MEMORANDUM

TO: SDSU Faculty and Staff
FROM: Stephen L. Weber, President
Re: Computing Resources

February 26, 2007

I am writing to ensure that we all have a clear understanding of the obligation we and San Diego State University have to protect our computing resources, including confidential information. Let me summarize the activities that have been and will be undertaken to meet those obligations, and the consequences should an individual or department fail to meet those obligations.

Multiple federal and state laws, as well as policies of the California State University, require that confidential or personal information be protected. The definition of what is information to be protected varies by the particular law or policy, but this generally includes records that pertain to personal identity, financial or health information, and/or student grades and similar data. Examples include: Social Security numbers, grades, dates of birth, patient medical records, and driver's license and credit card information. In addition to imposed legal and policy obligations, we also have a fiduciary duty to protect the information entrusted to us by our colleagues, our students, our alumni, and others of our campus community. Most of all, it is the right thing to do.

There is no single technology that can protect information. The only effective approach involves multiple layers of protective action, aided by technology. Security practices are being incorporated into a comprehensive campus information security plan.

As university employees, we all share in the responsibility to be familiar with, and abide by, existing campus policies and procedures concerning information security. These can be found at http://security.sdsu.edu/policy/. References to applicable federal and state laws can be found at the same site, including appropriate use of state resources.

We are each responsible to securely manage and use technology, including desktop or portable computers, servers, wireless devices, or portable storage media such as flash drives. Secure management means availing ourselves of the technical direction of departmental IT staff to ensure that machines are always secured with the latest patches and protective software. Secure use of technology requires that employees are aware of risks inherent with computing in a shared environment, including Internet browsing and email communications. Adherence to SDSU's Computing Acceptable Use Policy http://security.sdsu.edu/policy/aup.html reduces exposure to these risks.
In furtherance of our continuing efforts to maximize good security practices, a number of actions are underway:

- **Completion of the detailed campus information security plan**, which is a manual for management and technical IT support staff across campus. The first completed section of the plan, concentrating on how to respond to a security incident, can be found at [http://security.sdsu.edu/policy/SIRP.pdf](http://security.sdsu.edu/policy/SIRP.pdf). Other sections include the Vulnerability Management Program, the Security Awareness and Training Program, and the Disaster Recovery and Business Continuity Program, which we expect to complete by July 2007.

- **Completion of the network infrastructure build-out**, scheduled for April 2007. Concurrent with this build-out, unauthorized routers and hubs will be removed from the network while providing improved service to our campus community.

- **Enhancement of our network protection system** that will only allow pre-approved traffic to access our computing resources. This will greatly reduce the possibility of unauthorized access to our systems, reducing the risk of possible damage to our resources or access to valuable and confidential information. The first phase will be the installation of additional network firewalls in February 2007. This will be followed in the spring with additional hardware and software systems in support of the California State University Chancellor's Office security improvement project.

- **An increase in network and system scans, surveys, and other activities** to assess the campus's vulnerability to security attacks and to identify mitigating measures.

It is essential that each of us cooperate with the Information Technology Security Office and other University IT staff assigned to manage and secure the network, systems, and information. Because we all share the same network, violations of policy and good practice by one individual endanger all of us, including those individuals whose confidential information is entrusted to us. Failure to follow policies and/or violation of applicable laws involves consequences that range from loss of connection to the campus network and disciplinary proceedings, to possible criminal or civil actions and the requirement for the relevant campus department and division to bear the costs associated with security breach.

In summary, no part of our fast-changing world is moving more quickly than information technology. To give you a sense of the realities we face, we are now averaging over one million attempts per hour to probe and attack our systems. We each share the same professional responsibility in managing our students' information as well as in caring for our own information.

SLW:jnt