Executive Summary

Information security is the collective responsibility of all members of the SDSU community. In the furtherance of developing, and maintaining, adequate information technology security the university has established a comprehensive plan. This plan consists of four programs:

- ❑ The Information Technology Security Incident Response Program
- ❑ The Security Awareness Program
- ❑ **The Vulnerability Management Program**
- ❑ The Disaster Recovery Program

One of the key components of the Information Security Plan is the Vulnerability Management Plan (VMP). The VMP has been defined as a program to provide those individuals responsible for oversight of computing resources (IT managers) as well as IT support staff guidance on complying with SDSU security requirements. 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).

The Vulnerability Management Program defines:

- ❑ A standard for classifying information
- ❑ Standards for protecting systems, applications, and accounts
- ❑ Information security protections and access procedures
- ❑ Mobile device security protections
- ❑ Physical security protections
- ❑ Network security protections and access procedures
- ❑ A self-assessment process for IT managers
- ❑ The IT Security Office assessment process

All IT managers are responsible for ensuring that IT support staff apply the minimum protections described in this program and for ensuring that the minimum procedures for protecting information are followed.

Information technology security is a risk management discipline. This program provides information in order for IT managers and support staff to effectively contend with the threats and vulnerabilities to systems, networks, and information entrusted to the university. Although this document provides a central resource and framework for vulnerability management, the evolution of technology and the threat environment is so dynamic, it is the responsibility of IT managers to stay current through campus training and announcements from the IT Managers meeting, the IT Security mailing list, the Senate Instructional and Information Technology Sub-Committee, SDSUniverse, and the Daily Aztec. In addition, IT managers should receive trends and reports directly from Educause and vendors whose products are implemented in their areas of operations.

Table of Contents

Executive Summary 1
2.0 Introduction 6
2.1 Information Classification Standard 6
2.1.1 Protected Information Levels 6
2.1.1.1 Protected Level 1 7
2.1.1.2 Protected Level 2 7
2.1.1.3 Protected Level 3 8
2.1.2 SDSU Confidential Authorization Access Approval 10
2.2 Desktop Security 13
2.2.1 Patch Management 13
2.2.1.1 Patch Planning 14
2.2.1.2 Patch Implementation 15
2.2.1.3 Patch Compliance Reporting 16
2.2.2 Anti-Virus and Anti-Spyware Management 17
2.2.2.1 Anti-Virus (AV) 17
2.2.2.2 Anti-Spyware (AS) 18
2.2.3 Standard Hardware and Software Configurations 20
2.2.4 Authorized Software 20
2.2.5 Centralized Desktop Management Software 21
2.3 Laptop and Mobile Device Security 22
2.3.1 Laptop and Mobile Device Security 22
2.3.2 Mobile Data Device Security 23
2.4 Server Security 23
2.4.1 Server System Builds 24
2.4.2 Patch Management on Servers 24
2.4.3 Configuration of Services on Servers 24
2.4.4 Malware Content in Email 25
2.5 Change Management 25
2.5.1 Change Management of Documentation 26
2.5.2 Change Management of Information Systems 26
2.6 Account Management 28
2.6.1 Account Creation and Maintenance 28
2.6.1.1 Creating and Assigning Accounts 29
2.6.1.2 Accessing another User’s Account 30
2.6.1.3 Disabling, Reassigning or Deleting Accounts 31
2.6.2 Account Usage 31
2.6.3 Password Selection 33
2.7 Application Security 35
2.7.1 Application Security in the System Development Cycle 36
2.7.2 Application Security in Commercial or Legacy Systems 38
2.8 Remote Access Security 39
2.8.1 Securing the Remote Computer 39
2.8.2 Remote Access to Secure Web and Messaging Applications 40

2.8.3 Remote Programmatic, Management, and File Transfer Access to Computing Resources 40
2.8.4 Network Access to Level 1 Information or Critical Systems 41
2.9 Information Security 41
2.9.1 Storing Protected Information on SDSU Systems 41
2.9.2 Use of Personal Equipment 41
2.9.3 Use of File Servers 42
2.9.4 Use of Databases 42
2.9.5 Backups 42
2.9.5.1 Storing and Retrieving Backups 43
2.9.6 Disposal of IT Resources 43
2.9.7 Retention of IT Resources 44
2.10 Network Security 45
2.10.1 Border Firewall 45
2.10.2 New Internal Firewalls 46
2.10.3 Requesting Access through an Existing Internal Firewall 47
2.10.4 Firewall Logs 47
2.10.5 Intrusion Detection Protection Systems (IDP) 47
2.10.6 Wireless Network 47
2.10.7 Domain Name Service (DNS) 48
2.10.8 Dynamic Host Configuration Protocol (DHCP) 48
2.10.9 Mitigation of Network Risks 48
2.11 Physical and Environmental Security 49
2.11.1 Physical Access to Offices and Buildings 50
2.11.2 Physical Access in Server Rooms 50
2.11.3 Fire Safety 50
2.11.4 Electrical Systems 51
2.11.5 Plumbing and Cooling System (HVAC) Leaks 51
2.12 Residential Halls 52
2.13 Visitor Security 52
2.13.1 Vendors/Consultants 52
2.13.2 Visiting CSU Staff/Faculty 53
2.14 Departmental Assessments 53
2.14.1 Departmental Assessment Form 54
2.15 IT Security Office Assessments 56
Appendix A: Acronyms 58
Appendix B: Glossary 60
Appendix C: Determining Access to Confidential Information 62
Appendix D: Patch Management Plan Examples 63
Appendix E: Acquiring Anti-Virus Software for Home Use 72
Appendix F: Windows XP Workstation Standard Build Sample 73
Appendix G: Windows 2003 Server Standard Build Example 79
Appendix H: Application Security Attacks and Countermeasures 82
Appendix I: Backups and Backup Strategies 95
Appendix J: Encryption 103

Appendix K: Data Center Physical Security.. 106
Appendix L: References 107
Appendix M: Version Review Log.. 109

2.0 Introduction

This Vulnerability Management Program (VMP) provides 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. This Vulnerability Management Program will explain security mechanisms for:

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

2.1 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.

2.1.1 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.

2.1.1.1 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[1]
- ❑ 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)

2.1.1.2 Protected Level 2

Protected level 2 information must be guarded due to proprietary, ethical or privacy considerations. University standards will indicate the controls needed to protect the unauthorized access, modification, transmission, storage or other use of:

- ❑ Identity validation keys
    - Birth date (full: mm-dd-yyyy)
    - Birth date (partial: mm-dd only)
    - Mother's maiden name
- ❑ Name with personally identifiable educational records
    - Courses taken
    - Schedule
    - Test scores
    - Advising records
    - Educational services received
    - Disciplinary actions
    - Grades[2]

[1] Credit card number with expiration date and/or card verification code is also considered protected information

- SDSU identification number (RedID)[2]
- Race & Ethnicity[2]
- Gender[2]
- Transcripts[2]
- E-mail addresses[2]

❑ Name with personally identifiable employee information

- Employee net salary
- Employment history
- Home address
- Personal telephone numbers
- Personal email address
- Parents and other family members names
- Payment history
- Employee evaluations
- Background investigations
- Biometric information
- Electronic or digitized signatures
- Birthplace (City, State, Country)
- Ethnicity
- Gender
- Marital status
- Personal characteristics
- Physical description
- Photograph

❑ 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.)
- Linking a person with the specific subject about which the library user has requested information or materials

2.1.1.3 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

[2] Considered directory information by FERPA, but considered non-directory information by SDSU for SDSU student employees

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
  - Photograph
  - Major field of study
  - Dates of attendance
  - Degrees, honors and awards received
  - Most recent educational agency or institution attended
  - Participation in officially recognized activities and sports
  - Weight and height of members of athletic team
- ❑ 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)
  - SDSU identification number (RedID)
- ❑ Employee information designated as Directory 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)
  - Financial budget information
  - Signature (non-electronic)
  - SDSU identification number (RedID)

SDSU may disclose 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-SDSU (personal) protected information, such as personal credit reports or personal bank statements, must 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.

2.1.2 SDSU Confidential 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.

A) Have the President or VP of BFA acknowledge approval of Dean/VP management of all confidential information in the CSU, prior to access, including current access.

1) Delegation of approval has been signed to VPs and the College Deans. The VP of BFA will acknowledge the approval of the VPs and Deans.
2) Each VP/Dean will gather approvals performed by the data authority manager in their Division/College who has reviewed the university memo "Determining Access to Confidential Data"[3] and therefore understands the need to limit access and thereby risk to confidential information.
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 BFA VP signature will be March 1st, July 1st, and November 1st.
4) Delegation of approval will be renewed by the Provost on an annual basis, during the March 1st semester submission.
5) Confidential information has been scoped to Protected Level 1 financial information: Social Security Number, Tax ID, last four or more of SSN with DOB, Driver's license, credit card, and banking transactions such as ACH.
6) Protected information that must be authorized refers to electronic information, indicated by the CSU Senior Director of Information Security Management and approved by the CSU IT Auditor.
7) The first month of input will include all current confidential access and the repeating cycle will be either a full list again of access in the division/college, or add/change/delete's, whichever is most convenient for the data authority granting access to the information.

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 data authority is the manager who directly

[3] "Determining Access to Confidential Data" can be found in Appendix C

manages access to the information (not the system administrator who creates the access). The data authority 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 2005 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.*
Smith, Rowena
Wong, Min"

Submitted March 2005 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.*
Jones, Christina
Rodriguez, Dolores
Dove, Barbara"

3) The data authority 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:

Last, First Name	Red ID	Admission Apps with SSN	Scholarship Apps with SSN
Jones, Christina	800111222		March 05
Smith, Rowena	800222345	Feb 05	
Dove, Barbara	800333444		March 05
Roriquez, Dolores	800456789		March 05
Wong, Min	811765432	Feb 05	

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 data authority can send a memo to the Division VP/Dean indicating no changes. The email should be printed and be part of the authorization packet for the Division/College.

C) All employees with confidential 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. Data authorities 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[4] and turn it in with memos/account request justifications to the Division VP/Dean. Data authorities 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 VP/Dean to the Vice president of Business and Financial Affairs each quarter.
2) The VP of BFA will acknowledge the approval of the other division management, approve the BFA 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.

[4] http://bfa.sdsu.edu/ps/Revised62503Confidentiality%20Statement.pdf

2.2 Desktop Security

This section of the VMP explains desktop security in terms of patch management and anti-virus/anti-spyware implementation as well as documenting standard builds and authorized software.

2.2.1 Patch Management

A proactive patch management plan is a cost effective measure to counteract threats, and is required by the SDSU Computing Security Policy, section 6.5.[5] A patch management plan includes all forms of software revisions such as patches, upgrades, hot fixes and configuration changes. A patch management plan[6] also includes mechanisms for creating, maintaining and reporting a detailed asset inventory (as outlined in section 2.2.1.1). 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[7].

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[8] 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.

[5] http://security.sdsu.edu/policy/security-policy.html 11/7/2000

[6] Examples of a patch management plan may be found in Appendix D

[7] The SDSU IT managers sub-committee is investigating patch management software this year for campus-wide use. For current updates visit http://security.sdsu.edu/

[8] 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.

2.2.1.1 Patch Planning

IT support staff will be responsible for generating an inventory to be used in the patch management plan. The inventory should include:

- ❑ 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. 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.

Patch management progress must be reviewed by IT management, and obstacles resolved and updates charted on a continuous basis.

2.2.1.2 Patch Implementation

In order to facilitate testing of patches before implementation, a multi-tier deployment is recommended[9]. 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

[9] 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.

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 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. 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.

2.2.1.3 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.

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.

2.2.2 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.

2.2.2.1 Anti-Virus (AV)

SDSU has a site license for McAfee anti-virus (AV) and a site license for 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)[10]:

- ❑ The anti-virus client should be installed with active protection[11] turned on
- ❑ IT support staff should set AV clients to perform daily on demand[12] scans, preferably at the lowest use time on the desktop to minimize the impact to users

[10] Details on criteria and procedures for acquiring free copies of anti-virus software for home use may be found in Appendix E

[11] 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

- 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
- 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) should 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.[13]This is useful for situations where a virus is spreading, and no corresponding DAT file has yet been released.

2.2.2.2 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

[12] 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/anit-spyware vendors may use different terminology for this same functionality

[13] VirusScan Enterprise 8.0i Best Practices Guide, McAfee Security, August 2004, https://mysupport.mcafee.com/eservice_enu/default.htmstart.swe?SWECmd=Start&SWEHo=mysupport.mcafee.com

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) should 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.

2.2.3 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.[14] 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.

2.2.4 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 departments 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

[14] Sample documentation for workstation and server builds can be found in Appendix F, G, H and I.

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 should 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.

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.

2.2.5 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.

2.3 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.

2.3.1 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 should disable the wireless connection to prevent bridging the two networks.

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 2.2.1.1.

Full disk encryption[15] 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

[15] See Appendix J for more information on full disk encryption, encryption standards and key management

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 university Security Incident Response Program[16].

