS Server addresses&quot; The preferred DNS Server is 130.191.16.85. Alternate DNS server is 130.191.16.81. <code>&lt;Select&gt;</code> &quot;advanced.&quot; <code>&lt;Select&gt;</code> DNS&quot; tab. Under the DNS server addresses <code>&lt;select&gt;</code> &quot;add.&quot; Add 130.191.1.1 and then add 130.191.200.1. <code>&lt;Click&gt;</code> Ok</td>
</tr>
<tr>
<td></td>
<td>*** Next steps form image deployment systems only. If set up is for single computer then steps are completed. ***</td>
</tr>
<tr>
<td></td>
<td>SIDGEN Delete&lt;br&gt;If the primary image has been deployed SIDGEN must be deleted on each of the computers that received the image as well as on the primary computer. SIDGEN is found in the C:\Program Files\Altiris\Acient Directory. Delete after the first boot up of the computer.</td>
</tr>
<tr>
<td></td>
<td>Rename computer&lt;br&gt;rename the computer to its specific State ID Tag.</td>
</tr>
<tr>
<td></td>
<td>Install Altiris&lt;br&gt;See step 72 for instructions.</td>
</tr>
<tr>
<td></td>
<td>Join computer to BA Domain&lt;br&gt;Join the computer to the DEPT domain. Right Click <code>&lt;Computer&gt;</code> Select properties. <code>&lt;Select&gt;</code> change. Under &quot;member of&quot; menu, <code>&lt;select&gt;</code> Domain. Type &quot;BA.SDSU.EDU&quot; Enter your domain user name and password. <code>&lt;OK&gt;</code></td>
</tr>
</tbody>
</table>
Appendix H: Windows 2003 Server Standard Build Example

DISCLAIMER: Sample documentation provided in this section is for example only. Each department should develop their own documentation based on processes, requirements and risks that are unique to them.

The following is an example of a Windows Server 2003 Configuration.

<table>
<thead>
<tr>
<th>Item #</th>
<th>TO DO ITEM &amp; Details</th>
<th>Add'l Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Inventory</td>
<td>If the Server is new, give a PO-invoice copy to Department Mgr for inventory &amp; tagging.</td>
</tr>
<tr>
<td>2</td>
<td>Vendor Image</td>
<td>If server is new, use Altiris to create image of drive for possible emergency restoral.</td>
</tr>
<tr>
<td>3</td>
<td>DNS Register</td>
<td>Process DNS Registration request.</td>
</tr>
<tr>
<td>4</td>
<td>IP</td>
<td>Request IP from Bids IP Database.</td>
</tr>
<tr>
<td>5</td>
<td>Start OS installation</td>
<td>Boot from the Windows 2003 CD and format Drive. Do a reformat as NTFS whether old or new drive.</td>
</tr>
<tr>
<td>Network settings</td>
<td>Done during OS installation wizard:</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Under TCP/IP properties, configure network IP</td>
<td>Designate 130.191.1.1 &amp; 200.1 as DNS servers.</td>
</tr>
<tr>
<td>7</td>
<td>Click on &gt;Advanced &gt; DNS Tab</td>
<td>For “Append these DNS suffixes...” add “sdsu.edu” entry.</td>
</tr>
<tr>
<td>8</td>
<td>Add “sdsu.edu” in “DNS suffix for this connection”</td>
<td>Clear (deselect): “Register this connection’s addresses in DNS”.</td>
</tr>
<tr>
<td>9</td>
<td>Join dept.sdsu.edu domain using your individual domain admin account as authority</td>
<td>Computer name = Property tag # or C-series tag #.</td>
</tr>
<tr>
<td>10</td>
<td>Company &amp; Organization = SDSU &amp; DEPT</td>
<td>Using login as local Administrator:</td>
</tr>
<tr>
<td>11</td>
<td>Service Pack</td>
<td>Install the latest Service packs.</td>
</tr>
<tr>
<td>12</td>
<td>Local Accts</td>
<td>If it is not already done, rename local “Administrator” account to “jsmith” or other as announced; Renaming may occur automatically by DEPT domain policy if in effect. Sysadmin must enter his/her pwd manually.</td>
</tr>
<tr>
<td>13</td>
<td>Create local admin accounts. One primary account (renamed upon joining DEPT domain). One backup account.</td>
<td>Use local account logons minimally. Use local login in event of severance from domain &amp; to rejoin domain, domain login lock out or disablement of primary accounts.</td>
</tr>
<tr>
<td>14</td>
<td>Disable the built-in &quot;guest&quot; account &amp; assure it was renamed &quot;guest123&quot; by domain policy; if not, rename manually.</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Display Properties &gt; set Screen area to 1024 x 768</td>
<td>For servers, the typical condition should be a Logged out status.</td>
</tr>
<tr>
<td>17</td>
<td>For local admin profiles set Screen saver to Logon Screen Saver &gt; Wait: 5 min &gt; select &quot;Password Protected&quot;</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Local Area Connection properties = select &quot;Show icon in taskbar when connected&quot; so that network speed displays in sys-tray</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Start &gt; Run &gt; secpol.msc Account Policies &gt; Minimum password length = 8 characters; enable &quot;Passwords must meet complexity requirements&quot;</td>
<td>The need to perform these steps may be superceded by a Global Domain policy.</td>
</tr>
<tr>
<td>20</td>
<td>Start &gt; Run &gt; secpol.msc Local Policies &gt; Audit Policy &gt; Audit account logon events &gt; &quot;Audit these attempts&quot; select &quot;Failure&quot; &amp; &quot;Success&quot;</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Start &gt; Run &gt; secpol.msc Local Policies &gt; Security Options &gt; Additional restrictions for anonymous &gt; select &quot;Do not allow enumeration of SAM accounts and shares&quot;</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Start &gt; Run &gt; secpol.msc Local Policies &gt; Security Options &gt; Interactive login: Do not display last user name</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>Control Panels: enable Auto Update by selecting &quot;Keep my computer up to date.&quot; and Notify me but don’t automatically download or install them</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>Do not modify any object’s security settings</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>Record any, all created shares for server administration:</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>Record any disabled/stopped services:</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>Create standard TCP/IP Port for assigned printer</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>Server Standard Programs: Install from \Server1\Install Shortcuts</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>McAfee 8.X, plus ePO</td>
<td>Verify current status of DAT &amp; Scan Engine</td>
</tr>
<tr>
<td>30</td>
<td>Browser IE; current version plus all security patches</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>Adobe Acrobat, current version</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>WinZip 7 (Start with WinZip Classic)</td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>NovaNET: if backup of server is required, please submit request to NN sysadmin with</td>
<td></td>
</tr>
</tbody>
</table>

