Colorado State University Information Technology (IT) Security Policy
Version 1.3 Approved by ITEC February 15, 2005

Introduction

Colorado State University collects information of a sensitive nature to facilitate and enable its business/academic functions. Unauthorized access to such information may have many severe negative consequences, including adversely affecting the reputation of the University. Protection of such personally identifiable information from unauthorized access is required by various private sector, federal and state mandates, including among others the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), the Family Educational Rights and Privacy Act (FERPA), and the Payment Card Industry Data Security Standard. Sensitive information is stored on a variety of computer systems in the decentralized information technology (IT) environment at the University. As such systems are being subjected to increasing numbers and types of attempted unauthorized access, the adoption of these IT security policies will aid in the protection of such information.

Computers not containing sensitive information are also risk factors for the University and should be managed as such. Computer hackers are always searching for computers to compromise, whether or not sensitive information exists on their local storage devices. Possible consequences of improper security precautions include identity theft, the installation of remote administration utilities capable of monitoring key strokes as users authenticate into other computers and services, adding or deleting files, and using the computer to distribute copyrighted material without authorization. Indeed, there is even a black market for selling access to compromised computers for use in activities such as distributed denial of service attacks.

Therefore, the following IT security policies are adopted and put into place. The Associate Vice President for Information and Instructional Technology (AVPIIT) shall be responsible for overseeing the implementation and use of these policies beginning on the effective date of this document.

Definitions

Application is a computer software program run on a computer for the purpose of providing a business/academic function.

Computer server systems (Servers) are computers accessed by multiple individuals and/or computers.

Local Area Network (LAN) is an internal network within an institution, e.g. at Colorado State University.

Personal computers are comprised of desktops, laptops, tablets, personal digital assistants and other such devices of all brands, used principally by one individual at a time. This category includes laboratory computers.

Sensitive information includes social security numbers, personally identifiable health information, personally identifiable financial information including credit card information, personnel employment and student performance information, proprietary research and academic information, and any other information that through disclosure would adversely affect an individual or besmirch the reputation of the University.

Service – A server application offering specific functionality, typically to users over a network. Examples include web, email, and remote file access.

Virtual Private Network (VPN) is a mechanism for encrypting the information sent from an individual computer to a VPN concentrator that typically exists in a "secure" network location. Alternatively, VPN's may be implemented between subnetworks (subnets) to encrypt all of the traffic flowing between the subnets, in other words from LAN to WAN to LAN. User authentication is an important element of a VPN in either scenario.

Wide Area Network (WAN) is an external network that provides connectivity among LANs.

Other Resources

The Campus IT Security web page (see http://www.colostate.edu/services/acns/itsecurity.html) provides a variety of information regarding IT security that is useful in the implementation of these policies. Also, for credit cards, see https://sdp.mastercardintl.com/pdf/PCD_Manual.pdf.

CSU's IT Security policies are presented hereinafter in three separate sections. Section I contains general policies and guidelines that pertain to the University's overall IT environment, and are the responsibility of the department owning the IT environment. These general policies and guidelines are to be applied in varying degrees balancing risk, cost and access. As general policies, these are intended to be enduring. Section II contains mandatory, minimum IT security policies that are to be applied to every CSU IT system. These specific policies are intended to evolve over time to adjust to current threat levels, and as such, are more volatile than the general policies and guidelines in Section I. These mandatory, minimum IT security policies shall be reviewed and updated on at least an annual basis, and more frequently should the need arise, for example if significant new IT threats emerge that compromise IT security and that are not covered by the current specific policies. Section III pertains to specific requirements to protect credit card information, as mandated by the credit card industry.

Section I General IT Security Policies and Guidelines

Applicability

These policies encompass best practices that are in general to be applied comprehensively in the University's IT environment. However, common sense judgment is to be used in their application. For example, where extreme cost or impairment of business/academic functions would result from the immediate application of all elements of these policies, such as requiring an expensive upgrade to central administrative systems, these policies need not be immediately or comprehensively be put into effect. Instead, as systems are upgraded, they shall be brought into compliance, to the degree practicable, with these policies. Prudence dictates that those policies that can be effectively implemented without severely impeding the University's business/academic functions shall be implemented in the course of normal operations.

