Colorado State University Information Technology (IT) Security Policy

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), Colorado House Bills 03-1175 and 06-1157, 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 Vice President for Information Technology (VPIT) 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/social function.

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

CORA, Colorado Open Records Act – Under CORA, records of state institutions of higher education are generally open for public inspection. However, CORA also provides that inspection may be denied or must be denied, depending upon the circumstances. Information at the University, including e-mail and other electronic documents, may be public records subject to inspection upon request under CORA.

FERPA, Family Educational Rights and Privacy Act. FERPA sets forth certain requirements regarding student records, including the release and access to such records. Under FERPA, “education records” are defined as records that are directly related to a student and are maintained by the institution. Student education records, except public or directory information, typically may not be disclosed without consent.

Comment [L1]: Corrected

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.

Portable media includes all media or portable devices capable of storing data, including memory sticks, CDs, DVDs, PDAs, disk drives, magnetic tapes, iPods, and laptop computers.
Sensitive information includes social security numbers, personally identifiable health information, personally identifiable financial information including credit card information, driver's license information, personnel employment and student performance information, proprietary research and academic information, third-party proprietary information, FERPA-protected non-directory 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.acns.colostate.edu/Security) provides a variety of information regarding IT security that is useful in the implementation of these policies. Also, for credit cards, see https://www.pcisecuritystandards.org/security_standards/.

Comment [L2]: Updated

Comment [L3]: Updated

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 IV describes policies for data access, according to a general scheme of data classification. Section V defines the governance of these policies.

Comment [L4]: Added

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 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.

De Minimus Access

In general, access to, perusal of, use of, and storage of sensitive information should be kept to the minimum amount required to accomplish an employee's business function. Adherence to this precept will ensure that exposure of such sensitive information is limited to the extent possible. Where it is necessary to store sensitive information, the following policies and practices, especially those in Section 5, Files and File Storage, should be observed diligently.

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.acns.colostate.edu/Security. Servers shall be protected as follows:

Comment [L5]: Updated

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, and these archives should be secured physically to the degree warranted by the amount and nature of the sensitive information archived.
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 extent practicable, servers shall maintain log files to record events relevant to services offered on that system (e.g. user access, failed login attempts, application access, etc.). These log files shall be reviewed regularly, either manually or via an automated process. System administrators shall take appropriate action to investigate and respond appropriately to events of a suspicious or illicit nature. 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. 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.acns.colostate.edu/Security. In general, personal computers are subject to the following policies:

Comment [L6]: Updated

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, CenturyLink, 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, CDROM or DVD-ROM.

Comment [L7]: Updated

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.acns.colostate.edu/Policies/AUP.

Comment [L8]: Updated

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.

Scanning for vulnerabilities and to assess adequate patching levels is a fundamental IT security measure. ACNS has the authority, at its discretion, to scan any and all computers connected to the University's network without explicit permission from the computer's owner, operator or system administrator. ACNS shall use reasonable and prudent measures to inform subnet managers of the scope and nature of scans that are to be done. Departmental IT staff may develop policies and procedures for scanning their own systems. Except as noted above, no one is authorized to scan systems they do not own or administer without prior, written approval from departmental officials at an appropriate level.

4. Passwords

Comment [L9]: Whole section is new.

Passwords shall be employed in a manner that makes them difficult for others to guess or otherwise obtain. Prudent measures are to be used to ensure that passwords employed by users are resistant to guessing, that systems are configured to avoid password theft, and that users are encouraged to avoid fraudulent attempts to obtain their passwords. This is especially so for administrative accounts, and is a requirement for central authentication credentials (eID).