**APPENDIX H**
<table>
<thead>
<tr>
<th>Configure</th>
<th>Configurations Using admin2 logon profile:</th>
</tr>
</thead>
<tbody>
<tr>
<td>34</td>
<td>Windows Explorer view settings</td>
</tr>
<tr>
<td></td>
<td>Folder display: View &gt; Details Tools &gt; Folder Options &gt; Use Windows classic folders &gt; Apply; View &gt; Advanced Settings</td>
</tr>
<tr>
<td></td>
<td>Select: Display compressed files and folders with alternate color</td>
</tr>
<tr>
<td>35</td>
<td>Display the full path in the address bar; Show hidden files and folders; Display the full path in title bar</td>
</tr>
<tr>
<td></td>
<td>Deselect &quot;Hide file extensions of known file types&quot; &gt; Apply &gt; Like Current Folder &gt; Yes &gt; OK</td>
</tr>
<tr>
<td>36</td>
<td>Launch IE to configure without creating an e-mail account, with no selection for proxy server, and make sdsu.edu the home page</td>
</tr>
<tr>
<td></td>
<td>If server is an upgrade of a prior server, remember to save &amp; import existing useful IE Favorites</td>
</tr>
<tr>
<td>37</td>
<td>Go to Add/Remove &gt; Windows components to remove Outlook</td>
</tr>
<tr>
<td></td>
<td>Delete Outlook shortcuts &amp; extra unused icons</td>
</tr>
<tr>
<td>38</td>
<td>Right-click Task Bar &amp; clear &quot;Use Personalized Menus&quot;</td>
</tr>
</tbody>
</table>

**Server Rebuild**

39 If server administrator determines a rebuild of the server or reformatting of its drive(s) is necessary, please notify ITSO & submit rebuild plan to BIDS Manager.

**Additional Operational Notes:**

- **a** Server must remain a member of the dept.sdsu.edu domain at all times
- **b** Passwords: do not display server login passwords
- **c** Notify all DEPT Techs or/and department DAREs/End users as appropriate if shutdown or disable of networking on server is necessary, including date/time of outage.
- **d** Abide by the SDSU Computing Acceptable Use Policy published at: http://security.sdsu.edu/policy/aup.html
- **e** On-line subscriptions to mailing lists or other lists must have a defined business need to be approved by ITSO or DEPT Manager

**DATE:**

**SERVER ADMINISTRATOR SIGNATURE:**
Appendix I: Application Security Attacks and Countermeasures

Testing Application Dependencies

Applications are heavily dependent on the resources of their host operating system. Testing should be done to ensure that failures in the operating system will not result in unintended or new vulnerabilities in the application. There are different attacks to test for this.

Attack1: Blocking Access to Libraries; an attacker can exploit the dependency of application software on operating system or third party software libraries for functionality, causing the application to become insecure if the libraries fail to load.

Countermeasures:
- Application error handlers should be executed to maintain stability and communicate the error (if appropriate)

Attack2: Manipulating Registry Values; an attacker can exploit the dependency of application software on operating system registry values to locate and access files, directories and libraries, causing the application to become insecure if the registry values are changed or absent

Countermeasures:
- Do not store sensitive information in the registry

Attack3: Using Corrupt Files and File Names; an attacker can exploit the dependency of application software to read from and write to the file system during normal operation, causing the application to become insecure if the files or filenames are corrupt

Countermeasures:
- Ensure that files used exclusively by the application cannot be altered by any other process
- Application error handlers should be executed to ensure that the application can gracefully handle corrupt files or filenames without exposing sensitive information or becoming insecure

Attack4: Manipulating or Replacing Files Created by the Application: an attacker can exploit the dependency of application software to process information, causing the application to become insecure if the information is corrupt

Countermeasures:
- Ensure that information used exclusively by the application cannot be altered by any other process
Application error handlers should be executed to ensure that the application can gracefully handle corrupt information without becoming insecure.

**Attack5:** *Limiting Resource Availability*; an attacker can exploit the dependency of application software to use memory for loading and operating, and disk space or network availability for read and write operations, causing the application to become insecure if the resources are limited or removed.

*Countermeasures:*
- Ensure that sufficient memory and hard drive space are available to the application.
- Ensure that unused memory can be released for use if necessary.
- Ensure that the initial setup of the host operating system and application includes the use of disk partitioning to provide sufficient disk space for expansion.

**Testing the Application User Interface**

Many security issues related to the user interface are due to unintended and/or undocumented user behavior, or manipulation of the user interface functionality by an attacker. Applications should be able to handle unexpected input without becoming compromised. Attacks that may exploit the application user interface include:

**Attack1:** *Replay Attacks*; an attacker can capture an entire message and send it multiple times to a server, causing to server to repeat the requested operation, leading to the attacker gaining unauthorized access, or the server suffering a self-induced denial of service attack.

*Countermeasures:*
- Utilize timestamps from trusted time servers to protect against relayed messages.

**Attack2:** *Cookie Hijacking*; an attacker can exploit an application that uses persistent cookies on the user’s system to compromise the user’s account, if that attacker knows the user’s password, has physical access to the user’s computer, has administrative network access to the user’s computer, has broken into the user’s computer, or can see the network to sniff traffic.

*Countermeasures:*
- Require a separate login each session.
- Provide limited account access without re-authentication.
- Ensure all cookies should have a reasonable fixed expiration date that requires re-authentication.
Tie the cookie to identifying information other than the user, such as IP address, user agent string, and so on.

Never store actual user information in cookies; store a token that points to user information on the server's database.

Cookies can be marked secure, preventing their transmittal to non-SSL web pages.

Cookies also have domain and path properties to limit a cookie's scope. If you fail to set boundaries for cookies, it may be possible for an attacker to exploit a cross-site scripting flaw on another web page or even another server to hijack a user's cookie.

**Attack3:** *Altering Common Switches and Options*; an attacker can exploit a user interface which allows for the use of command line switches and options, causing the resulting change in configuration of the application (due to the use of a switch or option, such as changing memory allocation) to lead to the application being in an insecure state.

**Countermeasures:**
- Test the application for stability under all combinations of common switches and options.
- Restrict the code paths that can be manually specified using switches and options.
- Use application error handling routines to check configuration input before it is executed.

**Attack4:** *Using Escape Characters, Character Sets and Commands*; an attacker can exploit a user interface which allows for the use of special escape characters, character sets and commands, causing the application to become insecure.

Countermeasures:
- All allowable characters should be detailed in a documented security standard which addresses:
  - How the commands or characters are being interpreted.
  - The language the application is written in.
  - The libraries that are used.
  - The specific words and strings reserved by the underlying operating system.