IT Security Policies

1. Servers

Servers that contain sensitive information are subject to the policies of this section. It is recommended, however, that all servers at the University are brought into compliance with these policies. Personal computers are covered by the policies in the next section. Departments owning the servers are responsible for ensuring that their servers containing sensitive information are secured in

accordance with these policies. Guidelines and 'best practices' for securing Windows servers on campus are available at: http://www.colostate.edu/services/acns/itsecurity.html. Servers shall be protected as follows:

1. Such servers shall be housed in a physically secure facility where access is limited to only those individuals requiring access to perform routine or emergency maintenance on the system.
2. To the degree practicable, only operating systems and applications that provide high levels of security shall be used, and security updates (patches) shall be applied in a timely manner.
3. Server-side computer virus protection should be implemented and kept up to date.
4. Services and applications installed/enabled shall be the minimum necessary to accomplish the required business and/or academic functions. Such services and applications shall be reviewed periodically for conformance with this aspect of the policy.
5. Network traffic shall be limited to only those services and ports considered essential, unless exceptions to allow access to required services are requested and granted. Periodically, such exceptions shall be reviewed to be in conformance with this aspect of the policy.
6. In cases where computers are dedicated to specialized applications and cannot be brought into compliance with these policies, particularly with regard to minimum operating system versions, efforts shall be made to isolate the system from the campus environment using a private address and/or a hardware firewall.
7. Individual access shall be limited to only those needing access for legitimate business/academic purposes. Periodically, individual access shall be reviewed to be in conformance with this aspect of the policy.
8. The amount of sensitive information collected and stored shall be the minimum amount required for the efficient and effective conduct of business and academic functions. In particular, sensitive information that is old and not needed in the normal course of academic/business operations should be removed and archived elsewhere, e.g. on tape, CD-ROM or DVD-ROM.
9. Reasonable and prudent efforts shall be made to isolate sensitive data from open access, for example on a separate back-end database server accessible only from a front-end web server that has been diligently protected.
10. To the degree practicable, only secure connections and file transfers shall be allowed, for example by using secure web protocols (https), secure connections (e.g. ssl and ssh), and other secure mechanisms for connections. This policy is particularly relevant when allowing access from external (non-CSU) networks.
11. Server files shall be backed up on a regular schedule, and off-site storage of back-ups in a secure location shall be performed on a regular schedule. (Although this policy may appear to be more applicable to business/academic continuity, sometimes malicious computer hackers obtain unauthorized access to systems and corrupt the information on the system, making this an IT security issue.) ACNS offers secure, off-site storage to interested parties.
12. Where the server contains especially sensitive information that merits an additional measure of protection, either due to the quantity of sensitive information or information of an exceptionally sensitive nature, the integrity of systems logs should be preserved, for example by mirroring system logs on other servers, so that in the event of unauthorized access, analysis and traceback can be accomplished.

13. Such servers shall be registered with ACNS and scanned for vulnerabilities on a regular schedule. Vulnerabilities detected shall be addressed in a timely manner.
14. Contact information for system administrators of such servers shall be communicated to ACNS and kept up to date. This information shall include name, office telephone number, email address, and home, pager and cellular telephone numbers.
15. To prevent the inadvertent release of sensitive information stored on hard drives, all drives must be sanitized to a minimum of Department of Defense (DoD) 5220.22-M standards prior to release to Surplus Property or other agencies. The University has acquired site licensing for disk sanitization software for Windows and has determined that one pass of the software (the software writes multiple times per pass) is adequate protection. Other utilities meeting the DoD minimum standard may be used if desired. If hard drives arrive at Surplus Property without having been sanitized, Surplus Property will sanitize the drive and charge a nominal fee for this service.

2. Personal Computers

Personal computers as defined above shall be protected in accordance with a balance between the risks of not protecting them, the cost (effort and expense) of protecting them, and the required functionality (for example, sometimes specialized personal computers are required to meet research objectives and cannot and sometimes should not be protected at the same level as general purpose computers). Departments owning the personal computers are responsible for ensuring that their personal computers either containing or used to access sensitive information are secured in accordance with these policies. It is recommended, however, that all personal computers at the University are brought into compliance. Guidelines and 'best practices' for securing Windows desktops on campus are available at: http://www.colostate.edu/services/acns/itsecurity.html. In general, personal computers are subject to the following policies:

1. Only operating systems and applications that provide high levels of security shall be used, and security updates (patches) shall be applied in a timely manner.
2. Computer virus protection shall be implemented and kept up to date. This is especially the case for remote computers that are not owned or operated by the University, for example personal, at-home computers (note that the University has contracted for anti-virus software that may be installed at no additional cost on personally owned computers).
3. Services and applications offered shall be the minimum necessary to accomplish the desired business/academic functions.
4. Network traffic shall be limited to only those services and ports considered essential and required for legitimate business/academic purposes.
5. Access to campus resources from remote personal computers via external providers (such as Comcast, Qwest, hotel networks, or any wireless network), shall be secure, e.g. encrypted over a VPN connection terminated on the University's VPN concentrator.
6. To prevent the inadvertent release of sensitive information stored on hard drives, all drives must be sanitized to a minimum of Department of Defense (DoD) 5220.22-M standards prior to release to Surplus Property, release to other agencies, or disposal. The University has acquired a site license for disk sanitization software for Windows and has determined that one pass of rewriting the drive is adequate protection. Other utilities meeting the DoD minimum standard may be used if desired. If hard drives arrive at Surplus Property without having been sanitized, Surplus Property will sanitize the drive and charge a nominal fee.
7. The amount of sensitive information collected and stored shall be the minimum amount required for the efficient and effective conduct of business and academic functions. In particular, sensitive information that is old and not needed in the normal course of

academic/business operations should be removed and archived elsewhere, e.g. on tape, CD-ROM or DVD-ROM.

3. Network Security

The campus network is critical for the conduct of university business and instructional functions, and its integrity is dependent upon proper IT security implemented on all users' computers. IT support personnel and all users should be both familiar and compliant with the University's acceptable use policy for computing and network resources: http://www.colostate.edu/Services/acns/aup.html.

The best security model addresses vulnerabilities at multiple levels, a concept known as "defense in depth". This document focuses primarily on securing systems, via virus protection, application and operating system patch management, passwords, etc. ACNS strives to secure the central network infrastructure to the extent possible, though colleges and departments are responsible for maintaining their LANs. ACNS networking staff is available to assist IT managers with evaluating their current networking environment and will recommend solutions for improving security at the network level.

4. Passwords

Strong passwords that are difficult for others to obtain shall be employed as permitted by the operating system and/or application. Prudent measures are to be used to ensure that strong passwords are employed by the user. This is especially so for administrative accounts. Periodic password refresh (resetting) shall be encouraged, consistent with the scope of administrative access to systems and access to sensitive information.

A strong password often makes sense only to its owner, as opposed to a recognized word or concatenation of words. One common means of creating such a password is to take the first or last letter of a phrase, perhaps adding or substituting special characters. For example, the phrase "Peas porridge in the pot nine days old" could generate the password "Ppi+p9d0".

5. Files and File Storage

In general, users are responsible for their own files, including the information contained in those files and ensuring that files containing critical data are backed up and/or stored in multiple locations. Sensitive data in individual's files should be kept to a minimum, and reasonable and prudent protection of those files shall be implemented by the system administrator. In particular, sensitive information that is old and not needed in the normal course of academic/business operations should be removed and archived elsewhere, e.g. on tape, CD-ROM or DVD-ROM.

It is the responsibility of the owner of files containing sensitive data that are transmitted via the network to ensure that the files are reasonably protected against unauthorized access. Common measures that may be taken for files transmitted across unsecured networks are encryption of the files or establishing an encrypted network connection between the endpoints.

6. Personally-owned Computers

Personally-owned computers that routinely use University IT resources, including access to University networks, servers and/or other IT resources, and/or that contain sensitive University information are subject to the same policies as those computers owned and operated by the University.

7. Wireless Networks

In buildings where the central wireless network has been installed, wireless access points managed by individuals or departments are not permitted. Access to wireless networks shall not be via clear text, but instead all transmissions shall be encrypted so as not to be accessed or easily decoded by others. The administrator of the wireless access point is responsible for reasonably ensuring that unauthorized access to traffic will not be possible, for example through the implementation of encryption methods that are judged to be robust relative to the current state of the art. The department responsible for administration of the local network shall be responsible for authorizing all wireless access points on the local network, and all wireless access points shall be reported to ACNS to facilitate monitoring and operations of the network, especially in cases of IT security incidents. Unauthorized wireless access points shall not be installed on the University's LAN.