2.3.2 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 in situ).

2.4 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.

[16] http://security.sdsu.edu/policy/SIRP.pdf

2.4.1 Server System Builds

IT management must ensure that server system build configurations are documented by IT support staff.

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.

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

2.4.2 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.

2.4.3 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 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.

One of the services that IT support staff should utilize is system logging. 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.

2.4.4 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 an email notifying them of the removal of the malware from the email in case there was an error in the identification of the malware content.

2.5 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.

2.5.1 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 Vulnerability Management Program. 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.

2.5.2 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 simplified. For instance, if IT support staff need to change the permissions on a shared directory so that authorized access is granted; at a minimum, the IT support staff member should document the change made, so that other IT support staff will have knowledge of the action.

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

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 pro-active 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.

2.6 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 account usage and password selection for those accounts.

2.6.1 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.

2.6.1.1 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.

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.

2.6.1.2 Accessing another User's Account

At times, there may be a need for one user's account, or files, to be accessed by another user.

There needs to be a process to grant 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:

- ❑ The supervisor/user submitting a request for access to the appropriate IT or CHR manager
- ❑ The IT or CHR manager reviews and approves the request
- ❑ If files are to be accessed, IT support staff assigns updated permissions to the files and/or directories
- ❑ If an account is to be accessed[17]:
    - IT support staff assigns a temporary password to the employee's account

[17] Account passwords must be changed on unique accounts so the account owner is aware that the account has been accessed

- The supervisor/user logs in with the temporary password and must change the password

- ❑ The supervisor/user now has access to the account/files.

2.6.1.3 Disabling, Reassigning or Deleting Accounts

IT 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. IT managers are also responsible for tracking the expiration dates on generic, shared generic or temporary user accounts.

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.

2.6.2 Account Usage

1) *Using Any User Accounts*: All users are responsible for keeping their password confidential. Users must not share account 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), must not be authorized due to security concerns.

Instant messaging (IM) is an increasingly popular method for communicating over the Internet. 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 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.

2.6.3 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.

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
- □ They are generally longer than a password and may include whole words
- □ They 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!"

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 Password Selection*: In order to ensure that users follow good password procedure, 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 after 15 minutes (or less) of inactivity, or after five 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 five 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.

2.7 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.”[18]

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

[18] Web Application Break-In, Information Security Magazine, August 2006, http://informationsecurity.techtarget.com/magLogin/1,291245,sid42_gci1206289,00.html

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.

2.7.1 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.[19] IT programmers and developers should 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.[20]

1) Requirements Analysis: Security vulnerabilities not addressed during this phase will be compounded in later phases. IT support staff should 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 should 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

[19] Early Remediation Makes Most Cost Effective Security, Software Vulnerability Risk Management Newsletter, Ounce Labs Inc., http://www.ouncelabs.com/early.html
[20] Application Security by Design, Security Innovation, February 2006, http://www.securityinnovation.com/download.asp?template=whitepaper.html&product=pdf/Application%20Security%20by%20Design.pdf

- ❑ 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 should 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 should be used for code review and unit testing. Security defects uncovered by this process should 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 should 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 should 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 should 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 should have gained during the previous stages of the development process. IT support staff should 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.

2.7.2 Application Security in Commercial or Legacy Systems

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

However, because of the two defining characteristics of the COTS (lack of access to product source code, and lack of control over product evolution), there is a trade-off in that software development time can be reduced, but generally at the cost of a understanding the unique risks and potential security vulnerabilities (many of which may have been addressable if the software was developed in-house using a rigorous security configuration management process.

COTS solution systems comprise a single product or product suite, provided by one vendor that may be tailored to provide the system's functionality. The amount of tailoring, information conversion, and business practice reengineering is often significant. These systems may be found in application areas with general concurrence on application practices, examples being personnel management and financial management applications. PeopleSoft and Oracle are typical vendors.

Whatever type of COTS software is utilized, hackers have access to the same commercial components, and second-hand information about them, that the IT support staff do. The hackers can install them in their environment, and pick and probe at the components until a vulnerability is revealed. Once the vulnerability is revealed, the hacker can use it to compromise any system that uses that component.

IT managers need to ensure that a security assessment of potential COTS software is performed. The security assessment should be done prior to procurement, or immediately after installation. The security assessment should include details of who has access to the system and in what capacity, how the system will be used, if the system contains protected information, and what are the potential threats to the system or system information.

The IT manager should use this information to assess the likelihood of any compromise, and make a decision regarding any controls and countermeasures that may be required. The IT manager should contact the TSO if the assessment involves protected level 1 information. All of this information should be appropriately documented.

Appendix H lists some of the more common attacks[21] that IT support staff should 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).

2.8 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.

2.8.1 Securing the Remote Computer

Faculty, staff and students should ensure that their remote computer meets the same protection standards of anti-virus, anti-spyware, patching, and host firewall outlined in section 2.2 of this Vulnerability Management Program 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.

[21] The Ten Most Critical Web Application Security Vulnerabilities, Open Web Application Security Project (OWASP), January 2004, http://superb-east.dl.sourceforge.net/sourceforge/owasp/OWASPTopTen2004.pdf

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.

2.8.2 Remote Access to Secure Web and Messaging Applications

Faculty, staff and students who want to access their SDSU email, or Meeting Maker calendars, from home or other offsite location, should use Webmail, or Meeting Maker Remote, at https://mail.sdsu.edu and https://bfa.sdsu.edu/mmweb which utilize secure web protocols.

Alternatively, secure protocols such as POPS, IMAPS, and SSL, should be utilized when connecting to campus email and calendar systems using client software applications.

2.8.3 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 theses 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, 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 protected level 1 or level 2 information will be stored on the remote system.

2.8.4 Network Access to Level 1 Information or Critical Systems

Faculty and Staff who require network access to networks containing protected information (such as CHR, 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. This type of connection would be considered a privileged VPN connection, and would require a documented authorization process including the TSO

IT managers must assign an SDSU managed laptop to employees needing non-web application to access protected level 1 information and/or critical systems to ensure the security of the remote connection.

2.9 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.

2.9.1 Storing Protected Information on SDSU Systems

Protected level 1 information must not be stored on SDSU laptops or desktops. Protected information must be stored on secured databases or file servers,, or off-line media, such as CD and DVD storage. Off-line media should be encrypted[22], and must be stored in a secure location at the university or another site approved by IT management (including off-site backup services).

Users who need to have exceptions to these standards for storing protected information must have Dean or Vice-President signed approval.

2.9.2 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 information must not be stored on any personal

[22] See Appendix J for more information on encryption and encryption standards

equipment. Additionally, users must not send emails containing protected information to personal email accounts[23].

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.

2.9.3 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.

2.9.4 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.

In database systems, the use of encryption can cause serious performance issues if most or the entire database is encrypted. A better strategy is to encrypt only those parts of the database that contain protected level 1 information. This approach is sometimes referred to as columnar encryption

2.9.5 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 are responsible for implementing the plan. The backup plan should include items such as the schedule for the backups, encryption of protected information,

[23] Users must not send emails with protected level 1 information to any accounts

daily checking of the backup logs, regular verification of backed up information, 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.

2.9.5.1 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 I in the back of this document.

2.9.6 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 from the equipment sent to surplus. IT 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 erase any remnants of information or software. For drives containing protected information, rewriting three times is required to be sure the information cannot be recovered.

Writing over the hard drive in this manner is a sanitization process called clearing, and leaves the drive still usable. A more powerful sanitization technique called degaussing can increase the chances of the information not being recovered, but also increase the chances of the drive not being reusable since the magnets in the drive motors may be destroyed.

However, using the built-in ATA ANSI standard Secure Erase[24] command for newer ATA drives (more recent than 2001) bigger than 15GB can result in the same level of sanitization as degaussing, 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 degauss or shred them to prevent access to information or licensed software.

2.9.7 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.

IT managers are responsible for creating retention schedules for information not covered by these campus data authorities.

The retention schedules should document:

[24] Guidelines for Media Sanitization, NIST Special Publication 800-88

- ❑ 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
- ❑ 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.

IT 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. 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.

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).

2.10 Network Security

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

2.10.1 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. 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 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.

2.10.2 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.

2.10.3 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.

2.10.4 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.

2.10.5 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.

2.10.6 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 should 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.

2.10.7 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.[25] Requestors can expect DNS requests to take about five business days to complete.

2.10.8 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..

2.10.9 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:

[25] http://security.sdsu.edu/services/dns/

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.
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.

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:

- ❑ There will be no exceptions for the DHCP range (146.244.0.0.- 16)
- ❑ 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.

2.11 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 server rooms 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 K.

2.11.1 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 should 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.

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.

2.11.2 Physical Access in Server Rooms

1) The Server Room: Server rooms should be locked, and accessible only by authorized key access. Visitors (such as service personnel or contactors) 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 should 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.

2.11.3 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.

2.11.4 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.

2.11.5 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 off 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.

2.12 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).[26] 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.

2.13 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.

2.13.1 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 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

[26] The RezCon Acceptable Use Policy (AUP) can be found at http://rezcon.sdsu.edu/Violations.html

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.

2.13.2 Visiting CSU Staff/Faculty

Visiting CSU staff/faculty will be held to the same standards as SDSU staff/faculty.

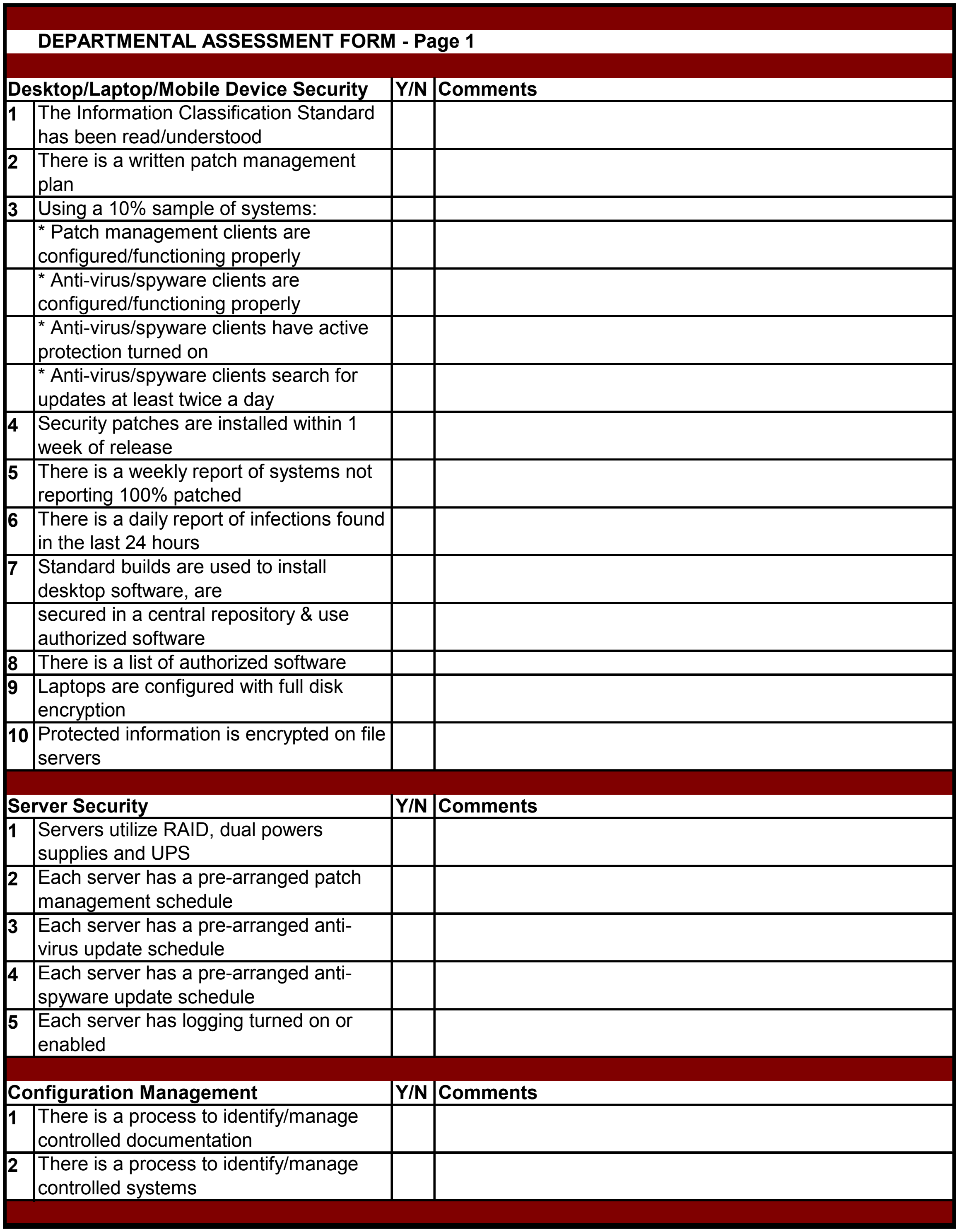
2.14 Departmental Assessments

IT management is responsible for ensuring that they and the IT support staff are familiar with the principles outlined in this Vulnerability Management Program, 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.