**Attack5:** *Unvalidated input*; an attacker can tamper with any part of the HTTP request (such as the URL, querystring, headers, cookies, form fields or hidden fields) to try to bypass a website’s security mechanisms.
Countermeasures:

- Use pre-tested code to ensure that all parameters are validated before they are used.
- Parameters should be validated against a positive specification that defines:
  - Data type (string, integer, and so on)
  - Allowed character set
  - Minimum and maximum length
  - Whether null is allowed
  - Whether the parameter is required or not
  - Whether duplicates are allowed
  - Numeric range
  - Specific legal ranges (enumeration)
  - Specific patterns (regular expressions)

Attack 6: Broken access control (authorization); an attacker can take advantage of a collection of access control rules for the same application, which were written for different reasons and at different times, and do not provide cohesive protection for the application

Countermeasures:

- Use an access control matrix to define the access control rules
- In the security standard, document access rules for types of users, the type of content they can access, and the functions they can perform
- Extensively test the access control mechanism to ensure there is no way to bypass the amalgamated collection of controls

Attack 7: Improper error handling; an attacker can use detailed messages referring to internal system errors to uncover flaws in the web application

Countermeasures:

- Error handling should be implemented according to a documented security standard which specifies which information should be reported back to the user, which information should be logged, and so on

Attack 8: View Source information; an attacker can search through the source of each page to find information such as user names, default passwords, e-mail addresses, auto-redirection information and external links in comment fields

Countermeasures:

- Do not store sensitive information in the comment fields of the source pages
**Attack 9:** Browsable directories; an attacker can use default browsable directories (those which show a listing of all files in the directory) to expose unnecessary information

**Countermeasures:**
- Set permissions to prevent access to all the directories that are not necessary to the function of the web server

**Attack 10:** Hidden form fields manipulation; an attacker can use hidden fields (those not being displayed to the user) to access information the application is storing about user names, passwords, financials, and so on

**Countermeasures:**
- Do not allow hidden input values

**Testing the Application Server**

Decisions and changes in the application design and implementation process (that do not go through a proper validation and verification process) can lead to component interaction and inherent flaws that create vulnerabilities in the finished product. IT support staff should have a list of specific security requirements that emphasize:

- Which interfaces their components should extend to the rest of the application
- What form of information will the components receive
- Which computations should be performed on that information

Without this, the implementation will be vulnerable to a number of attacks, such as:

**Attack 1:** Using System Accounts; an attacker can exploit hidden or undocumented user accounts in an application in which user actions are governed by the assigned level of access an account is given

**Countermeasures:**
- Ensure that user credentials are not cached
- Ensure that the application does not make use of any undocumented or unconfigurable system accounts with elevated privileges that may be exploited by application users

**Attack 2:** Utilizing Unprotected Test Interfaces; an attacker can exploit applications which allow both documented and undocumented Application Program Interfaces (API’s) and software hooks which bypass normal security checks, to be temporarily added to the application for testing purposes, only to become part of the eventual working product
Countermeasures:
- Identify all software libraries that are loaded and used by the application, and evaluate their impact on application security

Attack 3: *Fake the Information Source*; an attacker can exploit an application’s need to trust information based on the source of the information in order to function correctly, causing the application to become insecure if the information is corrupt.

Countermeasures:
- Ensure that only trusted sources are used, which cannot be compromised or imitated
- Ensure that applications have the ability to verify the source of information
- Ensure that applications have the ability to verify that the level of trust extended to that source is appropriate

Attack 4: *Unnecessary Ports and Services*; an attacker can exploit an application which opens ports which are not used by the application, but could be exploited by the attacker

Countermeasures:
- Scan the application to ensure that it does not attempt to use ports or services that are not necessary for the application’s functionality

Attack 5: *Using Loops with User Input, Script or Code*; an attacker can exploit an application which allows direct user input by executing that input repetitively, causing the application to become deadlocked

Countermeasures:
- Ensure that direct user input should not be able to use constructs such as loops to cause denial of service or other lack of availability situations

Attack 6: *Using Alternative Routes of Task Execution*; an attacker can exploit an application which allows the same task to be executed in more than one way, allowing a route that circumvents security controls to be utilized

Countermeasures:
- Each execution path should implement an appropriate security control

Attack 7: *Forcing the System to Reset Values*; an attacker can exploit an application which allows users to leave the fields in an online input form blank, and then choose *Finish* instead of *Next*; forcing the application to provide initialized variables values where they have not been input, leading to default values and configurations leaving the application in an insecure state
Countermeasures:
- Assign a value to a variable as soon as it is declared
- Ensure that all variables are initialized before being used by the application
- Avoid assigning default values and configurations to any variables

Attack 8: *Get between Time of Check Out and Time of Use*; an attacker may be able to infiltrate a transaction if too much time elapses between the time the information is checked out by the application and the time it is used, resulting in the attacker being able to force the application to perform some unauthorized action.

Countermeasures:
- Ensure that the time delay between check out and use is minimized
- Ensure that every time sensitive operations are performed, checks are made to guarantee that they will succeed securely

Attack 9: *Create Files with Same Name as Files Protected with a Higher Level of Classification*; an attacker can exploit an application that assigns special privileges to certain files, such as Dynamic Link Libraries, based on their location, resulting in an attack which takes advantage of execution or privilege decisions based on filename.

Countermeasures:
- Ensure controls on privileged locations prevent writing or modifying to those locations by unauthorized applications
- Ensure that files are verified using more than filename and location alone

Attack 10: *Force the Application to Display All Error Messages*; an attacker can use the information an application provides in error messages used to alert users of improper or disallowed actions, in order to discover a situation where no error message is displayed (meaning the error is not handled correctly) and the where the application attempts to process the bad value.

Countermeasures:
- Use pre-tested code to ensure that all parameters are validated before they are used.
- Parameters should be validated against a positive specification that defines:
  - Data type (string, integer, and so on)
  - Allowed character set
  - Minimum and maximum length
  - Whether null is allowed
  - Whether the parameter is required or not
• Whether duplicates are allowed
• Numeric range
• Specific legal ranges (enumeration)
• Specific patterns (regular expressions)

Attack11: Look for Temporary Files and Screen the File Contents for Protected Information; an attacker can exploit applications routinely write information to temporary files, in order to gain insecure access to that information

Countermeasures:
- Ensure that the mechanisms for storing this information are secure
- Ensure that the mechanisms for accessing this information are secure
- Understand when, where, how the application accesses file-system information
- Identify which information should not be exposed to other potential users of the system
- Find creative ways to gain insecure access to the protected information

Attack12: Passing Credentials; an attacker can exploit web service messages (such as XML) which convert the credentials to text format prior to being sent, resulting in the attacker gaining access to a clear text version of the credentials