Resistance to guessing is achieved by a combination of tactics, focusing on both password choice and system configuration:

1. Password strength (length and/or complexity)
2. Good password choice (avoiding common, easily guessed passwords)
3. Limited password lifetime (periodic refresh/reset)
4. Limited number of guesses over the password’s lifetime (lockout for consecutive failures)

System configuration choices that help protect passwords from theft include:

1. Up-to-date anti-malware
2. Current operating system and application patches
3. Limiting the use of administrator-level accounts
4. Not allowing the operating system or browser to remember (or “cache”) passwords

Users can help protect their passwords by avoiding:

1. Responding to “phishing” emails asking for personal information in reply emails or web links
2. Posting passwords in plain view
3. Sharing account information with others
4. Using the eID password on other systems, particularly outside the University

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. Files containing sensitive information are best maintained on a physically secured and “hardened” server.

Sensitive data in individuals’ files should be kept to a minimum, and reasonable and prudent protection of those files shall be implemented by the system administrator. In particular, files containing significant amounts of sensitive data not stored on portable devices must be protected with strong encryption. As currently interpreted by government regulations and industry standards, "strong encryption" means either the Triple Data Encryption Standard (3DES) or the Advanced Encryption Standard (AES). If AES is chosen, it should be used with the maximum available key length (256 bits). Furthermore, sensitive information that is old and not needed in the normal course of academic/business operations should be removed and securely archived elsewhere, e.g. on tape, CD-ROM or DVD-ROM.

All types of physical IT media (disks, tapes, CD-ROM, DVD-ROM, memory sticks, memory cards, etc.) containing sensitive data shall be disposed of properly, ensuring that the sensitive data is not accessible after disposal. This may be accomplished either by degaussing, or physically destroying the media (e.g. shredding), or both. The owner of physical media that is being disposed is responsible for ensuring that the sensitive information is not accessible after disposal.

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.

Having significant amounts of sensitive data in unencrypted form in insecure locations is prohibited. In particular, unencrypted back-up tapes containing sensitive information must be secured at all times, and should not be removed from University property.

In order to minimize the substantial risk associated with maintaining files containing unencrypted sensitive data, University IT staff may, with proper approval, scan files and monitor network traffic for sensitive data. Such scanning is solely for the purpose of protecting sensitive information. IT staff are not permitted to access others' personal files without their permission for any other purpose, nor are they permitted to disclose such information other than for the purposes of ensuring that sensitive data are protected. ACNS will work with campus IT administrators, recommending tools and procedures for scanning departmental computers for sensitive data. Upon detection of files containing sensitive data, the owner will be contacted and asked to comply with this CSU IT Security Policy.

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.

7a. Guest Wireless Access

It has become evident that guest faculty, researchers, and conference attendees find the campus wireless security requirements overly burdensome to the point of denying reasonable and timely access. To resolve this issue, guest accounts may be requested for individuals not affiliated with the University for the purpose of gaining access to the wireless network. Such access will be limited to web, mail, and VPN, and no local access to University networks will be provided.

8. Social Security Numbers

After September 30, 2006, social security numbers (SSNs) shall not be stored on University computers unless written authorization for doing so has been obtained from the Vice President for Information Technology. SSNs stored on portable devices must be encrypted using the technologies described above in Section 5 above. See http://csuid.colostate.edu/for more information, including the form for applying for exceptions to allow SSNs to be stored on University computers.

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 VPIT. Authorization forms for this can be obtained from the office of the VPIT.

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 significant 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~~7276. 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 including the department may be formed, at the discretion of ACNS, and may involve the Provost should the incident be severe The incident response team shall decide upon a response proportionate to the incident. Should there not be agreement in how to respond, the Director of ACNS or the Provost, if involved, 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 has 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, CDs, DVDs 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.acns.colostate.edu/Security).

Comment [L10]: Updated

1. Operating Systems

Only operating systems that are secure according to current best practices and require strong authentication shall be used. In particular, only currently supported Windows operating systems shall be used (see http://www.acns.colostate.edu/Policies/DesktopSoftware). If an older Windows operating system is required, an exception must be applied for (see http://www.acns.colostate.edu/Security/Exemption~~http://newurlhere~~). Security patches and updates shall be applied in a timely manner. Where possible, updates shall be automatically applied to both operating systems and applications.

Comment [L11]: Updated

Comment [L12]: The request form is included as a separate document; new URL request pending with Middleware.