8. Primary Identifiers

To the extent possible, social security numbers (SSNs) shall not be used as the primary numeric identifier for individuals. The central electronic identity (eID), the University identifier (UID), or a similar identification mechanism shall be used for access to University computer systems. This particular policy applies to all forms of information, both electronic and non-electronic, including identification cards.

9. Communications Rooms

Communications rooms housing telephone networks, data networks, servers, security systems including surveillance, alarm and card access systems, and other similar electronic devices and systems shall be physically secure, and access shall be limited only to those personnel directly responsible for operating and maintaining those systems. Any additions to hardware in communications rooms (other than replacement of existing hardware) must be authorized by the AVPIIT. Authorization forms for this can be obtained from the office of the AVPIIT.

Responses to IT Security Incidents

IT security incidents should be immediately reported to Academic Computing and Networking Services (ACNS). ACNS may assemble an IT security response team after becoming aware of IT security incidents. This response team will generally be comprised of 1) the director of ACNS or designee, 2) appropriate technical staff from ACNS and from the affected department(s), and 3) administrative staff from the affected department(s). All personnel so engaged should be prepared to devote the needed time and effort to dealing with the incident from the time the incident is identified until the incident is resolved or otherwise as agreed upon by the team.

The timeliness and extent of responses to IT security incidents should in general be proportionate to the risk associated with the incident. For example, where the incident involves a large quantity of sensitive data, the incident involves data of a highly sensitive nature, or the activity may be illegal, a timely and significant response should ensue.

In the event of an incident, the following general procedure should be followed:

1. ACNS should be contacted by departmental staff. This may be done during off hours by calling the ACNS trouble number 970.491.7443. During business hours, ACNS should be available by calling 970.491.5133. The responsible administrator(s) in the affected department(s) should be contacted and brought into discussions.
2. ACNS will assign staff to the incident. An incident response team may be formed, at the discretion of ACNS. ACNS, in consultation with departmental staff, shall decide upon a

response proportionate to the incident. Should there not be agreement in how to respond, the Director of ACNS shall determine the response.

3. Should it be appropriate, ACNS will contact CSU Legal Counsel for their advice. This may involve contacting law enforcement, but this shall be done only by ACNS, and only after CSU Legal Counsel have been consulted.
4. No information regarding the incident should be released unless authorized by CSU Legal Counsel. Information should only be released through ACNS who shall coordinate such release with CSU Legal Counsel.
5. In general, the affected computer(s) should be disconnected from the network but not turned off, or rebooted. Also, no modifications should be made to the systems until ACNS staff and departmental staff have agreed upon a set of appropriate next steps.

Section II Mandatory, Minimum IT Security Requirements

The requirements in this section are mandatory, minimum requirements that shall be implemented on all IT systems associated with the University. This includes University-owned devices and personally-owned devices that interact with University systems, even if only by a physical means such as sharing removable media such as floppy disks, CD's, DVD's or other storage devices. If it is not possible or practicable to meet these requirements, the responsible department may petition ACNS for an exception to these requirements. The form for applying for an exception may be found on ACNS' web page dealing with IT security http://www.colostate.edu/Services/acns/itsecurity.html.

1. Operating Systems

Only operating systems that are secure according to current best practices and require strong authentication shall be used. In particular, only Windows 2000 or later Windows operating systems shall be used. If an older Windows operating system is required, an exception must be applied for. Security patches and updates shall be applied in a timely manner. Where possible, updates shall be automatically applied to both operating systems and applications.

2. Network Security

Following recommendations from the Campus IT Security Technical Advisory Committee, with input from the campus IT community, all incoming connections from the Internet will be blocked by default. Exceptions to this policy may be requested by contacting ACNS, for example to allow inbound mail connections to departmental mail servers or access to designated web servers. By blocking the large volume of malicious connection attempts, the University's IT security environment is greatly enhanced.

ACNS networking staff have the authority to take appropriate action when the University's acceptable use policy (http://www.colostate.edu/Services/acns/aup.html) has been violated, or as otherwise required to maintain the integrity and functionality of the University's IT environment. This may include, but is not limited to, traffic analysis and disabling access to individual or multiple computers. Reasonable attempts to contact the appropriate IT staff will be made by ACNS staff in such cases.