Countermeasures:
- Encrypt all protected information such as passwords and private keys

Attack13: Broken Authentication and Session Management; an attacker can make use of a session token that is not properly protected to hijack a session and assume the identity of the user

Countermeasures:
- Use a credential management scheme which consistently enforces the security standard, paying special attention to:
  • Password strength (minimum size and complexity)
  • Password use (defined number of allowable login attempts per unit time)
  • Password change controls (uniformly use the same mechanism to change the password)
  • Password storage (should be stored in hashed or encrypted form for protection)
  • Protecting credentials in transit (encrypt the entire login transaction with a secure protocol as such as SSL)
• Session ID protection (encrypt the entire user session with a secure protocol as such as SSL)

• Account lists (avoid allowing users to gain access to a list of account names on site; if necessary display a pseudonym list that maps to the real list instead)

• Browser caching (authentication pages should be marked with a no cache tag to prevent someone from using the back button in a user’s browser to access the login page and resubmit the credentials)

• Trust relationships (avoid implicit trust between components whenever possible; each component should have to authenticate itself to the other component)

**Attack14:**  *Cross site scripting (XSS) flaw;* an attacker can cause a web application to send malicious code (generally in the form of a script) to be executed through a victim’s browser

*Countermeasures:*

- Input filtering: properly sanitize user input information by validating all headers, cookies, query strings, form fields and hidden fields
- Output filtering: filter and properly sanitize user information when it is sent back to the user’s browser
- Use of firewall: use third party application firewall which intercepts and blocks cross site script before it reaches the web server or vulnerable scripts
- Disable client side scripting: The best protection is to disable scripting when it is not required
- Use signed scripting: use signed scripting such that any script with an invalid or untrusted signature will not be run automatically

**Attack15:**  *Buffer overflows;* an attacker can send crafted input to a web application, causing it to execute arbitrary code which corrupts the execution stack, allowing the attacker to take over the system

*Countermeasures:*

- Apply the latest security patches to the web application
- Periodically scan the web code looking for buffer overflow flaws in the web server or application
- Properly sanitize user input information by validating all headers, cookies, query strings, form fields and hidden fields
**Attack16:** Injection flaws: an attacker can relay malicious code through one web application to another

*Countermeasures:*
- Avoid using external operating system shell commands to pass function calls, relying instead on internal language specific libraries to do the same function
- For calls to backend databases, carefully validate the information provided to ensure it does not contain any malicious content

**Attack17:** Insecure storage: an attacker can take advantage of an application’s need to store protected information by locating insecurely stored information

*Countermeasures:*
- Encrypt all critical information
- Encrypt all keys, certificates and passwords
- Encrypt all secrets in memory
- Choose strong algorithms
- Use proven encryption algorithms
- Provide supporting mechanisms for encryption key changes, and so on
- Whenever reasonable, rather than store protected information in an encrypted form, force the user to re-enter the information

**Attack18:** Denial of service; an attacker can use a web application’s inability to tell the difference between valid traffic and traffic generated for an attack, to force the web application to attempt to handle excessive numbers of concurrent users or traffic volumes, causing the web application to cease functioning in a normal manner

*Countermeasures:*
- Establish quotas to limit the amount of load a given user can generate
- Handle one request per user at a time by synchronizing on the user’s session
- Drop any requests currently being processed for a user when another request from that user arrives
- Check the error handling scheme to ensure an error cannot affect the overall operation of the application

**Attack19:** Insecure configuration management: an attacker can use improper system configuration to exploit the web application

*Countermeasures:*
- Patch all security flaws in the server software
- Configure the application software to limit directory listing or directory traversal
Remove unnecessary default, backup or sample files; including scripts, applications, configuration files and web pages
Correctly configure file and directory permissions
Correctly configure user, group and role permissions
Disable unnecessary services, including content management and remote administration
Change default passwords on default accounts
Disable unnecessary administrative or debugging functionality
Correctly configure SSL certificates and encryption settings
Use signed certificates for authentication
Ensure proper authentication with external systems

Attack20: Identifying the web server vendor and version by banner grabbing; an attacker may use the disclosure of unnecessary information in the web server banner to attempt to gain access to the web server

Countermeasures:
- If possible, change the server tag in response header.

Attack21: Identifying the web server vendor and version by using default files; an attacker may use the normal behavior of the server to expose default directories, file extensions, and pages in the default installation

Countermeasures:
- Set permissions to prevent access on default pages of the server.

Attack22: Identifying the web server vendor and version by identifying the modules running on the web server; An attacker may use the response header to identify the modules running, which in turn will identify the operating system and which modules can be exploited

Countermeasures:
- Change the server tag

Attack23: Product specific issues; an attacker can use knowledge of the modules running on the web server to get access to the remote machine

Countermeasures:
- Patch the web server and web applications regularly
Appendix J: Backups and Backup Strategies

IT managers need to plan for backups in terms of time and space required. However, most modern backup software can compress the backup files to reduce both the time required to backup, as well as the media size needed.

Regardless of the backup software or hardware that is chosen, the backup itself can come in three different methods; full, incremental or differential.

A full backup:

- Is often the starting point for all other backups
- Most comprehensive and are self-contained backup
- Takes a long time to run
- Takes a considerable amount of backup media to accomplish
- A restore from a full backup is much quicker
- Running a full backup on a regular basis to restart the incremental and differential method will help reduce the time and media size needed
- Often delegated to a weekly or monthly schedule.

An incremental backup:

- Stores all files that have changed since the last full, differential or incremental backup
- Provides a faster method of backing up information than repeatedly running full backups
- Takes the shortest amount of time to complete the backup
- Takes the least amount of backup media to accomplish
- The effort to restore from an incremental backup can be very time consuming, as multiple tapes are restored.

When restoring from incremental backup, the most recent full backup is needed, as well as every incremental backup that was made since the last full backup. For example, if a full backup was done on Friday and incremental backups on Monday, Tuesday and Wednesday, and the backed-up machine crashes Thursday morning; all four backup media would be needed; Friday's full backup plus the incremental backup for Monday, Tuesday and Wednesday.

A differential backup:

- Contains all files that have changed since the last full backup
- Shortens overall restore time compared to a full backup with incremental backups
- The upside for using full and differential backups is that only two backup media are needed to perform a complete restore.
Restoring a differential backup is a faster process than restoring several incremental backup. For example, if a full backup was done on Friday and differential backups on Monday, Tuesday and Wednesday, and the backed-up machine crashes Thursday morning only two backup media days would be needed; Friday's full backup plus Wednesday's differential backups; that is, the latest full backup and the latest differential.

The difference between these three backup strategies is illustrated in Figure 1: Comparing Backup Strategies. Here, the full backup backs up everything up each time it is run as illustrated by the first row on the diagram.