2.14.1 Departmental Assessment Form[27]



	DEPARTMENTAL ASSESSMENT FORM - Page 1		
Desktop/Laptop/Mobile Device Security		**Y/N**	**Comments**
1	The Information Classification Standard has been read/understood		
2	There is a written patch management plan		
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		**Y/N**	**Comments**
1	Servers utilize RAID, dual powers supplies and UPS		
2	Each server has a pre-arranged patch management schedule		
3	Each server has a pre-arranged anti-virus update schedule		
4	Each server has a pre-arranged anti-spyware update schedule		
5	Each server has logging turned on or enabled		
Configuration Management		**Y/N**	**Comments**
1	There is a process to identify/manage controlled documentation		
2	There is a process to identify/manage controlled systems		

[27] An electronic copy of this form can be found at http://security/sdsu.edu/forms/dep_assess_form.pdf

	DEPARTMENTAL ASSESSMENT FORM - Page 2		
Account Management		**Y/N**	**Comments**
1	A process exists to create, reassign, disable or delete accounts		
2	Workstations are locked after 15 mins inactivity or when unattended		
3	Passwords automatically expire each 90 days or semester		
4	Accounts are configured to support good password guidelines		
5	Accounts below standard password strength are reported		
6	Accounts are reviewed every quarter or semester		
Information Security		**Y/N**	**Comments**
1	Protected information is not stored on mobile equipment		
2	Protected information is not emailed		
3	Daily backups are executed and verified		
4	A scheduled restoration is used with all backups		
5	A schedule exists to rotate and replace backup media		
6	There is a process to wipe and properly document surplus for pickup		
7	A retention schedule is used for all protected information		
8	All controlled media is secured, logged or accounted for		
Application Security		**Y/N**	**Comments**
1	Applications are tested for known vulnerabilities		
2	Controls for vulnerabilities are implemented		
Network Security		**Y/N**	**Comments**
1	All systems with protected level 1 information are behind a firewall		
2	All systems used for campus business are connected to the wired network		
3	Wireless networking is disabled		
Physical and Environmental Security		**Y/N**	**Comments**
1	Server room doors are self-closing, locked, and fail-safe		
2	Server room access is restricted		
	Manager Signature		**Date**

2.15 IT Security Office Assessments

The purpose of the Vulnerability Management Plan 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 takes 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.

Appendix A: Acronyms

ACH	Automated Clearing House
AES	Advanced Encryption System
AFP	Apple Filing Protocol
ANSI	American National Standards Institute
AS	Anti-spyware
ATA	Advanced Technology Attachment
AUP	Acceptable Use Policy
AV	Anti-virus
CD-R	Compact Disc Recordable
CIO	Chief Information Officer
CHR	Center for Human Resources
COTS	Commercial-off-the-shelf
CPU	Central Processing Unit
CVS	Concurrent Versions System
DAT	Data File
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DVD	Digital Video Disc
ECDSA	Elliptic Curve Digital Signature Algorithm
ePO	ePolicy Orchestrator
FERPA	Family Education Rights and Privacy Act
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GA	Graduate Assistant
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over SSL
HVAC	Heating Ventilating Air Conditioning
IDP	Intrusion Detection Protection
IM	Instant Messaging
IMAPS	Internet Message Access Protocol over SSL
ISA	Intern Student Assistant
OS	Operating System
OU	Organizational Unit
OWASP	Open Web Application Security Project
PDA	Personal Digital Assistant
PHP	PHP Hypertext Preprocessor
PKI	Public Key Infrastructure
POPS	Post Office Protocol over SSL
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RCA	RezCon Assistant

RDP	Remote Desktop Protocol
RedID	SDSU Identification Number
RPC	Remote Procedure Call
RSA	Rivest Shamir Adleman
SFTP	Secure FTP
SHA	Secure Hash Algorithm
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
TA	Teacher Assistant
Tax ID	Tax Identification Number
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supplies
SIMS/R	Student Information Management System Relational
SHS	Student Housing Services
VMP	Vulnerability Management Program
VNC	Virtual Network Computing
VP	Vice President

APPENDIX A

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.

IT Management: Includes Executive Vice Presidents, Vice Presidents, Assistant Vice Presidents, Divisional Managers and Departmental Managers. Primary responsibilities include creating and managing plans to implement the principles outlined in the SDSU Security Plan, and the supervision of the supervision of IT support staff in the execution of those plans.

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.

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.

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.

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.

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.

Appendix C: Determining Access to Confidential 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 assess 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 D: 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 mangers, DARES 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, DAREs, 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:

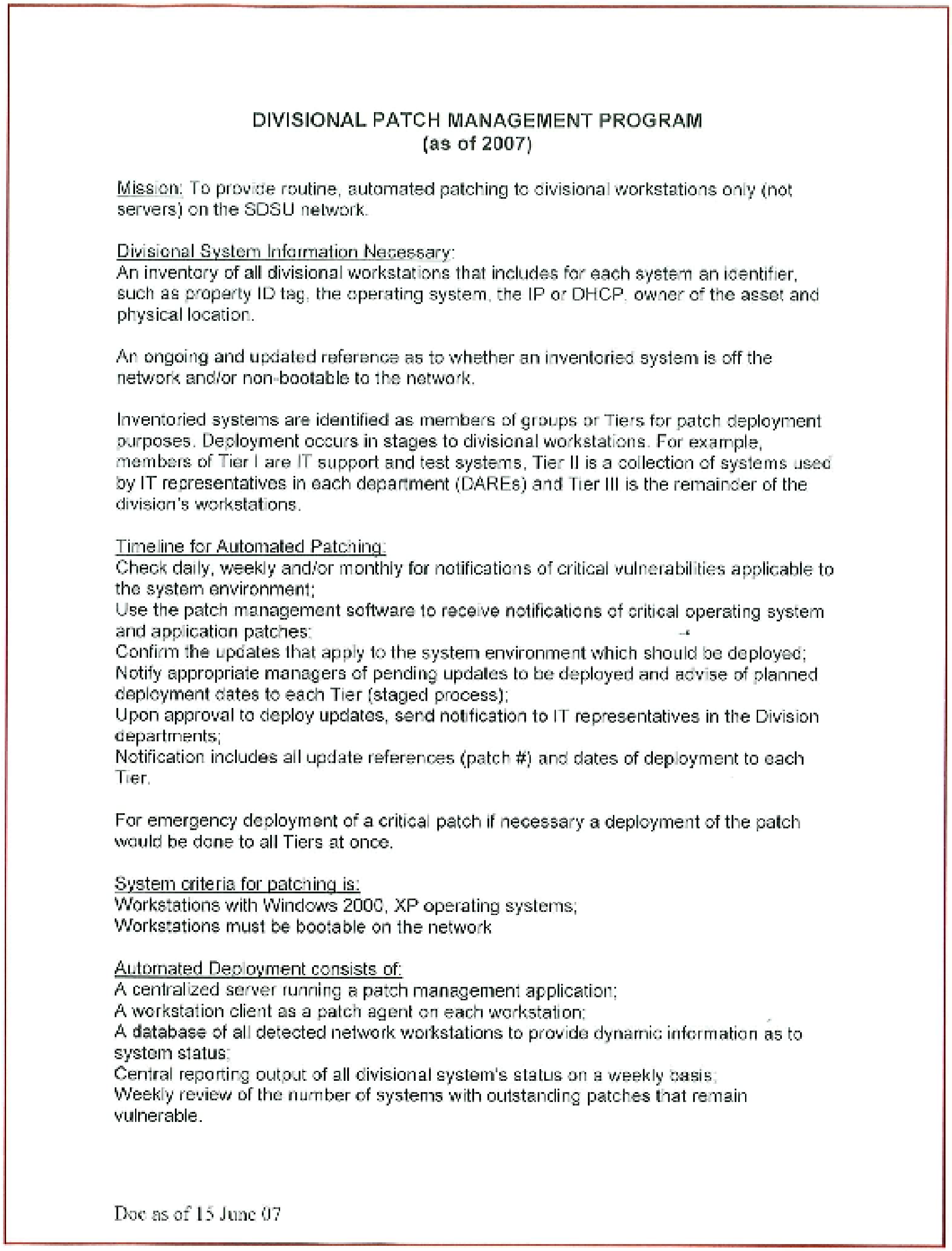
- Date of deployment
- Patch name(s)
- Source of patch
- Priority of patch
- System(s) affected
- Impact of vulnerability
- Time line for deployment

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 PROGRAM
(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.

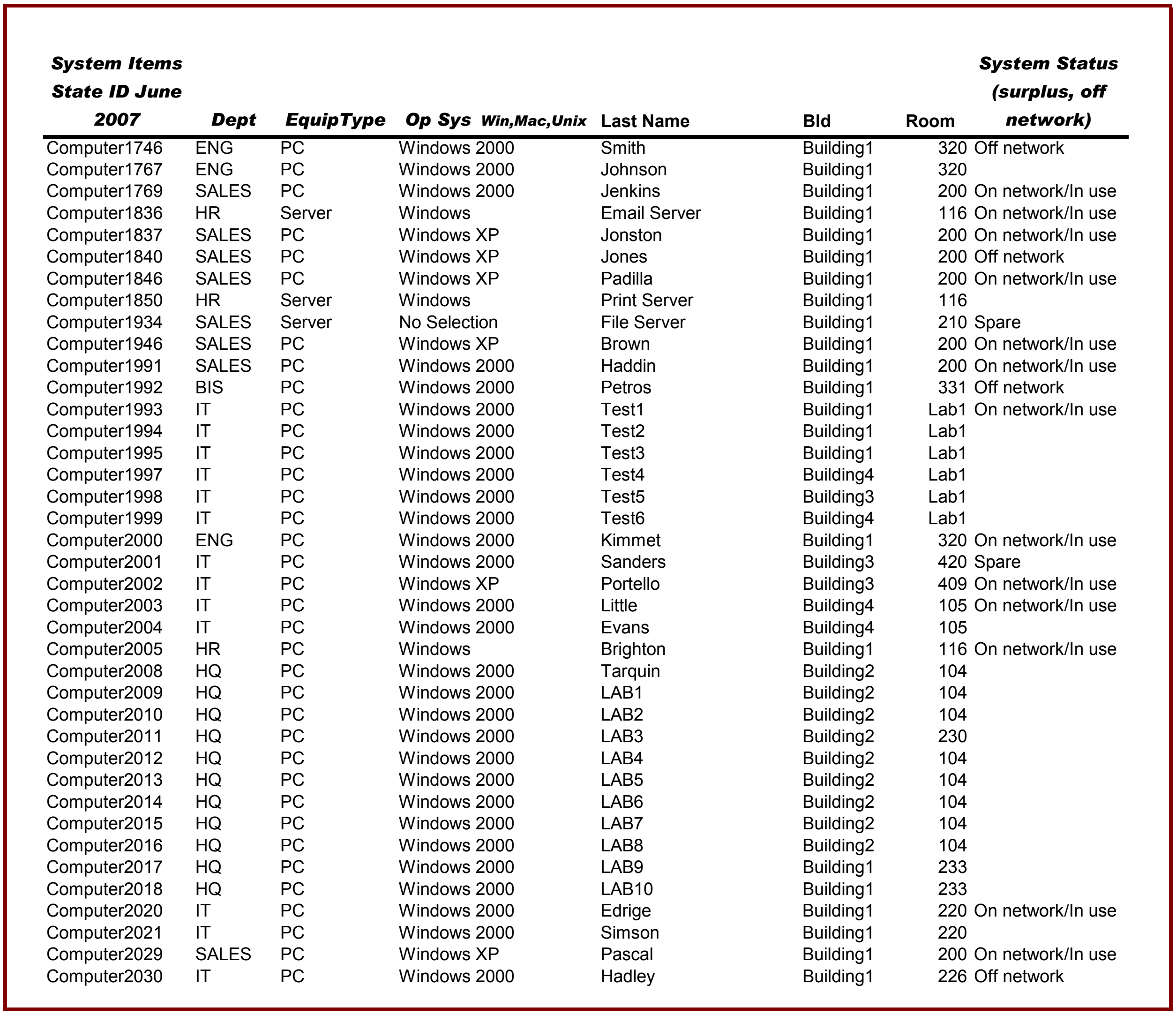
System criteria for patching is:
Workstations with Windows 2000, XP operating systems;
Workstations must be bootable on the network

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.