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.acns.colostate.edu/Policies/AUP) 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.

Comment [L13]: Updated

~~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~~3. Anti-~~spyware~~malware

~~Appropriate measures to reasonably~~Where applicable, all client computers shall deploy University-standard software for protection ~~protect all client computers~~ against ~~spyware~~ various forms of malicious software ("malware", including viruses, spyware, etc.)~~shall be taken~~. ~~The current version of anti-virus/anti-spyware software shall be installed and configured as approved~~ (see ~~http://www.acns.colostate.edu/?page=products~~). ~~This~~ Anti-malware software ~~should~~ shall be configured to automatically update ~~the spyware~~ malware definition files. Other means of providing equivalent levels of protection against ~~spyware~~ malware may be used, at the discretion of local IT managers, provided an ex~~c~~eemp~~p~~tion ~~request~~ has been approved (see http://www.acns.colostate.edu/Security/Exemption) .

Comment [L14]: The market has moved away from considering spyware as a target for a freestanding application; we no longer have a supported anti-spyware product separate from our general endpoint security product. Consider deleting this section, and/or merging it with Anti-virus. Recommend one section on endpoint protection/behavior, which would encompass sections 3 and 4.

Comment [L15]: No longer works.

~~5~~4. Server Registration

All servers containing sensitive information shall be registered with ACNS on http://www.acns.colostate.edu/Security/Compliance) ~~on ACNS' web page dealing with IT security (see http://www.acns.colostate.edu/?page=security_compliance_index)~~.The initial registration and updates thereof shall be coordinated through the subnet managers.

~~6~~5. Passwords

Comment [L16]: Whole section is new.

Passwords are widely used to protect computers, networks, and information, but they are particularly susceptible to compromise if the passwords are weak (easily guessed) or if systems performing user authentication do not enforce measures to limit guessing attacks. The following are mandatory, minimum requirements that shall be implemented for central (eID) authentication. All campus systems must use strong passwords, and must configure server-level password-guessing protection technologies of similar strength where ~~available~~practicable; the requirements below are suggested as a combination of strength and guessing protection that meets current government and industry standards.~~The following are mandatory, minimum requirements that shall be implemented by all users and on all systems that perform user authentication~~:

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

   1. Passwords for general systems shall be at least fifteen (15) characters in length (note that numbers, upper-case letters, and special characters are NOT required, though they are allowed).
   2. Passwords shall not be derived from a user's name or login ID.
   3. Passwords shall not be derived from system-specific information such as hostname, aliases or entries in users' files.
   4. Passwords shall not consist of a single-word entry in a dictionary (*astrobiologists*), or a commonly chosen phrase that would easily be guessable based on organizational affiliation (*fightonyoustalwartrams*) or personal/professional interests (*businessadministration* or *denverbroncosfan*). Rather, a good password is easily memorized but not obvious (*ends-justify-means*, *darwin#beagleship*, or *stereochemrocks*).
   5. Default passwords supplied by vendors shall always be changed immediately after implementation.

b. In addition to enforcing good choice of passwords, systems that perform user authentication shall be configured to reduce the likelihood of a successful guessing attack and limit the scope of inappropriate access in the event of a compromise.

   a. Passwords shall be changed at least once per year.

   b. Systems shall be configured to track failed login attempts, as excessive failures may signal an automated guessing attack. Systems shall lock user accounts for one hour whenever the system detects fourteen (14) consecutive failed logins.

   c. 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.

~~7~~6. Browser Cookies

Because browser cookies and files that exist on computers as a result of web browsing may contain sensitive information and subject to access via spyware, malware and other illicit means of access, their existence on IT systems should particularly be minimized. Periodically, at least once per week and more frequently if significant amounts of sensitive information may exist in browser cookies on computers, users should delete the browser cookies and files on their computers that exist as a result of web browsing. Users must take individual action to delete this information (for instructions on how to delete this information, see http://www.acns.colostate.edu/Security/SecureBrowser).

Comment [L17]: Updated

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, CDs, DVDs 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.