The incremental backup backs up only new or changed items from the previous incremental backup (with a full backup starting the process). This is illustrated by the second row on the diagram.

A differential backup backs up all new or changed items from the last time a full backup was run, as illustrated by the third row of the diagram.
Figure 1: Comparing Backup Strategies
Sample Backup Strategies

The following information is presented as best practices guidelines only. All backup routines should balance time, expense and effort against risk. Each department should develop a strategy that is appropriate to their specific requirements. However, some ideas for developing a backup strategy include:

- Develop a written backup plan that identifies:
  - What is being backed up
  - Where it is being backed up to
  - How often backups are performed
  - What is the life of the backup media
  - Who is in charge of performing backups
  - Who is in charge of backup verifications; completion of jobs and testing of media
  - Schedules of test restores

- Database and accounting files are critical information assets and should be backed up before and after any significant amount of information entry and/or use. For most departments, this means backing these files up every day.

- Virus or spyware quarantine directories should be excluded from backups.

- Work related documents and files (for example, the "My Documents" folders) and email files/folders might be backed up once a week. This frequency should reflect the level of criticality that the department associates with the information.

- Copies of backups should be stored off-site to ensure recovery against disaster such as a fire, earthquake or flood. Users typically require restoration of files recently backed up. So, one recommendation is to keep the most current set of backups onsite and send the rest of the backups offsite.

- It is not usually necessary to backup the complete contents of each hard drive. Most of that space is taken up the operating system and program files, which can be easily reloaded from CD or images. The only exception is if the department has a dedicated file server; it's a good practice to do a full backup.

- The backup plan also needs a strategy to backup laptops and mobile devices which may not be available at regular or convenient times.

- Backups should be tested BEFORE they are needed. To ensure confidence in the backups, the backup software should allow for full read-back verification. Additionally, it is a good practice to try restoring a few files on each set of full, incremental and differential backups.

---

49 Backups kept onsite should be stored in a fire proof safe for media protection.
Choosing appropriate backup hardware is also key to the success of the backup plan. Considerations include:

- Determine how much information you need to backup. Inventory each machine on the network (or a representative sample) to determine the total backup space.
- Be sure to leave room to add a new staff information and to plan for growth.
- Choose a backup device that uses tape cartridges with a capacity that is at least twice the total amount of information you need to backup.

**Sample Media Rotation Strategies**

In combination with a backup method strategy, it is recommended that IT support staff also use a backup tape (or other media of choice) rotation strategy. This will prevent the same media being used repeatedly, and so risking data loss.
The Parent-Child Tape Backup Strategy

<table>
<thead>
<tr>
<th>Day</th>
<th>Tape</th>
<th>Backup Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Friday</td>
<td>Tape 1</td>
<td>Full Backup</td>
</tr>
<tr>
<td>Monday</td>
<td>Tape 2</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Tuesday</td>
<td>Tape 3</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Wednesday</td>
<td>Tape 4</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Thursday</td>
<td>Tape 5</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Friday</td>
<td>Tape 6</td>
<td>Full Backup</td>
</tr>
<tr>
<td>Monday</td>
<td>Tape 2</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Tuesday</td>
<td>Tape 3</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Wednesday</td>
<td>Tape 4</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Thursday</td>
<td>Tape 5</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Friday</td>
<td>Tape 7</td>
<td>Full Backup</td>
</tr>
<tr>
<td>Monday</td>
<td>Tape 2</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Tuesday</td>
<td>Tape 3</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Wednesday</td>
<td>Tape 4</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Thursday</td>
<td>Tape 5</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Friday</td>
<td>Tape 8</td>
<td>Full Backup</td>
</tr>
<tr>
<td>Monday</td>
<td>Tape 2</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Tuesday</td>
<td>Tape 3</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Wednesday</td>
<td>Tape 4</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Thursday</td>
<td>Tape 5</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Friday</td>
<td>Tape 9</td>
<td>Full Backup</td>
</tr>
<tr>
<td>Monday</td>
<td>Tape 2</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Tuesday</td>
<td>Tape 3</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Wednesday</td>
<td>Tape 4</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Thursday</td>
<td>Tape 5</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Friday</td>
<td>Tape 10</td>
<td>Full Backup</td>
</tr>
<tr>
<td>Monday</td>
<td>Tape 2</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Tuesday</td>
<td>Tape 3</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Wednesday</td>
<td>Tape 4</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Thursday</td>
<td>Tape 5</td>
<td>Differential Backup</td>
</tr>
</tbody>
</table>

**Figure 2: The Parent-Child Tape Backup Strategy**

The *Parent-Child Tape Backup Strategy* is an example of a 10 tape rotation strategy, which uses four tapes during the week and the others each consecutive Friday. The strategy starts on a Friday with a full system backup on Tape 1. The following Monday, Tape 2 is used to perform a differential backup (targeting the data that has changed since Friday’s full system backup). On Tuesday, Tape 3 is used to perform a differential backup (again targeting the data that has changed since Friday’s full system backup). Tapes 4 and 5 are used in the same manner for Wednesday and Thursday respectively.
In this strategy, the week day tapes are referred to as daily backups, since using the differential backups; only the last full backup and last daily backup will need to be used to completely restore a system.

Finally, IT support staff should also use an archival or monthly backup strategy. An example of this would be the Grand Parent-Parent-Child Tape Backup Strategy. This is an example of a 22 tape rotation strategy, which builds directly on top of the Parent-Child Tape Backup Strategy in that it uses a sub-set of 10 tapes; four tapes during the week and the others each consecutive Friday.

However, there are 12 additional tapes which are used for monthly full backups. These 12 tapes will be kept indefinitely, will not be reused, and should be stored at an appropriate off-site location.

Figure 4 illustrates the Grand Parent-Parent-Child Tape Backup Strategy. This is very similar to the Parent-Child Tape Backup Strategy illustrated in Figure 2. However, each fourth Friday, a monthly full backup is performed instead of the weekly full backup. As per Figure 3, at the end of the first month, Tape 11 is used. Then at the end of the second month, Tape 12 is used, and so on.