Doc as of 15 June 07

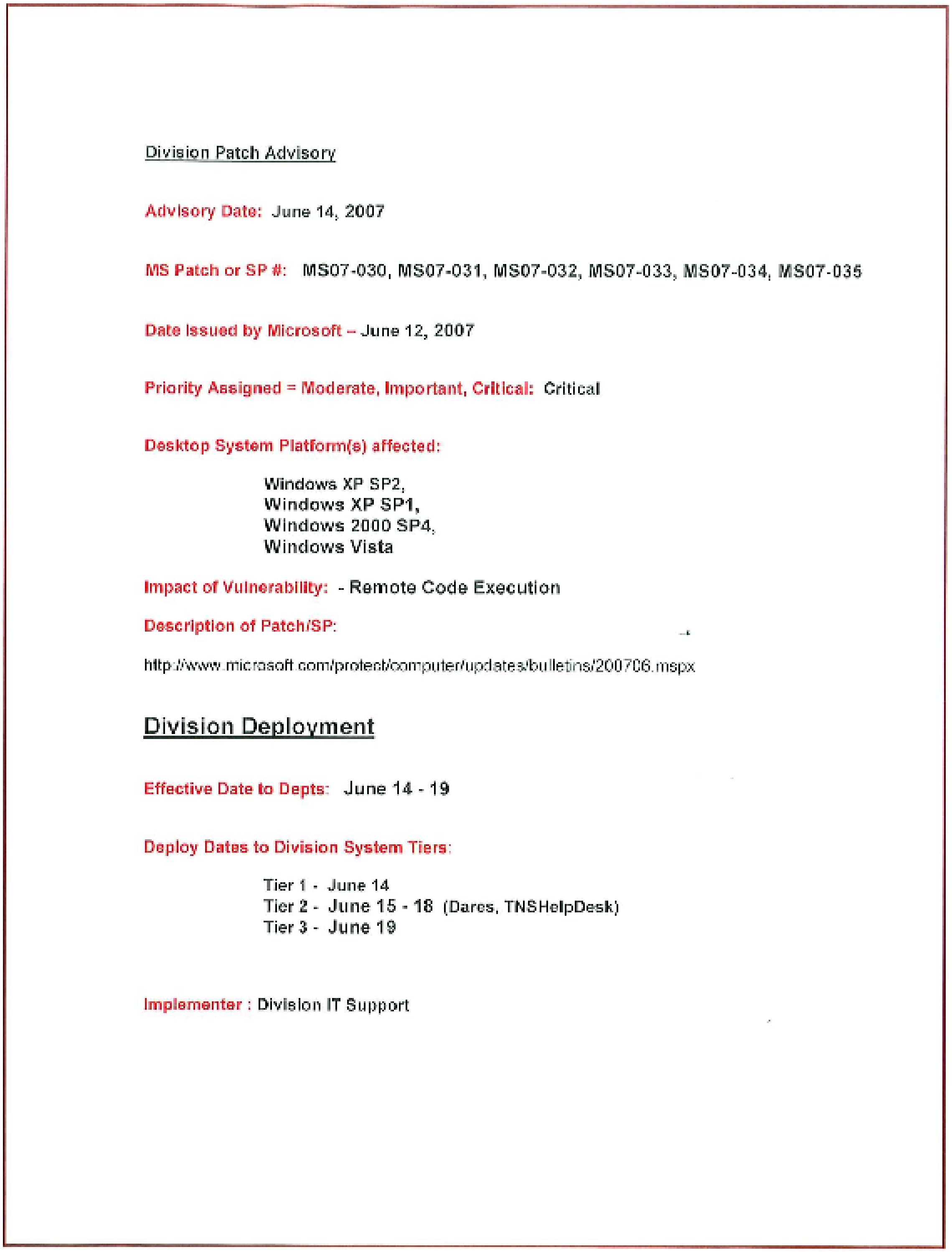
Figure 1: Example of a patch management plan

APPENDIX D



System Items State ID June 2007	Dept	EquipType	Op Sys Win,Mac,Unix	Last Name	Bld	Room	System Status (surplus, off network)
Computer1746	ENG	PC	Windows 2000	Smith	Building1	320	Off network
Computer1767	ENG	PC	Windows 2000	Johnson	Building1	320	
Computer1769	SALES	PC	Windows 2000	Jenkins	Building1	200	On network/In use
Computer1836	HR	Server	Windows	Email Server	Building1	116	On network/In use
Computer1837	SALES	PC	Windows XP	Jonston	Building1	200	On network/In use
Computer1840	SALES	PC	Windows XP	Jones	Building1	200	Off network
Computer1846	SALES	PC	Windows XP	Padilla	Building1	200	On network/In use
Computer1850	HR	Server	Windows	Print Server	Building1	116	
Computer1934	SALES	Server	No Selection	File Server	Building1	210	Spare
Computer1946	SALES	PC	Windows XP	Brown	Building1	200	On network/In use
Computer1991	SALES	PC	Windows 2000	Haddin	Building1	200	On network/In use
Computer1992	BIS	PC	Windows 2000	Petros	Building1	331	Off network
Computer1993	IT	PC	Windows 2000	Test1	Building1	Lab1	On network/In use
Computer1994	IT	PC	Windows 2000	Test2	Building1	Lab1	
Computer1995	IT	PC	Windows 2000	Test3	Building1	Lab1	
Computer1997	IT	PC	Windows 2000	Test4	Building4	Lab1	
Computer1998	IT	PC	Windows 2000	Test5	Building3	Lab1	
Computer1999	IT	PC	Windows 2000	Test6	Building4	Lab1	
Computer2000	ENG	PC	Windows 2000	Kimmet	Building1	320	On network/In use
Computer2001	IT	PC	Windows 2000	Sanders	Building3	420	Spare
Computer2002	IT	PC	Windows XP	Portello	Building3	409	On network/In use
Computer2003	IT	PC	Windows 2000	Little	Building4	105	On network/In use
Computer2004	IT	PC	Windows 2000	Evans	Building4	105	
Computer2005	HR	PC	Windows	Brighton	Building1	116	On network/In use
Computer2008	HQ	PC	Windows 2000	Tarquin	Building2	104	
Computer2009	HQ	PC	Windows 2000	LAB1	Building2	104	
Computer2010	HQ	PC	Windows 2000	LAB2	Building2	104	
Computer2011	HQ	PC	Windows 2000	LAB3	Building2	230	
Computer2012	HQ	PC	Windows 2000	LAB4	Building2	104	
Computer2013	HQ	PC	Windows 2000	LAB5	Building2	104	
Computer2014	HQ	PC	Windows 2000	LAB6	Building2	104	
Computer2015	HQ	PC	Windows 2000	LAB7	Building2	104	
Computer2016	HQ	PC	Windows 2000	LAB8	Building2	104	
Computer2017	HQ	PC	Windows 2000	LAB9	Building1	233	
Computer2018	HQ	PC	Windows 2000	LAB10	Building1	233	
Computer2020	IT	PC	Windows 2000	Edrige	Building1	220	On network/In use
Computer2021	IT	PC	Windows 2000	Simson	Building1	220	
Computer2029	SALES	PC	Windows XP	Pascal	Building1	200	On network/In use
Computer2030	IT	PC	Windows 2000	Hadley	Building1	226	Off network

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:

http://www.microsoft.com/protect/computer/updates/bulletins/200706.mspx

Division Deployment

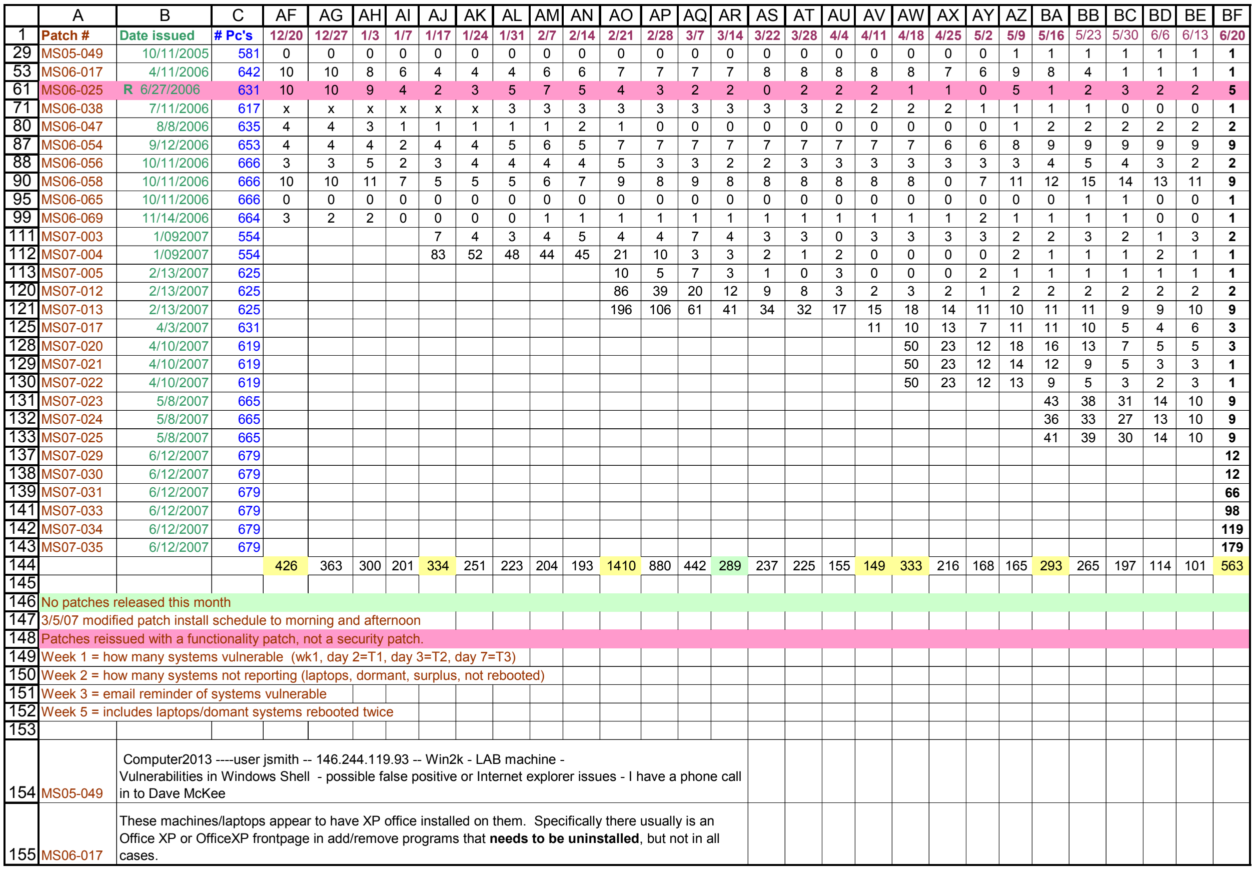
Effective Date to Depts: June 14 - 19

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



	A	B	C	AF	AG	AH	AI	AJ	AK	AL	AM	AN	AO	AP	AQ	AR	AS	AT	AU	AV	AW	AX	AY	AZ	BA	BB	BC	BD	BE	BF
1	Patch #	Date issued	# Pc's	12/20	12/27	1/3	1/7	1/17	1/24	1/31	2/7	2/14	2/21	2/28	3/7	3/14	3/22	3/28	4/4	4/11	4/18	4/25	5/2	5/9	5/16	5/23	5/30	6/6	6/13	6/20
29	MS05-049	10/11/2005	581	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	**1**
53	MS06-017	4/11/2006	642	10	10	8	6	4	4	4	6	6	7	7	7	7	8	8	8	8	8	7	6	9	8	4	1	1	1	**1**
61	MS06-025	R 6/27/2006	631	10	10	9	4	2	3	5	7	5	4	3	2	2	0	2	2	2	1	1	0	5	1	2	3	2	2	**5**
71	MS06-038	7/11/2006	617	x	x	x	x	x	x	3	3	3	3	3	3	3	3	3	2	2	2	2	1	1	1	1	0	0	0	**1**
80	MS06-047	8/8/2006	635	4	4	3	1	1	1	1	1	2	1	0	0	0	0	0	0	0	0	0	0	1	2	2	2	2	2	**2**
87	MS06-054	9/12/2006	653	4	4	4	2	4	4	5	6	5	7	7	7	7	7	7	7	7	7	6	6	8	9	9	9	9	9	**9**
88	MS06-056	10/11/2006	666	3	3	5	2	3	4	4	4	4	5	3	3	2	2	3	3	3	3	3	3	3	4	5	4	3	2	**2**
90	MS06-058	10/11/2006	666	10	10	11	7	5	5	5	6	7	9	8	9	8	8	8	8	8	8	0	7	11	12	15	14	13	11	**9**
95	MS06-065	10/11/2006	666	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	**1**
99	MS06-069	11/14/2006	664	3	2	2	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	0	0	**1**
111	MS07-003	1/092007	554					7	4	3	4	5	4	4	7	4	3	3	0	3	3	3	3	2	2	3	2	1	3	**2**
112	MS07-004	1/092007	554					83	52	48	44	45	21	10	3	3	2	1	2	0	0	0	0	2	1	1	1	2	1	**1**
113	MS07-005	2/13/2007	625										10	5	7	3	1	0	3	0	0	0	2	1	1	1	1	1	1	**1**
120	MS07-012	2/13/2007	625										86	39	20	12	9	8	3	2	3	2	1	2	2	2	2	2	2	**2**
121	MS07-013	2/13/2007	625										196	106	61	41	34	32	17	15	18	14	11	10	11	11	9	9	10	**9**
125	MS07-017	4/3/2007	631																	11	10	13	7	11	11	10	5	4	6	**3**
128	MS07-020	4/10/2007	619																		50	23	12	18	16	13	7	5	5	**3**
129	MS07-021	4/10/2007	619																		50	23	12	14	12	9	5	3	3	**1**
130	MS07-022	4/10/2007	619																		50	23	12	13	9	5	3	2	3	**1**
131	MS07-023	5/8/2007	665																						43	38	31	14	10	**9**
132	MS07-024	5/8/2007	665																						36	33	27	13	10	**9**
133	MS07-025	5/8/2007	665																						41	39	30	14	10	**9**
137	MS07-029	6/12/2007	679																											**12**
138	MS07-030	6/12/2007	679																											**12**
139	MS07-031	6/12/2007	679																											**66**
141	MS07-033	6/12/2007	679																											**98**
142	MS07-034	6/12/2007	679																											**119**
143	MS07-035	6/12/2007	679																											**179**
144				426	363	300	201	334	251	223	204	193	1410	880	442	289	237	225	155	149	333	216	168	165	293	265	197	114	101	563
145																														
146	No patches released this month																													
147	3/5/07 modified patch install schedule to morning and afternoon																													
148	Patches reissued with a functionality patch, not a security patch.																													
149	Week 1 = how many systems vulnerable (wk1, day 2=T1, day 3=T2, day 7=T3)																													
150	Week 2 = how many systems not reporting (laptops, dormant, surplus, not rebooted)																													
151	Week 3 = email reminder of systems vulnerable																													
152	Week 5 = includes laptops/domant systems rebooted twice																													
153																														
154	MS05-049	Computer2013 ----user jsmith -- 146.244.119.93 -- Win2k - LAB machine - Vulnerabilities in Windows Shell - possible false positive or Internet explorer issues - I have a phone call in to Dave McKee																												
155	MS06-017	These machines/laptops appear to have XP office installed on them. Specifically there usually is an Office XP or OfficeXP frontpage in add/remove programs that **needs to be uninstalled**, but not in all cases.																												