2. Credit Card Information Stored in Electronic Form

Computers shall not store credit card information in any form, unless approved in writing by Business and Financial Services. If so approved, 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, DVD) 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.

3. Systems that Support On-line Credit Card Authorization

The University is required to comply with the Payment Card Industry's Data Security Standards for on-line processing (see https://www.pcisecuritystandards.org/security_standards/).
Units may use Paypal Pay Flow Link, Authorize.net, or Colorado's State Internet Portal Authority (SIPA) for on-line processing. To maintain appropriate internal controls and compliance with both the card industry's and the university's policies, departments that wish to process credit cards on-line shall coordinate the establishment of their vendor agreements and merchant accounts with the Bursar's office. All systems that process credit cards on-line shall use one of the above named systems, and be configured such that no credit card information traverses University networks or systems. After the purchase is initiated via an on-campus system, all credit card transactions are required to be handed off the credit card processing to the vendor's system prior to any credit card processing. To prevent credit card fraud, all use of these vendor's systems shall be configured to

request the Card Verification Value (CVV) number (found on the back of credit cards), but need not require the CVV to be validated for processing payment to accommodate international credit cards. Other security features may also be required at the direction of Provost, as recommended by the University's Vice President for Information Technology and the University Controller. Exceptions to this policy may be applied for in writing (via email is fine) to the University's Vice President for Information Technology, and shall be approved by the University's Vice President for Information Technology and the University Controller.

Formatted: Space After: 0 pt, Line spacing: single, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Section IV Access to Central Data

The University generates, stores, and makes accessible to authorized individuals central data from its Systems of Record (the Student Information System, the Human Resource System, the Financial Management System, the Research Management System, etc.). This section contains the definitions and policies pertinent to such central data.

Central data are classified into three categories of access, defined for each System of Record by the Data Authority for the System of Record. Data classifications are defined in the Definitions section below. In all cases, de minimus access as defined herein in Section II is applicable.

Definitions

Central Units – Central IT departments reporting to the VP for Information Technology, including Information Systems, Academic Computing and Networking Services, and Institutional Research.

Data Authority – The position responsible for a central administrative system from a functional standpoint. This includes the Registrar for the Student Information System, the Director of HR for the Human Resources System, the Controller for the Kuali Financial System, and others as may be identified for systems where central data is provided.

Data Steward – The position responsible for local Data Users in a unit, typically a College or a VP unit. This position is granted authority by the Data Authorities, and is responsible for controls associated with data users.

Data User – The position that uses the data, under the auspices of the Data Steward.
Default Data – Data of a non-sensitive nature that are widely available. Data Stewards may grant access to default data to their Data Users.

Restricted Data – Data of a more sensitive nature that are available only by approval of the Data Authority for the System of Record.

Private Data – Data of a highly sensitive nature, that are not available for general business intelligence, but that are available to only a small subset of users on the System of Record. These data include SSNs, CCNs, etc.

Policies for Data Access

Data are accessed in accordance with the definitions and roles as defined in this Section IV.

Data Stewards are responsible for controls to data and ensuring policies and best practices are adhered to by their Data Users. Data Stewards are responsible for:

1) endorsing and forwarding requests for their Data Users to access central data,
2) endorsing and forwarding requests for access to Restricted data for their Data Users,
3) at least once per year, reviewing and approving access to central data for Data Users under their auspices,
4) serving as the liaison with central units including recommending modification or revocation of access privileges for their Data Users when job duties change,
5) coordinating training and communications for Data Users, and

6) identifying and referring actions of their Data Users in conflict with these policies to the department head and dean or VP of the Data User’s unit.

Data Users and Data Stewards must apply and be approved for data access by the Data Authorities for the systems to which data access is granted. Application forms for this purpose are available on CSU’s Campus Administrative Portal at http://cap.is.colostate.edu under the ODS tab in the Campus Reporting section.

Section V 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 Technology (UTC) 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 Vice President for Information Technology, Dr. Patrick J. Burns, Patrick.Burns@ColoState.EDU.