<table>
<thead>
<tr>
<th>Month</th>
<th>Tape</th>
</tr>
</thead>
<tbody>
<tr>
<td>Month 1</td>
<td>Tape 11</td>
</tr>
<tr>
<td>Month 2</td>
<td>Tape 12</td>
</tr>
<tr>
<td>Month 3</td>
<td>Tape 13</td>
</tr>
<tr>
<td>Month 4</td>
<td>Tape 14</td>
</tr>
<tr>
<td>Month 5</td>
<td>Tape 15</td>
</tr>
<tr>
<td>Month 6</td>
<td>Tape 16</td>
</tr>
<tr>
<td>Month 7</td>
<td>Tape 17</td>
</tr>
<tr>
<td>Month 8</td>
<td>Tape 18</td>
</tr>
<tr>
<td>Month 9</td>
<td>Tape 19</td>
</tr>
<tr>
<td>Month 10</td>
<td>Tape 20</td>
</tr>
<tr>
<td>Month 11</td>
<td>Tape 21</td>
</tr>
<tr>
<td>Month 12</td>
<td>Tape 22</td>
</tr>
</tbody>
</table>

**Figure 3: Tape Usage in the Grand Parent-Parent-Child Tape Backup Strategy**
The Grand Parent-Parent-Child Tape Backup Strategy

<table>
<thead>
<tr>
<th>Day</th>
<th>Tape</th>
<th>Backup Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Friday</td>
<td>Tape 1</td>
<td>Full Backup</td>
</tr>
<tr>
<td>Monday</td>
<td>Tape 2</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Tuesday</td>
<td>Tape 3</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Wednesday</td>
<td>Tape 4</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Thursday</td>
<td>Tape 5</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Friday</td>
<td>Tape 6</td>
<td>Full Backup</td>
</tr>
<tr>
<td>Monday</td>
<td>Tape 2</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Tuesday</td>
<td>Tape 3</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Wednesday</td>
<td>Tape 4</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Thursday</td>
<td>Tape 5</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Friday</td>
<td>Tape 7</td>
<td>Full Backup</td>
</tr>
<tr>
<td>Monday</td>
<td>Tape 2</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Tuesday</td>
<td>Tape 3</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Wednesday</td>
<td>Tape 4</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Thursday</td>
<td>Tape 5</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Friday</td>
<td>Tape 8</td>
<td>Full Backup</td>
</tr>
<tr>
<td>Monday</td>
<td>Tape 2</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Tuesday</td>
<td>Tape 3</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Wednesday</td>
<td>Tape 4</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Thursday</td>
<td>Tape 5</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Friday</td>
<td>Tape 9</td>
<td>Full Backup</td>
</tr>
<tr>
<td>Monday</td>
<td>Tape 2</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Tuesday</td>
<td>Tape 3</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Wednesday</td>
<td>Tape 4</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Thursday</td>
<td>Tape 5</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Friday</td>
<td>Tape 10</td>
<td>Full Backup</td>
</tr>
<tr>
<td>Monday</td>
<td>Tape 2</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Tuesday</td>
<td>Tape 3</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Wednesday</td>
<td>Tape 4</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Thursday</td>
<td>Tape 5</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Friday</td>
<td>Tape 11</td>
<td>Monthly Full Backup</td>
</tr>
<tr>
<td>Monday</td>
<td>Tape 2</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Tuesday</td>
<td>Tape 3</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Wednesday</td>
<td>Tape 4</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Thursday</td>
<td>Tape 5</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Friday</td>
<td>Tape 12</td>
<td>Monthly Full Backup</td>
</tr>
<tr>
<td>Monday</td>
<td>Tape 2</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Tuesday</td>
<td>Tape 3</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Wednesday</td>
<td>Tape 4</td>
<td>Differential Backup</td>
</tr>
<tr>
<td>Thursday</td>
<td>Tape 5</td>
<td>Differential Backup</td>
</tr>
</tbody>
</table>

Figure 4: The Grand Parent-Parent-Child Tape Backup Strategy
Appendix K: Encryption

Encryption/Hash

Encryption is the process of protecting information by obscuring it in such a way that it cannot be read, accessed or modified without special knowledge and/or a special token.

In many cases it is desirable that nobody can see the information as it travels the network or is stored on a computer locally. This may apply to the entire message being processed, or only to certain parts of it; in either case, some type of encryption is required to conceal the content.

When a computer receives information, it might be necessary to confirm if the sender created the information, or if the information was modified. Such confirmation may be achieved using encryption with a shared secret key.

File and Disk Encryption

File system encryption refers to encrypting selected files and directories on a hard drive. File system encryption does not usually involve encrypting the system files. As such, file system encryption does not protect the host operating system itself, which may then be open to attempted compromises such as brute force password guessing. File system encryption is suitable for use on desktops and servers to protect selected information.

Disk encryption (or full disk encryption) can be done at a hardware or software level, and encrypts the operating system, the swap file, the temporary files, and all information files and directories. In this way, the threat of compromise via operating system exploitation (as with file system encryption) is avoided. Additionally, full disk encryption supports pre-boot authentication. Due to these reasons, full disk encryption is suitable for portable devices such as laptops.

Supporting Encryption/Hash

Encryption is done using either shared key (also known as symmetric) or private/public key (also known as asymmetric) encryption. Normally, shared key encryption algorithms are used to encrypt bulk information, since they are significantly faster than the private/public keys. Private/public key encryption is commonly applied to protect the shared session keys, which, in many implementations, are valid for one communication only and are subsequently discarded. An example of private/public key encryption would be using a secure protocol, such as HTTPS, for a web based transaction on the Internet.

The usual mechanism to protect information tampering is by hash. An example of this is password encryption; which ensures that a password never gets passed in a readable format. Instead, the password is encrypted by a hashing algorithm as it is entered by the user. The hash
value generated by this encryption process is then compared with the hash value of stored password, and if the two hash values match, the entered password is accepted.

**Key Management**

IT support staff need to understand how these processes work in order to ensure that they are implemented correctly. Regardless of the type of encryption that is being used, a critical issue is that of key management. The compromising of a secret key will lead to the compromising of all information encrypted with the key. The longer a secret key is used, the more exposure it receives, and the greater the chance that it may be compromised. So, for keys that are used to encrypt protected information, the length of key life should be short (no more than 90 days or a semester).

Other critical factors in the key management process include mechanisms by which keys are generated, escrowed, updated, shared, revoked, and destroyed. The use of key management technologies such as Kerberos or Public Key Infrastructure (PKI) can assist with these issues.

Given that the key management process is complicated and may require exhaustive co-ordination with IT support staff, the use of encryption is not suitable for every application. For instance, in database systems, where the configuration of the key management factors can be controlled (either manually or automatically), then encryption is viable since IT support staff can choose the appropriate level of encryption for each of the data elements in the database table.

In email systems, the use of encryption is viable in some instances, but not in others. For example, IT support staff can control the key on the email server, and University desktops or laptop client systems under their control, in which case, encryption is viable. But IT support staff have no control over email clients outside of the University that may also receive the email message, in which case, encryption is not a viable solution.