Figure 4: Example of Tracking Microsoft Patches

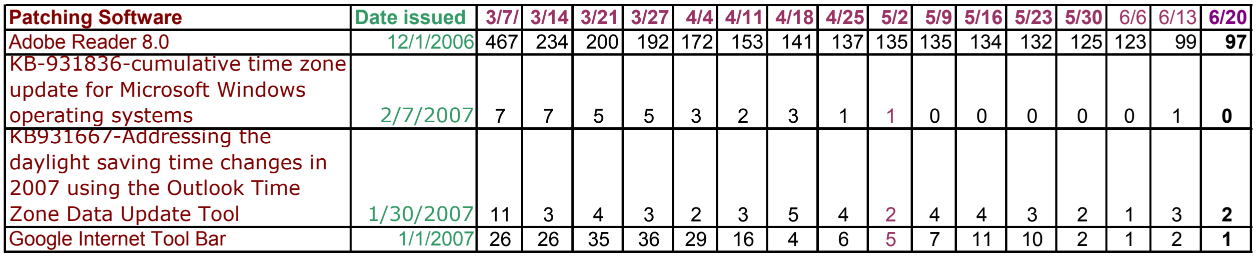
The report shown in Figure 4 is a very useful mechanism for tracking the deployment of patches. The numbers in the columns AF to BF show the number of systems which are reporting as unpatched between the dates 12/20/2006 and 6/20/2007. In theory, the number of system reporting unpatched should become 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.

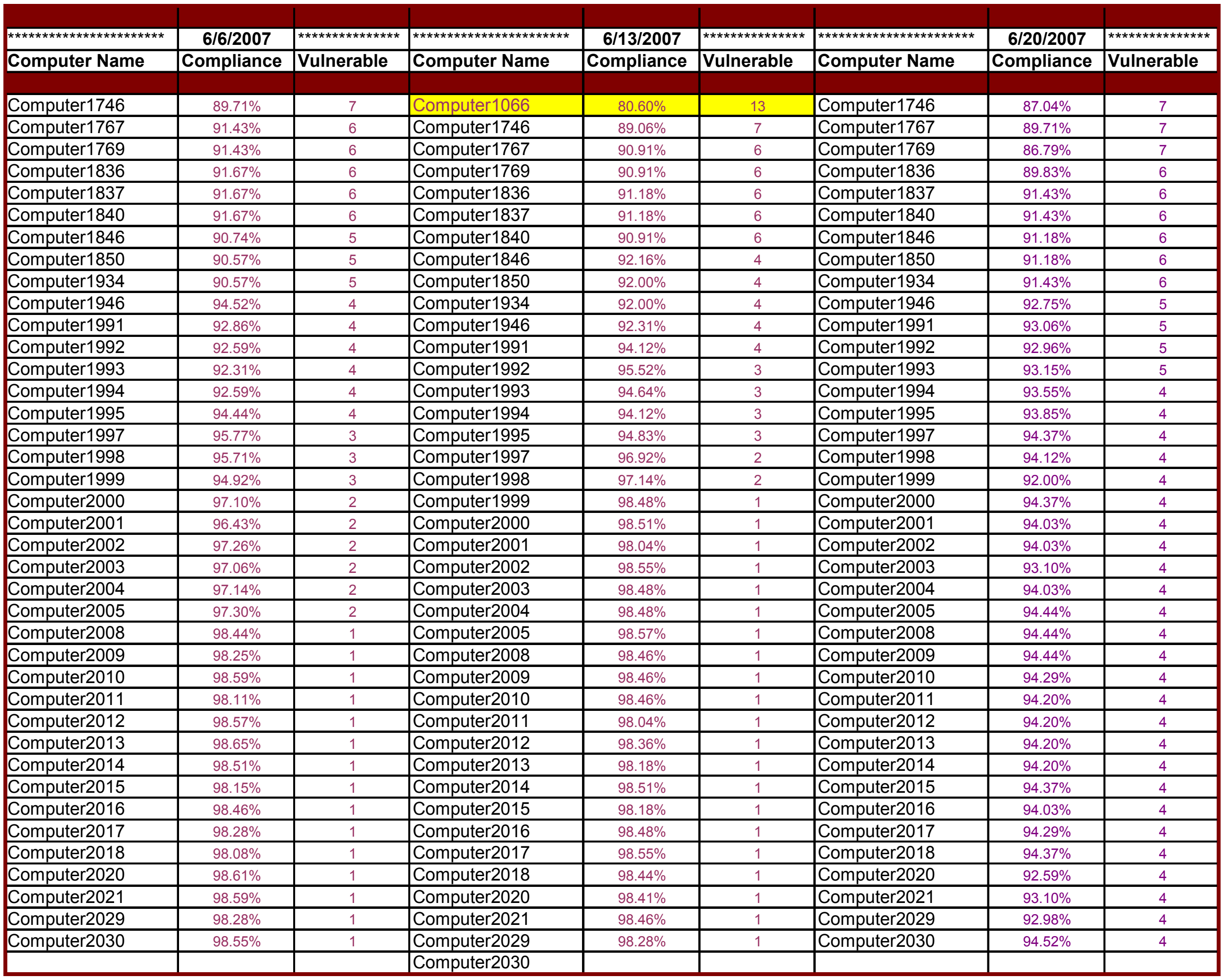


Patching Software	Date issued	3/7/	3/14	3/21	3/27	4/4	4/11	4/18	4/25	5/2	5/9	5/16	5/23	5/30	6/6	6/13	6/20
Adobe Reader 8.0	12/1/2006	467	234	200	192	172	153	141	137	135	135	134	132	125	123	99	**97**
KB-931836-cumulative time zone update for Microsoft Windows operating systems	2/7/2007	7	7	5	5	3	2	3	1	1	0	0	0	0	0	1	**0**
KB931667-Addressing the daylight saving time changes in 2007 using the Outlook Time Zone Data Update Tool	1/30/2007	11	3	4	3	2	3	5	4	2	4	4	3	2	1	3	**2**
Google Internet Tool Bar	1/1/2007	26	26	35	36	29	16	4	6	5	7	11	10	2	1	2	**1**

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.

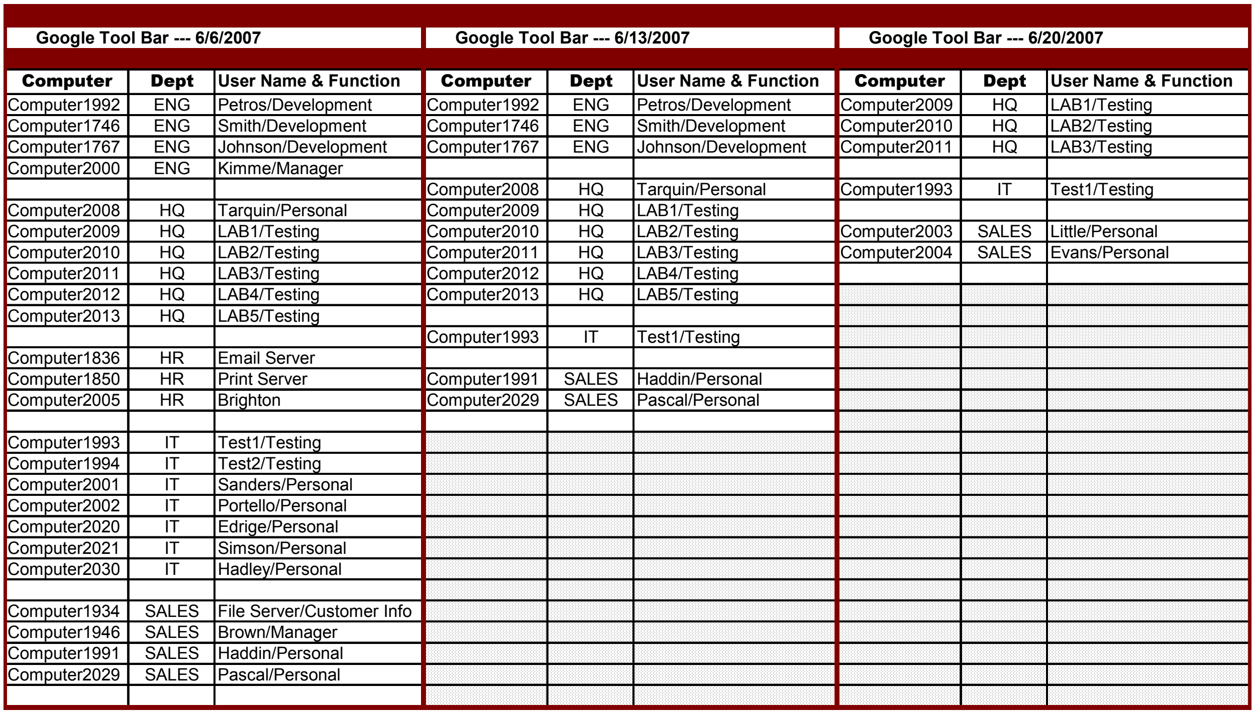


***********************	6/6/2007	***************	***********************	6/13/2007	***************	***********************	6/20/2007	***************
Computer Name	Compliance	Vulnerable	Computer Name	Compliance	Vulnerable	Computer Name	Compliance	Vulnerable
Computer1746	89.71%	7	Computer1066	80.60%	13	Computer1746	87.04%	7
Computer1767	91.43%	6	Computer1746	89.06%	7	Computer1767	89.71%	7
Computer1769	91.43%	6	Computer1767	90.91%	6	Computer1769	86.79%	7
Computer1836	91.67%	6	Computer1769	90.91%	6	Computer1836	89.83%	6
Computer1837	91.67%	6	Computer1836	91.18%	6	Computer1837	91.43%	6
Computer1840	91.67%	6	Computer1837	91.18%	6	Computer1840	91.43%	6
Computer1846	90.74%	5	Computer1840	90.91%	6	Computer1846	91.18%	6
Computer1850	90.57%	5	Computer1846	92.16%	4	Computer1850	91.18%	6
Computer1934	90.57%	5	Computer1850	92.00%	4	Computer1934	91.43%	6
Computer1946	94.52%	4	Computer1934	92.00%	4	Computer1946	92.75%	5
Computer1991	92.86%	4	Computer1946	92.31%	4	Computer1991	93.06%	5
Computer1992	92.59%	4	Computer1991	94.12%	4	Computer1992	92.96%	5
Computer1993	92.31%	4	Computer1992	95.52%	3	Computer1993	93.15%	5
Computer1994	92.59%	4	Computer1993	94.64%	3	Computer1994	93.55%	4
Computer1995	94.44%	4	Computer1994	94.12%	3	Computer1995	93.85%	4
Computer1997	95.77%	3	Computer1995	94.83%	3	Computer1997	94.37%	4
Computer1998	95.71%	3	Computer1997	96.92%	2	Computer1998	94.12%	4
Computer1999	94.92%	3	Computer1998	97.14%	2	Computer1999	92.00%	4
Computer2000	97.10%	2	Computer1999	98.48%	1	Computer2000	94.37%	4
Computer2001	96.43%	2	Computer2000	98.51%	1	Computer2001	94.03%	4
Computer2002	97.26%	2	Computer2001	98.04%	1	Computer2002	94.03%	4
Computer2003	97.06%	2	Computer2002	98.55%	1	Computer2003	93.10%	4
Computer2004	97.14%	2	Computer2003	98.48%	1	Computer2004	94.03%	4
Computer2005	97.30%	2	Computer2004	98.48%	1	Computer2005	94.44%	4
Computer2008	98.44%	1	Computer2005	98.57%	1	Computer2008	94.44%	4
Computer2009	98.25%	1	Computer2008	98.46%	1	Computer2009	94.44%	4
Computer2010	98.59%	1	Computer2009	98.46%	1	Computer2010	94.29%	4
Computer2011	98.11%	1	Computer2010	98.46%	1	Computer2011	94.20%	4
Computer2012	98.57%	1	Computer2011	98.04%	1	Computer2012	94.20%	4
Computer2013	98.65%	1	Computer2012	98.36%	1	Computer2013	94.20%	4
Computer2014	98.51%	1	Computer2013	98.18%	1	Computer2014	94.20%	4
Computer2015	98.15%	1	Computer2014	98.51%	1	Computer2015	94.37%	4
Computer2016	98.46%	1	Computer2015	98.18%	1	Computer2016	94.03%	4
Computer2017	98.28%	1	Computer2016	98.48%	1	Computer2017	94.29%	4
Computer2018	98.08%	1	Computer2017	98.55%	1	Computer2018	94.37%	4
Computer2020	98.61%	1	Computer2018	98.44%	1	Computer2020	92.59%	4
Computer2021	98.59%	1	Computer2020	98.41%	1	Computer2021	93.10%	4
Computer2029	98.28%	1	Computer2021	98.46%	1	Computer2029	92.98%	4
Computer2030	98.55%	1	Computer2029	98.28%	1	Computer2030	94.52%	4
			Computer2030					