3. Anti-virus

Where applicable, all client computers shall have the University standard anti-virus software, configured for automatic updates to the virus definition files.

4. Server Registration

All servers containing sensitive information shall be registered with ACNS. There is a registration form on ACNS' web page dealing with IT security. The initial registration and updates thereof shall be coordinated through the subnet managers.

5. Passwords

Strong passwords shall be implemented on all systems. The following are mandatory, minimum requirements that shall be implemented by all users (it is noted that system administrators can reasonably enforce only some of the following rules, and that users bear the ultimate responsibility for compliance):

a. Passwords for general systems shall be at least eight (8) characters in length. Passwords for server administrative access on Windows operating systems shall be a *minimum* of 15 characters.
b. Passwords shall not be derived from a user's name or login ID.
c. Passwords shall not be derived from system-specific information such as hostname, aliases or entries in users' files.
d. Commonly used words or words appearing in either English or foreign language dictionaries shall not be used.

In addition, passwords should follow a minimum rule set for complexity. One such set of rules for password complexity that should be considered (there are others) is that passwords shall conform to at least three (3) of the following conditions:

a. Contain one or more upper case characters
b. Contain one or more lower case characters
c. Contain one or more numerals (0, 1, 2… 9)
d. Contain one or more special characters (non-alphabetic and non-numeric e.g., punctuation symbols or any of #, $, %, ^, &, *)

Finally, use of the same administrative or "root" password across administrative boundaries is prohibited. For example, system administrators should select an administrative password for configuring network hardware in their area, another password for administering their Windows servers, and yet another unique root password for unix servers. Separate and distinct passwords shall also be used for units managing more than one Windows domain.

Section III Protection of Credit Card Information

The requirements in this section are mandatory, minimum requirements that shall be implemented on all IT systems that process, store, transfer or transport credit card information. This includes University-owned devices and personally-owned devices that interact with University systems, even if only by a physical means such as sharing removable media such as floppy disks, CD-ROM's, DVD-ROM's or other storage devices. If it is not possible or practicable to meet these requirements, the responsible department may petition Business and Financial Services (B&FS) for an exception to these requirements.

1. Credit Card Information Stored in Non-electronic Form

Credit card information that is stored in non-electronic form is subject to the policies contained in the latest version of the "CSU Personal Records Privacy and Security Policy." In particular, such materials must be stored in secure locations, e.g. behind locked doors, etc.

2. Credit Card Information Stored in Electronic Form

Credit card information that is stored in electronic form, including on non-removable devices (i.e. hard disks) and removable devices (e.g. floppy disks, removable hard disks, CD-ROM, DVD-ROM, etc.) is also subject to the policies contained in the latest version of the "CSU Personal Records Privacy and Security Policy." In particular, such materials must be stored in secure locations, e.g. behind locked doors, etc.

Computers that store credit card information in any form shall not be connected to the campus network.

3. Systems that Support On-line Purchases

The University has reviewed the credit card industry's IT security requirements for on-line processing (see https://sdp.mastercardintl.com/pdf/PCD_Manual.pdf), and determined that the VeriSign Pay Flow Link and the CASHNet eMarket Checkout systems, if implemented properly, will allow the University to be in compliance with the requirements. However, due to limited resources for technical and administrative oversight of these complex systems, the University has standardized on a single solution, the CASHNet eMarket Checkout system. Therefore, systems that process credit cards on-line shall be configured to use the CASHNet eMarket Checkout system, where no credit card information traverses University systems. Rather, after the purchase is initiated, the credit card processing is handed off to the CASHNet system for processing. All that is returned to the University is transaction information containing no personally identifiable credit card information.

Governance of These Policies

The Information Technology Executive Committee (ITEC) is responsible for these policies, including adoption, modification and change. Changes to these policies are to be widely reviewed by the campus, including the University Information Technology Support Services (UITSS) Committee, the Campus IT Security Technical Subcommittee, the General Counsel, and the ITEC Advisory Council (IAC), prior to being taken to ITEC for their final approval.

Questions regarding this policy should be addressed to the Associate Vice President for Information and Instructional Technology, Dr. Patrick J. Burns, Patrick.Burns@ColoState.EDU.