**Requirements for Strong Encryption of Protected Information**

As a good rule of thumb, protected information should use the following FIPS-approved cryptographic algorithms:

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Type</th>
<th>Key Sizes (bits)</th>
<th>FIPS Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>Symmetric</td>
<td>128, 192, 256</td>
<td>FIPS 197</td>
</tr>
<tr>
<td>3DES</td>
<td>Symmetric</td>
<td>168</td>
<td>FIPS 46-3 &amp; 81</td>
</tr>
<tr>
<td>DSA</td>
<td>Asymmetric</td>
<td>1024</td>
<td>FIPS 186-2</td>
</tr>
<tr>
<td>RSA</td>
<td>Asymmetric</td>
<td>1024 or higher (2048 rec.)</td>
<td>FIPS 186-2</td>
</tr>
<tr>
<td>ECDSA</td>
<td>Asymmetric</td>
<td>160 or higher</td>
<td>FIPS 186-2</td>
</tr>
<tr>
<td>SHA</td>
<td>Hashing</td>
<td>160 (SHA-1), 224, 256, 384</td>
<td>FIPS 180-2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>512</td>
<td></td>
</tr>
</tbody>
</table>
Appendix L: Data Center Physical Security

This appendix outlines the additional physical and environmental security controls, which would be excessive for most server rooms, but are appropriate for data centers. All physical and environmental security controls listed in Section 3.11 apply as baseline requirements for data centers; and then the following controls should be used to augment this baseline set of controls.

Physical Access to the Data Center

Physical access to the data center should be controlled, starting outside the entrance. The area around the data center should be considered a restricted access area. IT managers should ensure that personnel who are authorized to access a restricted access area should carry easily recognizable identifiers, such as badges. Visiting personnel (such as service personnel or contactors) should be escorted at all times, and should sign-in and sign-out in a secure log.

The data center walls and ceilings should be constructed using material with an appropriate fire rating. Walls should be reinforced in areas around doors and windows, and should extend from the floor to the structural ceiling such that there is no space for an intruder to climb over the partition. The ceiling should be sufficiently waterproof as to prevent leakage from an upper floor. The data center floor should be raised, and should be constructed using material with a two hour fire rating. The floor should be electrically grounded, and utilize a non-conducting material.

For mission critical servers, a sign-in/sign-out key access log may be used. Power outlets, UPS’s, keyboards and mice, console screens, KVM switches, and so on should also be protected within the lockable cage. Additionally, on mission critical servers, floppy/CD/DVD/USB drives should be disabled, removed or require authentication for use.

Perimeter security should include the use of cameras for monitoring, and heat sensitive alarms for alerts when temperatures are unsafe for computers.

Electrical Systems

Due to the high electrical use requirements, data centers should install power line monitors to detect changes in frequency and voltage amplitude, and electrical line filters to filter voltage spikes. Proper grounding for all electrical devices is necessary to protect against short circuits and static electricity. IT managers are responsible for ensuring that an appropriate load is assigned to each power outlet (if in doubt, Physical Plant should be consulted). Additionally, a backup power source or generator should be used to protect against long duration power failures.
Appendix M: Recommended Sources of Security Training

SDSU campus training may include:

- SDSU IT Security meetings/mailing list
- IT Manager meetings/ mailing list
- Instructional Academic Computing Committee (IACC)
- Senate IIT meetings
- Minimum Workstation and Software Site License Sub-committee (MWSSLS) meetings/ mailing list
- System Administrator (Sysadmins) meetings/ mailing list

Recommended conferences, 1 day seminars, or courses may include:

- EDUCAUSE conferences
- SANS or USENIX courses
- Courses offered at Vortex, New Horizons, or other local providers
- Local Information Systems Security Association (ISSA) meetings
- CSU Secure IT
- Vendor technical conferences
- Topic specific conferences on or off campus

Recommended books and email lists may include:

- General security books
- Technology specific books
- Strategic or general security magazines
- Security mailing lists
- Local city and county meetings
Appendix N: Memorandum from President Weber

February 26, 2007

MEMORANDUM

TO: SDSU Faculty and Staff
FROM: Stephen L. Weber, President
Re: Computing Resources

I am writing to ensure that we all have a clear understanding of the obligation we and San Diego State University have to protect our computing resources, including confidential information. Let me summarize the activities that have been and will be undertaken to meet those obligations, and the consequences should an individual or department fail to meet those obligations.

Multiple federal and state laws, as well as policies of the California State University, require that confidential or personal information be protected. The definition of what is information to be protected varies by the particular law or policy, but this generally includes records that pertain to personal identity, financial or health information, and/or student grades and similar data. Examples include: Social Security numbers, grades, dates of birth, patient medical records, and driver’s license and credit card information. In addition to imposed legal and policy obligations, we also have a fiduciary duty to protect the information entrusted to us by our colleagues, our students, our alumni, and others of our campus community. Most of all, it is the right thing to do.

There is no single technology that can protect information. The only effective approach involves multiple layers of protective action, aided by technology. Security practices are being incorporated into a comprehensive campus information security plan.

As university employees, we all share in the responsibility to be familiar with, and abide by, existing campus policies and procedures concerning information security. These can be found at http://security.sdsu.edu/policy/. References to applicable federal and state laws can be found at the same site, including appropriate use of state resources.

We are each responsible to securely manage and use technology, including desktop or portable computers, servers, wireless devices, or portable storage media such as flash drives. Secure management means availing ourselves of the technical direction of departmental IT staff to ensure that machines are always secured with the latest patches and protective software. Secure use of technology requires that employees are aware of risks inherent with computing in a shared environment, including Internet browsing and email communications. Adherence to SDSU’s Computing Acceptable Use Policy http://security.sdsu.edu/policy/aup.html reduces exposure to these risks.
In furtherance of our continuing efforts to maximize good security practices, a number of actions are underway:

- **Completion of the detailed campus information security plan**, which is a manual for management and technical IT support staff across campus. The first completed section of the plan, concentrating on how to respond to a security incident, can be found at [http://security.sdsu.edu/policy/SIRP.pdf](http://security.sdsu.edu/policy/SIRP.pdf). Other sections include the Vulnerability Management Program, the Security Awareness and Training Program, and the Disaster Recovery and Business Continuity Program, which we expect to complete by July 2007.

- **Completion of the network infrastructure build-out**, scheduled for April 2007. Concurrent with this build-out, unauthorized routers and hubs will be removed from the network while providing improved service to our campus community.

- **Enhancement of our network protection system** that will only allow pre-approved traffic to access our computing resources. This will greatly reduce the possibility of unauthorized access to our systems, reducing the risk of possible damage to our resources or access to valuable and confidential information. The first phase will be the installation of additional network firewalls in February 2007. This will be followed in the spring with additional hardware and software systems in support of the California State University Chancellor’s Office security improvement project.