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 13th 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.



Google Tool Bar --- 6/6/2007			Google Tool Bar --- 6/13/2007			Google Tool Bar --- 6/20/2007		
Computer	**Dept**	**User Name & Function**	**Computer**	**Dept**	**User Name & Function**	**Computer**	**Dept**	**User Name & Function**
Computer1992	ENG	Petros/Development	Computer1992	ENG	Petros/Development	Computer2009	HQ	LAB1/Testing
Computer1746	ENG	Smith/Development	Computer1746	ENG	Smith/Development	Computer2010	HQ	LAB2/Testing
Computer1767	ENG	Johnson/Development	Computer1767	ENG	Johnson/Development	Computer2011	HQ	LAB3/Testing
Computer2000	ENG	Kimme/Manager						
			Computer2008	HQ	Tarquin/Personal	Computer1993	IT	Test1/Testing
Computer2008	HQ	Tarquin/Personal	Computer2009	HQ	LAB1/Testing			
Computer2009	HQ	LAB1/Testing	Computer2010	HQ	LAB2/Testing	Computer2003	SALES	Little/Personal
Computer2010	HQ	LAB2/Testing	Computer2011	HQ	LAB3/Testing	Computer2004	SALES	Evans/Personal
Computer2011	HQ	LAB3/Testing	Computer2012	HQ	LAB4/Testing			
Computer2012	HQ	LAB4/Testing	Computer2013	HQ	LAB5/Testing			
Computer2013	HQ	LAB5/Testing						
			Computer1993	IT	Test1/Testing			
Computer1836	HR	Email Server						
Computer1850	HR	Print Server	Computer1991	SALES	Haddin/Personal			
Computer2005	HR	Brighton	Computer2029	SALES	Pascal/Personal			
Computer1993	IT	Test1/Testing						
Computer1994	IT	Test2/Testing						
Computer2001	IT	Sanders/Personal						
Computer2002	IT	Portello/Personal						
Computer2020	IT	Edrige/Personal						
Computer2021	IT	Simson/Personal						
Computer2030	IT	Hadley/Personal						
Computer1934	SALES	File Server/Customer Info						
Computer1946	SALES	Brown/Manager						
Computer1991	SALES	Haddin/Personal						
Computer2029	SALES	Pascal/Personal						

Figure 7: Tracking Specific Vulnerabilities by Computer

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 E: 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 F: 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.

Win XP Pro Standard Workstation Configuration

Last Updated xx/xx/2007

STEP	PROCESS	INSTRUCTIONS
		Consolidate & Backup User's Data
1	User Prep	Request user complete the Standard Desktop Application Configuration Request Form. Schedule preliminary meeting with user to discuss data transition.
2	Update Inventory	If PC is new, request copy of Purchase Order from the department. Tag machine and record State ID on Purchase order. Forward to appropriate manager.
3	Vendor Image	For new PC, create Altiris image as received from vendor, for emergency restoration. For rebuilds/replacement build, create a before-installation image. Image preserved for (30) days for restore purposes.
4	Local Account Profiles	Create a local user account with a temporary password. Create temporary network directory to save data; i.e., \\server1\DeptName\Users…\
5	Active Directory Profiles	Request department forward new user domain information to Sys Admin to create a domain account, group membership, network share directories, and if user to be assigned a local, admin account.
6	Consolidate/Backup Data	User/DARE to consolidate all user's data in "My Documents" on "C" drive. Archive email attachments to CD, Zip, or floppy. Make a temporary copy of the Eudora directory to the users' "My Documents"; for example, C:\Documents and Settings\jsmith\My Documents. Save Brio query files, ADI themes, and other application configuration files to "My Documents" on "C". Entire "My Documents" on "C" should be saved to CD or Network before proceeding.
		Install and Configure Win XP
1	Notify AD Admin	Send email with the machine ID#(s) and department name to Active Directory Admin so the machine(s) are added to appropriate domain Org Unit.
2	Create a fresh installation	Configure the BIOS to boot from CD-ROM. **Unplug the network cable**, place the Win XP Pro SP2 CD into the drive and cold-start the PC. Follow the onscreen prompts to delete any existing Windows installation and partitions. Create and format a single, new partition.
3	Begin process	To begin, press **<Enter>** at the prompt, "To set up Win XP now, press <ENTER>".
4	License agreement	Press **<F8>** if you agree to the Licensing Agreement.
5	Select installation	To continue installing a fresh copy of Win XP without repairing, press **<ESC>**
6	Delete old partitions	To delete the selected partition, press **<D>**
7	Delete system partition	To delete this partition, press **<ENTER>**

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.
33	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>**
34	Log in as Administrator	Log in using user name: administrator
35	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>**
		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>**
38	Change Folders to List View	Open the "My Documents" Folder. **<Select>** "view" and then "details".**<Select>** "tools" and then "folder options." **<Select>** the "view" tab and click "Apply to all folders" and then click "yes."
39	Taskbar and Start Menu Properties	Double click **<Taskbar and Start Menu>**. The "Taskbar and Start Menu Properties" dialog box displays. Select the **<Taskbar>** tab. Under the heading "Taskbar appearance", **<de-select>** (uncheck) "Lock the taskbar" and **<select>** (check) "Show Quick Launch". Under the heading, "Notification area", **<de-select>** (uncheck) "Hide inactive icons", then press **<Apply>**
40	Start Menu Tab	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 **<OK> | <Apply> | <OK>**
41	Add or Remove Programs, Windows Components	Double Click **<Add or Remove Programs>** | **<Add/Remove Windows Components>**. Under the heading "Components", from the scrolll-down menu, **select <Accessories and Utilities>** | **<Details> | de-select** (uncheck) **<Games>** | **<OK>**
42	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.
43	Bios Boot Sequence	On restart enter the computer BIOS. Reset the boot sequence to **(1)** hard drive, **(2)** CD-ROM, and **(3)** Floppy Drive
44	Log On to Windows	Log on as administrator.
45	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>**
46	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>**
47	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.
48	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>**.
49	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>**
	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.

50	Search for files and folders	Click on **<Start>** | **<Search>** | **<For Files or Folders>**. The "Search Results" window displays. Click on the link **<Change Preferences>**. When prompted, "How do you want to use search companion?", click on the link **<Change Files and Folders Search Behavior>** | **<select>** (click on) **<Advanced> | <OK>** | **<Close Window>**
51	Desktop Icons	Rename "My Network Places" to "Network". Rename "My Computer" to "Computer".
52	Load Drivers	Remove the Win XP installation disk from the CD-ROM drive and insert the vendor's "Drivers and Utilities" CD to install drivers for onboard components such as: NIC, Video, and sound adapters.
53	Connect network cable	Connect network cable to the computer
54	Map Network Drive	**\\server1\DeptName\.** Connect with user name and password. Open "Install Shortcuts" folder.
55	Install McAfee from Quark	Double-Click on McAfee 8.0i icon and install McAfee, For license expiry type select "perpetual". On next screen select "typical" setup. When complete uncheck **Run On-Demand Scan.** press **<Finish>** McAfee updates and then click **<OK>** and restart computer.
56	Log On to Windows	Log on as administrator.
57	Install Microsoft Update	Start Internet Explorer, (click on) **<Tools> | <Windows Update>. <Select> Don't Install** for Windows Update. <**Select>** Microsoft Update. (New browser window opens) **<Select>** Start now.**<Continnue> | <OK> | <Select>** Install the ActiveX control from the toolbar. **<Select>** Install. **<Select>** Install. Install will continue. You may have to restart your computer. If so, restart and run Microsoft update again following the steps here.
58	Change Automatic Updates	Leave off and **<Select>** Check for updates. **<Select>** custom. Select all available updates. Continue the updates (sometimes restarting computer) untill all updates are completed.
59	Delete Windows Update	From desktop click **<Start>** and right click on windows update and delete, click **<Yes>.**
		Install Standard BFA Desktop Applications
60	Install Shortcuts	Map a drive to \\server1\DeptName\Install Shortcuts, then install applications from network by launching each of the following shortcuts
61	Acrobat Reader 7.0	Double Click "AcrobatReader708.exe" **<next>|<next>|<next>|<install>**
62	Eudora Installation	Eudora 7.0.1. Do not select **<deselect>** 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 & .toc, and descmap.pce. Also include attachments, embedded, Filters, Sigs, Stationery, Nickname & any user-created mailbox folder.
	Eudora Configuration	*After Eudora has been installed, launch the application under the user's profile to configure the Eudora settings. Eudora Junk settings -- set score to (50), deselect "put not Junk-ed senders in Address Book", select "Mail is not junk if sender is in Address book", adjust "Remove mail" to (10) days old.*
63	DEPT W2K-XP Changes.reg	Double-click DEPT W2K-XP Changes.reg. **<select>** "yes" and "ok"
64	Winzip	Double Click "Winzip (Run this 1st!)" **<ok>|<next>.** License agreement click **<yes>|<se;ect>** "start with WinZip Classic" **<next>. <select>** "Express setup" **<next>|<finish>,** close open windows. In \\Quark\install shortcuts double click "Winzip (Run this 2nd!)" Click-on "Setup" **<ok>|<ok>|<ok>|<next>.** License agreement click **<yes>. <se;ect>** "start with WinZip Classic" **<next> <select>** "Express setup" **<next>|<finish>,** close open windows.
65	FTP	Double Click "WS_FTP32". **<Continue>** and then **<select>** "A student, faculty member or staff of an educational institution." **<next>| <select>** boxes "At School" and "For academic work" **<next>|<ok>|<ok>|<ok>|<ok>|<ok>**
66	SpyBot	See SpyBot documentation for install

67	Meeting Maker 8.5	Double-Click "Meeting Maker 8.5" **<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	Microsoft Update	**<Start> <Microsoft Update>** Select "custom" and install updates for Office Programs and other updates that were missed. Continue to check for updates until none are available.
70	Disconnect Network Drives	Disconnect \\Server1\DeptName as a mapped drive.
71	Shortcuts	set up shortcuts in Quick Launch bar for applications MeetingMaker, Eudora, Excel, Word and others that user may want.
	***	**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.
	***	**Next steps are for prepping machine as primary for image deployment. If this install is for a single machine then skip this section and proceed to "Domain Set UP and DNS Servers."**
73	Install A-Client & SIDGEN	On \\Server1\PCApps\Altiris\Aclient double click on Aclient.exe to install Aclient. In first window **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>**
	***	**Next steps for single install. If set up is for deployment by image this step should be done on each separate computer after deployment.**
		Domain Set Up and DNS Servers
74	Join computer to DEPT Domain	Join the computer to the DEPT domain. Right Click **<Computer>** Select properties. **<Select>** change. Under "member of" menu, **<select>** Domain. Type "**DEPT.SDSU.EDU**" Enter your domain user name and password. **<OK> | <OK>.** Restart computer.
		The BA Domain, Active Directory re-names the Administrator account to Claub. If you desire, copy the appropriate account profile and copy it to Default Users; i.e., copy the user profile if configured, or claub profile if a user account was not created. For any new user, Win XP uses the Default User profile to set the desktop and configuration settings, the first time that user logs on. All standard BFA profile settings will be carried over to the new users profile.
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.