- **An increase in network and system scans, surveys, and other activities** to assess the campus’s vulnerability to security attacks and to identify mitigating measures.

It is essential that each of us cooperate with the Information Technology Security Office and other University IT staff assigned to manage and secure the network, systems, and information. Because we all share the same network, violations of policy and good practice by one individual endanger all of us, including those individuals whose confidential information is entrusted to us. Failure to follow policies and/or violation of applicable laws involves consequences that range from loss of connection to the campus network and disciplinary proceedings, to possible criminal or civil actions and the requirement for the relevant campus department and division to bear the costs associated with security breach.

In summary, no part of our fast-changing world is moving more quickly than information technology. To give you a sense of the realities we face, we are now averaging over one million attempts per hour to probe and attack our systems. We each share the same professional responsibility in managing our students’ information as well as in caring for our own information.

SLW/jnt
Appendix O: Process for Retaining Computing Systems or Storage Drives

During an incident investigation it may be necessary for the IT Security Office to retain computing systems or storage drives for forensic investigation. This hardware retention may be needed to:

- confirm protected information was not accessed,
- help scope the incident,
- retain evidence that might needed for law enforcement investigation,
- gather information for the notification process,
- analyze details about the incident.

Since the retention of hardware may negatively impact the affected department, it is the last resort towards satisfying the incident needs. The determination of whether or not hardware must be retained is made by the TSO. The TSO will contact the IT manager responsible for oversight of the hardware to coordinate pick up. Depending on the urgency of the incident, and availability of the direct manager, the TSO may coordinate the pick up details with other line management.

The TSO will coordinate:

- the approximate pick up time,
- the name of the individual from the IT Security Office who will physically pick up the equipment, and
- who to contact at the department where the hardware is located.

The IT Security Office employee picking up the equipment will present their SDSU ID card to the department point of contact and fill out the SDSU IT Security Office Equipment Receipt form. Both the IT Security Office employee and manger will sign the form. A copy of the form will be left with the manager and another copy placed in the IT Security Office incident file. Figure P-1 illustrates the equipment receipt used by the IT Security Office for hardware retention.

Once the hardware has been retained, the manager should prepare for resumption of duties without the hardware, as it may not be returned for several weeks or months. The TSO will keep the manager apprised of the hardware status until it is returned, or permanently stored to respond to anticipated legal actions.
## SDSU IT Security Office Equipment Receipt Form

**Date:**

**Time:**

**Department:**

**Equipment Removed:**

**Comments:**

**ITSO Employee Printed Name:**

**ITSO Employee SDSU Card #:**

**ITSO Employee Signature:**

**Manager Printed Name:**

**Manager Signature:**

**Receipt Number:**

For updated information on this incident please email security@sdsu.edu or call (619) 594-0142

**USE THIS RECEIPT NUMBER AS A REFERENCE**

For further information and IT Security Office policies, please see [http://security.sdsu.edu](http://security.sdsu.edu)

---

**Figure P-1: Equipment receipt used by the IT Security Office for hardware retention**
Appendix P: References

ACT Security Policy, University of California, San Diego

Application Security by Design, Security Innovation, February 2006,

Auditing Web Site Authentication, Security Focus, April 2003,
http://www.securityfocus.com/infocus/1688

Brown University, Administrative Information Systems Information and Data Security Manual

(CATCH) San Diego, Riverside, and Imperial Counties High Tech Crimes Task Force,
www.catchteam.org


Computer Analysis Response Team FBI Laboratory, http://www.fbi.gov/

Computing and Communications Services Security Guide, San Francisco State University

Computer and Network Use Policy, Keene State College

Computing Ethics and Security, San Francisco State University

Computer Use Policy, University of California, Berkeley

Computer Security Policy, Texas A&M University

Computer Security Resource Center, National Institute of Standards and Technology,
http://csrc.nist.gov/index.html (NIST SP 800-61 ) NIST SP 800-3

Creating a Patch and Vulnerability Management Program (NIST SP 800-40), Computer Security Resource Center, National Institute of Standards and Technology,

Developing an Effective Incident Cost Analysis Mechanism, [http://online.securityfocus.com/infocus/1592](http://online.securityfocus.com/infocus/1592)


EDUCAUSE web site


Electronic Frontier Foundation web site

Electronic Mail Policy, University of California, Office of the President


General Catalog, 1999-2000, San Diego State University

Guidelines for Administering Appropriate Use of Campus Computing and Network Services, University of California, Berkeley


HTCIA San Diego Chapter, [www.htcia-sd.org](http://www.htcia-sd.org)

Humboldt State University, Appropriate Use Policy


Information Technology Resources and Internet Access -- Guidelines for Use, Princeton University
Information Technology Services: Appropriate Use Policy, Yale University

InfraGard, www.infragard.net

International Association of Computer Forensics Specialists, www.cops.org


National Infrastructure Protection Center,
http://www.calea.org/Online/newsletter/No75/The%20National%20Infrastructure%20Protection%20Center.htm

Network Security at UCSD, University of California, San Diego

Policy on Use of Computing and Communications Technology, California State University, Chico

Policy for Responsible Computing, University of Delaware

Regional Computer Forensic Laboratory at San Diego, http://www.rcfl.org

Rules for Responsible Computing, Texas A&M University

SANS Institute, SANS Top-20 Internet Security Attack Targets (2006 Annual Update),
http://www.sans.org/top20/


VirusScan Enterprise 8.0i Best Practices Guide, McAfee Security, August 2004,  

Web Application Break-In, Information Security Magazine, August 2006,  
http://informationsecurity.techtarget.com/magLogin/1,291245,sid42_gci1206289,00.html

Web Application Security, Information Systems Control Journal, November 2002,  
http://www.isaca.org/Template.cfm?Section=Archives&CONTENTID=16173&TEMPLATE=/ContentManagement/ContentDisplay.cfm

Why is security important for NPACI sites and users?, San Diego Supercomputer Center
## Appendix Q: Version Review Log

<table>
<thead>
<tr>
<th>Version</th>
<th>Date Completed</th>
<th>Reviewed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1.0</td>
<td>October 26th 2007</td>
<td>ISO and ISP</td>
</tr>
<tr>
<td>Version 1.1</td>
<td>November 28th 2007</td>
<td>CIO and IT Security Office</td>
</tr>
<tr>
<td>Version 1.2</td>
<td>November 30th 2007</td>
<td>AA IT Coordinator, SA IS Manager, Senate IIT Committee Chair, IT Support Expert, Auxillaries, IT Managers, IT Security, IACC, Senate IIT, MWSSLS, System Administrators</td>
</tr>
<tr>
<td>Version 1.3</td>
<td>December 21st 2007</td>
<td>President's Cabinet</td>
</tr>
</tbody>
</table>