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.
		Select **<Copy To>** and browse/navigate to "C:\Documents and Settings\Default User", click **<OK>.** In the Permitted to use field click **<Change>** and type "EVERYONE" Click **<OK>.** You will then need to log in using your domain login account. Click **<OK> | <YES>.** Log off computer as admin2.
78	Login using claub account	From desktop, right click **<Computer>** select properties. Click **<Advanced>** tab and click **<Settings>** under the User Profiles menu. Under user profiles select the user profile for the admin2 account. Click **<Delete>,** delete the admin2 user profile. Confirm click **<Yes>.**
78	remove admin2 account	Launch Control Panel to delete the admin2 account set up in step 30. **<Control Panel> | <User Accounts>.** Select the admin2.. Click **<Remove> | <Yes> | <OK>.**
79	Configure Network Settings	Right-click on the "Network" icon from the desktop **<select>** "properties". Right-click on the "Local Area Connection" and **<select>** "properties." Left-click on "Internet Protocol (TCP/IP)" and **<select>** "Properties." 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.
80	Configure DNS Servers (if unable to do so at Step 28)	**<Click>** "Use the following DNS Server addresses" The preferred DNS Server is 130.191.16.85. Alternate DNS server is 130.191.16.81. **<Select>** "advanced." **<Select>** "DNS" tab. Under the DNS server addresses **<select>** "add." Add 130.191.1.1 and then add 130.191.200.1.**<Click>** Ok | OK | Close.
	***	**Next steps forimage deployment systems only. If set up is for single computer then steps are completed.**
	SIDGEN Delete	If the primary image has been deployed SIDGEN must be deleted on each of the computers that recived the image as well as on the primary computer. SIDGEN is found in the C:\Program Files\Altiris\Aclient Directory. Delete after the first boot up of the computer.
	Rename computer	Rename the computer to its specific State ID Tag.
	Install Altiris	See step 72 for instructions.
	Join computer to BA Domain	Join the computer to the DEPT domain. Right Click <Computer> Select properties. <Select> change. Under "member of" menu, <select> Domain. Type "BA.SDSU.EDU" Enter your domain user name and password. <OK> | <OK>. Restart computer.

Appendix G: 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.

		Windows 2003 Server Configuration-Standardized Checklist & Procedure	
		Configuration #2	**As of : xx/xx/2007**
This config checklist is to be signed by server admin and put in the server audit binder.			
Note: When communicating on contents, please refer to the **ITEM #**'s in first **column.**			
Item #		**TO DO ITEM & Details**	**Add'l Info**
1	**Inventory**	If the Server is new, give a PO-invoice copy to Department Mgr for inventory & tagging	
2	**Vendor Image**	If server is new, use Altiris to create image of drive for possible emergency restoral	
3	**DNS Register**	Process DNS Registration request	
4	**IP**	Request IP from Bids IP Database.	
5	**Start OS installation**	Boot from the Windows 2003 CD and format Drive	Do a reformat as NTFS whether old or new drive
	Network settings #1	**Done during OS installation wizard:**	
6		Under TCP/IP properties, configure network IP	Designate 130.191.1.1 & 200.1 as DNS servers
7		Click on >Advanced > DNS Tab	For “Append these DNS suffixes:..” add “sdsu.edu” entry
8		Add “sdsu.edu” in “DNS suffix for this connection”	Clear (deselect):”Register this connection’s addresses in DNS”
9		Join dept.sdsu.edu domain using your individual domain admin account as authority	
10		Company & Organization = SDSU & DEPT	Computer name = Property tag # or C-series tag #
		Using login as local Administrator:	
11	**Service Pack**	Install the latest Service packs	
12	**Local Accts**	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

13		Create local admin accounts. One primary account (renamed upon joining DEPT domain). One backup account.	Use local account logons minimally. Use local login in event of severance from domain & to rejoin domain, domain login lock out or disablement of primary accounts.
14		Disable the built-in "guest" account & assure it was renamed "guest123" by domain policy; if not, rename manually	
15			
16	**Display & Screen Saver**	Display Properties > set Screen area to 1024 x 768	
17		For local admin profiles set Screen saver to Logon Screen Saver > Wait: 5 min >select "Password Protected"	For servers, the typical condition should be a Logged out status.
18	**Network settings #2**	Local Area Connection properties = select “Show icon in taskbar when connected” so that network speed displays in sys-tray	
19	**Security Patches & Polices**	Start > Run > secpol.msc Account Policies > Minimum password length = 8 characters; enable "Passwords must meet complexity requirements"	The need to perform these steps may be superceded by a Global Domain policy.
20		Start > Run > secpol.msc Local Policies > Audit Policy > Audit account logon events > “Audit these attempts” select “Failure” & "Success"	
21		Start > Run > secpol.msc Local Policies > Security Options > Additional restrictions for anonymous > select “Do not allow enumeration of SAM accounts and shares”	
22		Start > Run > secpol.msc Local Policies > Security Options > Interactive login: Do not display last user name	
23		Control Panels: enable Auto Update by selecting "Keep my computer up to date." and Notify me but don't automatically download or install them	
24	**NTFS Security Settings**	Do not modify any object’s security settings	
25	**Shares**	Record any, all created shares for server adminstration:	
26	**Services**	Record any disabled/stopped services:	
27	**Printing**	Create standard TCP/IP Port for assigned printer	
	Software	**Server Standard Programs: Install from \\Server1\Install Shortcuts**	
28		McAfee 8.X, plus ePO	Verify current status of DAT & Scan Engine
29		Browser IE; current version plus all security patches	
30		Adobe Acrobat, current version	
31		WinZip 7 (Start with WinZip Classic)	
32		NovaNET: if backup of server is required, please submit request to NN sysadmin with	
33	**Product Software**	Install the primary applications for the server's purpose. Record software installed:	
	a	Certain software is disallowed due to security vulnerabilities. Consult SDSU AUP for list.	
	b	Use of remote access software such as VNC and PC-Anywhere must be approved by	

	Configure	**Configurations Using admin2 logon profile:**	
34	**Windows Explorer view settings**	Folder display: View > Details Tools > Folder Options > Use Windows classic folders > Apply; View >Advanced Settings	Select: Display compressed files and folders with alternate color
35		Display the full path in the address bar; Show hidden files and folders; Display the full path in title bar	Deselect "Hide file extensions of known file types" > Apply > Like Current Folder > Yes > OK
36		Launch IE to configure without creating an e-mail account, with no selection for proxy server, and make sdsu.edu the home page	If server is an upgrade of a prior server, remember to save & import existing useful IE Favorites
37		Go to Add/Remove > Windows components to remove Outlook	Delete Outlook shortcuts & extra unused icons
38		Right-click Task Bar & clear "Use Personalized Menus"	
		Server Rebuild	
39		If server administrator determines a rebuild of the server or/and 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 H: 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 set up 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;* and 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)

Attack6: *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 by pass the amalgamated collection of controls

Attack7: *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

Attack8: *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

Attack9: *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

Attack10: *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:

Attack1: *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

Attack2: *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

Attack3: *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

Attack4: *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

Attack5: *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

Attack6: *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

Attack7: *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

Attack8: *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

Attack9: *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

Attack10: *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 loin 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 H

Appendix I: 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.

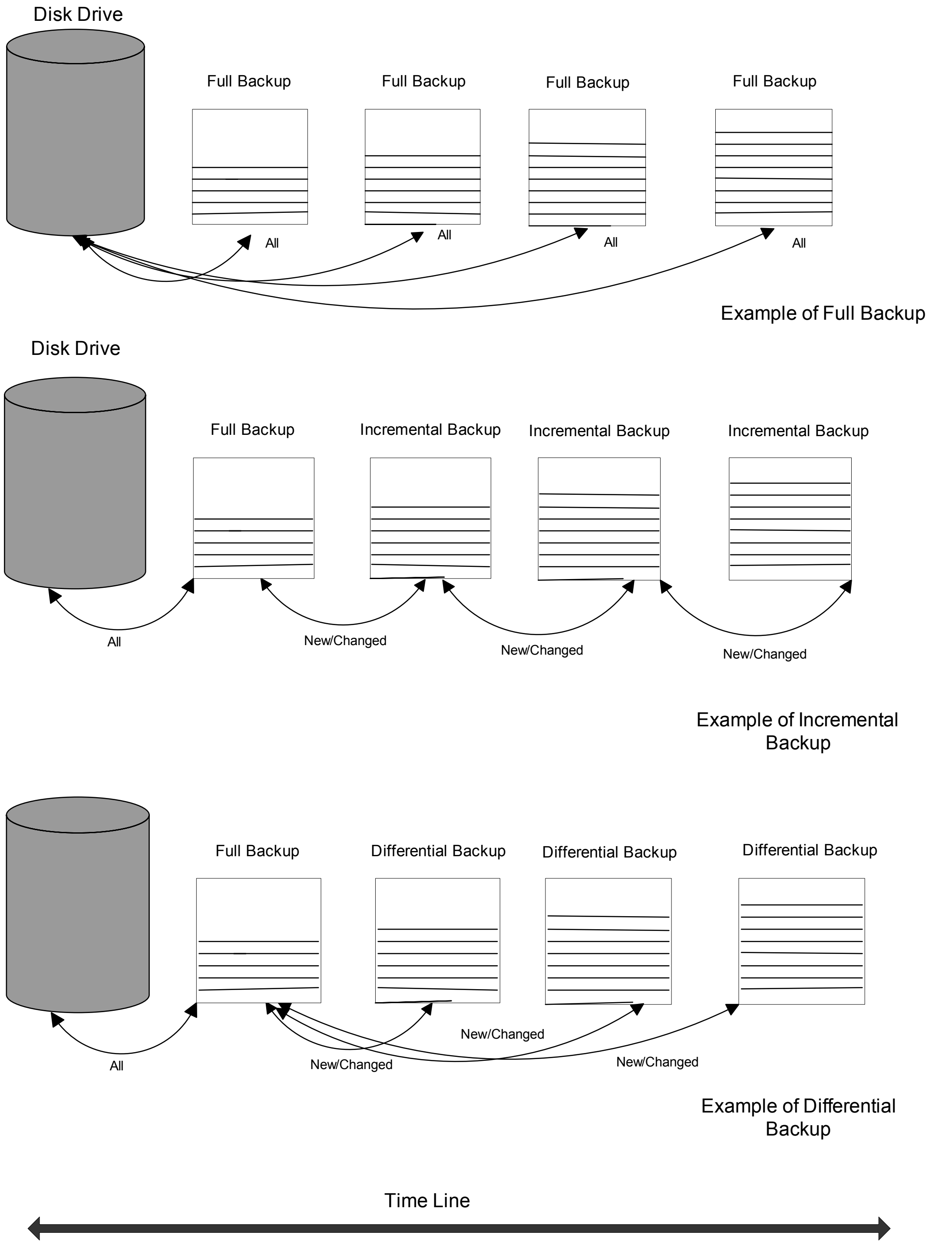


Figure 1: Comparing Backup Strategies

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.
- 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, earth quake or flood. Users typically require restoration of files recently backed up. So, one recommendation is to keep the most current set of backups onsite[28] 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.

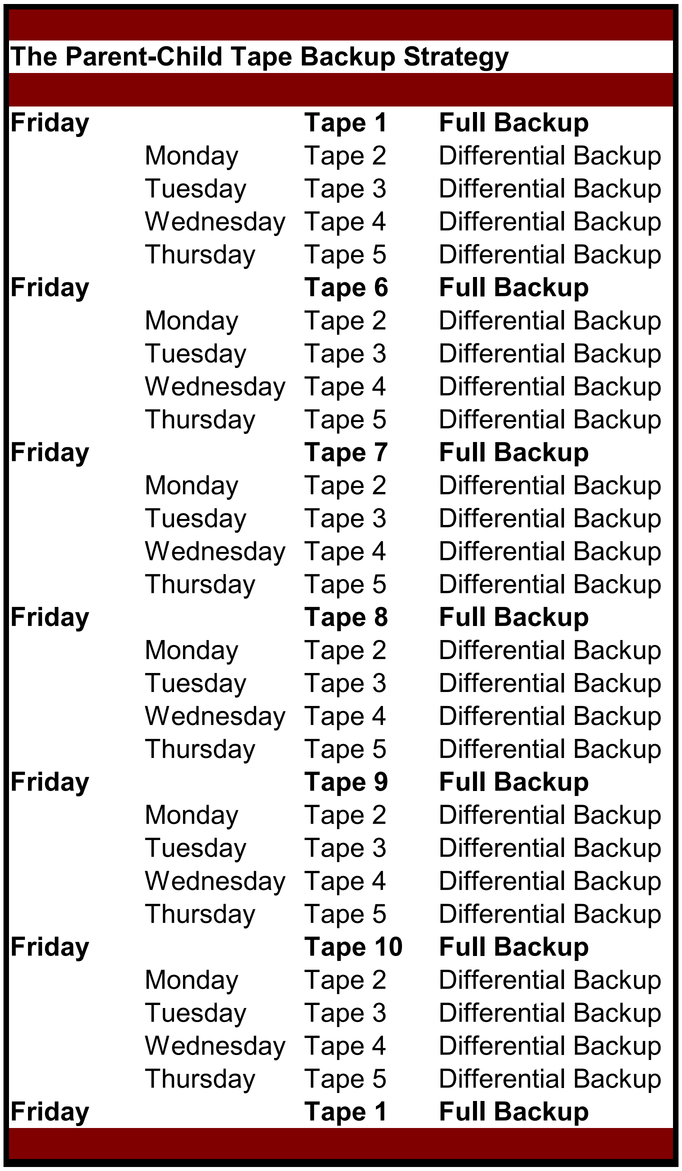
[28] Backups kept onsite should be stored in a fire proof safe for media protection

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

Friday		**Tape 1**	**Full Backup**
	Monday	Tape 2	Differential Backup
	Tuesday	Tape 3	Differential Backup
	Wednesday	Tape 4	Differential Backup
	Thursday	Tape 5	Differential Backup
Friday		**Tape 6**	**Full Backup**
	Monday	Tape 2	Differential Backup
	Tuesday	Tape 3	Differential Backup
	Wednesday	Tape 4	Differential Backup
	Thursday	Tape 5	Differential Backup
Friday		**Tape 7**	**Full Backup**
	Monday	Tape 2	Differential Backup
	Tuesday	Tape 3	Differential Backup
	Wednesday	Tape 4	Differential Backup
	Thursday	Tape 5	Differential Backup
Friday		**Tape 8**	**Full Backup**
	Monday	Tape 2	Differential Backup
	Tuesday	Tape 3	Differential Backup
	Wednesday	Tape 4	Differential Backup
	Thursday	Tape 5	Differential Backup
Friday		**Tape 9**	**Full Backup**
	Monday	Tape 2	Differential Backup
	Tuesday	Tape 3	Differential Backup
	Wednesday	Tape 4	Differential Backup
	Thursday	Tape 5	Differential Backup
Friday		**Tape 10**	**Full Backup**
	Monday	Tape 2	Differential Backup
	Tuesday	Tape 3	Differential Backup
	Wednesday	Tape 4	Differential Backup
	Thursday	Tape 5	Differential Backup
Friday		**Tape 1**	**Full Backup**

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.

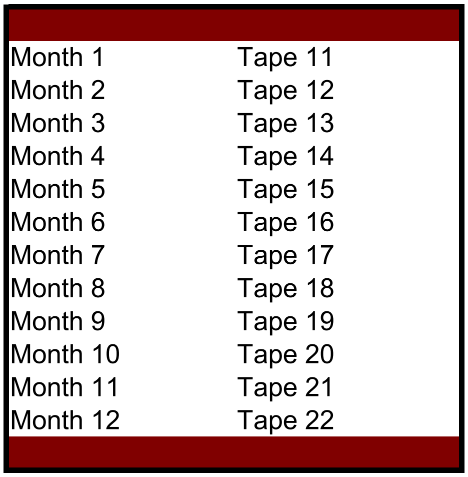
]

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.

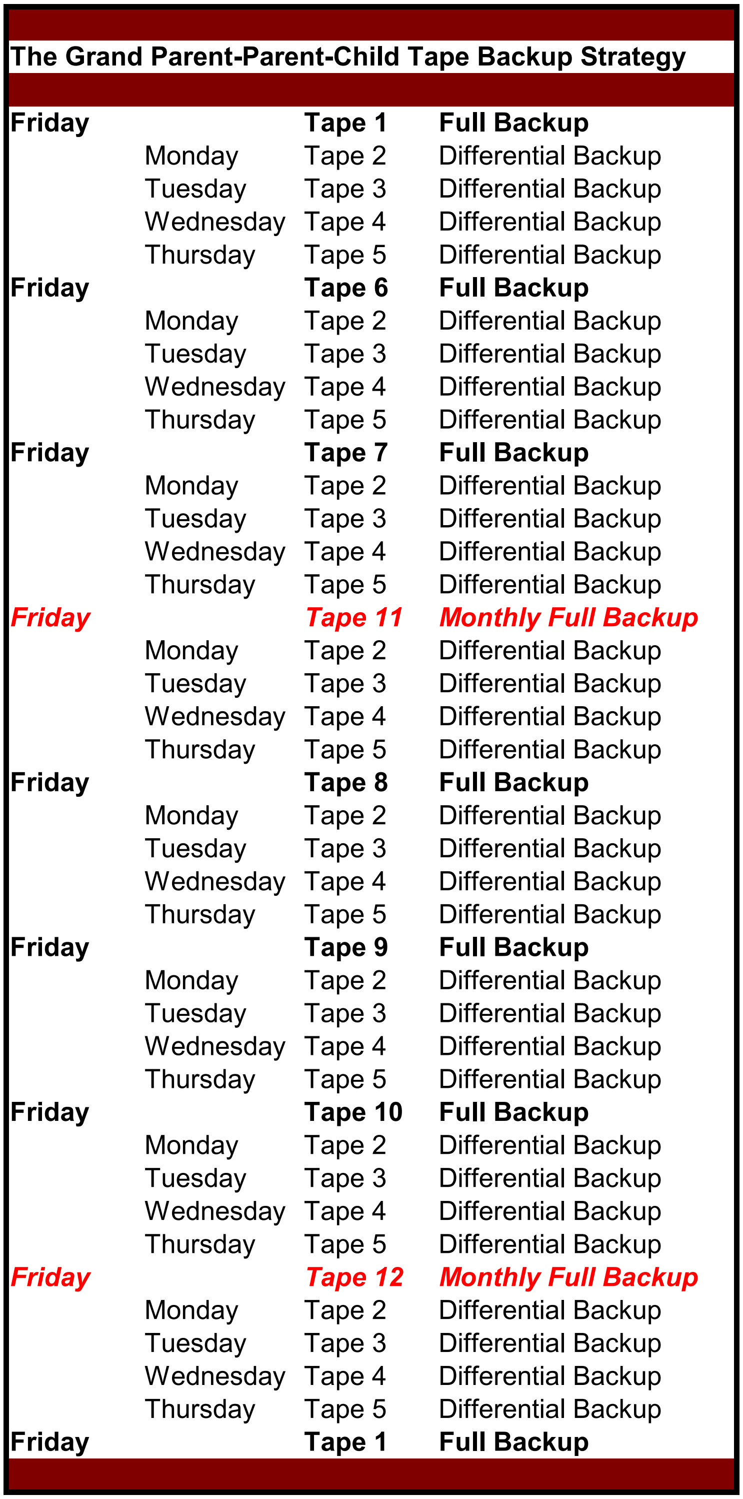
However, there are 12 additional tapes which are used for monthly full backups. These 12 tapes will be kept indefinitely, will not be reused, and should be stored at an appropriate off-site location.

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.



Month 1	Tape 11
Month 2	Tape 12
Month 3	Tape 13
Month 4	Tape 14
Month 5	Tape 15
Month 6	Tape 16
Month 7	Tape 17
Month 8	Tape 18
Month 9	Tape 19
Month 10	Tape 20
Month 11	Tape 21
Month 12	Tape 22

Figure 3: Tape Usage in the Grand Parent-Parent-Child Tape Backup Strategy



The Grand Parent-Parent-Child Tape Backup Strategy			
Friday		**Tape 1**	**Full Backup**
	Monday	Tape 2	Differential Backup
	Tuesday	Tape 3	Differential Backup
	Wednesday	Tape 4	Differential Backup
	Thursday	Tape 5	Differential Backup
Friday		**Tape 6**	**Full Backup**
	Monday	Tape 2	Differential Backup
	Tuesday	Tape 3	Differential Backup
	Wednesday	Tape 4	Differential Backup
	Thursday	Tape 5	Differential Backup
Friday		**Tape 7**	**Full Backup**
	Monday	Tape 2	Differential Backup
	Tuesday	Tape 3	Differential Backup
	Wednesday	Tape 4	Differential Backup
	Thursday	Tape 5	Differential Backup
Friday		***Tape 11***	***Monthly Full Backup***
	Monday	Tape 2	Differential Backup
	Tuesday	Tape 3	Differential Backup
	Wednesday	Tape 4	Differential Backup
	Thursday	Tape 5	Differential Backup
Friday		**Tape 8**	**Full Backup**
	Monday	Tape 2	Differential Backup
	Tuesday	Tape 3	Differential Backup
	Wednesday	Tape 4	Differential Backup
	Thursday	Tape 5	Differential Backup
Friday		**Tape 9**	**Full Backup**
	Monday	Tape 2	Differential Backup
	Tuesday	Tape 3	Differential Backup
	Wednesday	Tape 4	Differential Backup
	Thursday	Tape 5	Differential Backup
Friday		**Tape 10**	**Full Backup**
	Monday	Tape 2	Differential Backup
	Tuesday	Tape 3	Differential Backup
	Wednesday	Tape 4	Differential Backup
	Thursday	Tape 5	Differential Backup
Friday		***Tape 12***	***Monthly Full Backup***
	Monday	Tape 2	Differential Backup
	Tuesday	Tape 3	Differential Backup
	Wednesday	Tape 4	Differential Backup
	Thursday	Tape 5	Differential Backup
Friday		**Tape 1**	**Full Backup**

Figure 4: The Grand Parent-Parent-Child Tape Backup Strategy

Appendix J: 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 fays 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.

In database systems, the use of encryption can cause serious performance issues if most or the entire database is encrypted. A better strategy is to encrypt only those parts of the database that contain protected information. This approach is sometimes referred to as columnar encryption.

Requirements for Strong Encryption of Protected Information

As a good rule of thumb, protected information should use the following FIPS-approved cryptographic algorithms[29]:

Algorithm	Type	Key Sizes (bits)	FIPS Documents
AES	Symmetric	128, 192, 256	FIPS 197
3DES	Symmetric	168	FIPS 46-3 & 81
DSA	Asymmetric	1024	FIPS 186-2
RSA	Asymmetric	1024 or higher (2048 rec.)	FIPS 186-2
ECDSA	Asymmetric	160 or higher	FIPS 186-2
SHA	Hashing	160 (SHA-1), 224, 256, 384 512	FIPS 180-2

[29] http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

Appendix K: 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 2.11 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 L: References

1. San Diego State University Computing Security Policy 11/7/2000, http://security.sdsu.edu/policy/security-policy.html

2. Guide to Secure Web Services (NIST Draft SP 800-95), Computer Security Resource Center, National Institute of Standards and Technology, http://csrc.nist.gov/publications/drafts/Draft-SP800-95.pdf

3. Creating a Patch and Vulnerability Management Program (NIST SP 800-40), Computer Security Resource Center, National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf

4. SANS Institute, SANS Top-20 Internet Security Attack Targets (2006 Annual Update), http://www.sans.org/top20/

5. Web Application Break-In, Information Security Magazine, August 2006, http://informationsecurity.techtarget.com/magLogin/1,291245,sid42_gci1206289,00.html

6. The Ten Most Critical Web Application Security Vulnerabilities, Open Web Application Security Project (OWASP), January 2004, http://superb-east.dl.sourceforge.net/sourceforge/owasp/OWASPTopTen2004.pdf

7. Auditing Web Site Authentication, Security Focus, April 2003, http://www.securityfocus.com/infocus/1688

8. Web Application Security, Information Systems Control Journal, November 2002, http://www.isaca.org/Template.cfm?Section=Archives&CONTENTID=16173&TEMPLATE=/ContentManagement/ContentDisplay.cfm

9. Top 10 Web 2.0 attack vectors, Net Square Solutions, October 2006, http://net-square.com/whitepapers/Top10_Web2.0_AV.pdf

10. Application Security by Design, Security Innovation, February 2006, http://www.securityinnovation.com/download.asp?template=whitepaper.html&product=pdf/Application%20Security%20by%20Design.pdf

11. VirusScan Enterprise 8.0i Best Practices Guide, McAfee Security, August 2004, https://mysupport.mcafee.com/eservice_enu/default.htmstart.swe?SWECmd=Start&SWEHo=mysupport.mcafee.com

12. Early Remediation Makes Most Cost Effective Security, Software Vulnerability Risk Management Newsletter, Ounce Labs Inc., http://www.ouncelabs.com/early.html

13. Damage Control, C-Net News, February 2003, http://news.com.com/2009-1001-983540.html

14. Guidelines for Media Sanitization, NIST Special Publication 800-88, http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf

Appendix M: Version Review Log

Vulnerability Management Program Version Review Log

Version	**Date Completed**	**Reviewed By**
Version 1.0	December 13th 2006	ISO and ISP
Version 1.1	July 12th 2007	CIO and IT Security Office
Version 1.2		AA IT Coordinator, SA IS Manager, Senate IIT Committee Chair, IT Support Expert, Auxillaries, IT Managers, NAC-Security, IACC, Senate IIT, MWSSLS, System Administrators
Version 1.3		President