# CSU POLICY: INFORMATION TECHNOLOGY SECURITY

| | |
|---|---|
| Policy Title: Information Technology Security | Category: Information Technology |
| Owner: Vice President for Information Technology | Policy ID#: 4-1018-009 version 15 |
| Contact:<br>Academic Computing and Networking Services<br>Web: http://www.acns.colostate.edu<br>Phone: 970-491-5133 | Original Effective Date: 2/5/2013<br>Last Major Revision: 6/2/2016<br>***Print Version:*** ***Click Here to Print*** |

## TABLE OF CONTENTS


PURPOSE OF THIS POLICY
DEFINITIONS USED IN THIS POLICY
POLICY STATEMENT
POLICY PROVISIONS
SECTION I General IT Security Policies and Guidelines
Applicability
Principle of Least Privilege
IT Security Policies
Responses to IT Security Incidents
SECTION II Mandatory, Minimum IT Security Requirements
SECTION III Protection of Credit Card Information
SECTION IV Access to Central Data
Definitions
Policies for Data Access
SECTION V Cloud Computing
Definitions
Policies for Cloud Computing
SECTION VI Governance of These Policies
OTHER RESOURCES
APPROVALS


## PURPOSE OF THIS POLICY

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 (PCI-DSS). 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 USED IN THIS POLICY

Application is a computer software program run on a computer for the purpose of providing a business/academic/social function.
Cloud Computing – Any network, remote server, application, digital storage facility, or related service that is hosted or provisioned on infrastructure external to CSU, and accessed via the Internet, to store, manage, or process data. It does not include infrastructure or services that are owned, controlled and/or operated solely by or for the University. Examples include externally hosted file storage services (e.g. Dropbox, Google Drive, Microsoft OneDrive, Box); mail services (gmail, Hotmail, Yahoo mail, etc.); application services (e.g., Google Apps); and social networking applications, blogs and wikis.
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.
Data Classification Levels:

- Private Data – Private Data are the most sensitive data at CSU, and as such are subject to the greatest protections. Because of legal, ethical, or other constraints, Private Data may not be accessed without specific authorization, and access may be granted only selectively with final approval from the appropriate Data Authority. Private data encompasses social security numbers, financial

information including credit card information, driver's license information, federally protected personnel information, proprietary research information, third-party proprietary information, personal health information, and any other information that is highly regulated or that through disclosure would adversely affect an individual or tarnish the reputation of the University. Private data may not be shared outside of the University.

- Restricted Data – Restricted Data must be treated with propriety, and used only within the confines of the University, unless specific and appropriate approval is provided for sharing, generally from the Office of the General Counsel. Restricted Data may be accessed by all eligible employees of the University needing such access in the conduct of University business. Employees accessing data are responsible to conform to the Principle of Least Privilege, where they are personally responsible for accessing only the minimum amount of data required in the conduct of their business. Employees are also personally responsible for adhering to any and all pertinent University policies, including this IT Security Policy, the Acceptable Use Policy, etc. Any requests for data from a member of the public should be referred to the appropriate data authority or the Office of the VP and General Council.
- Public Data – Public data are directory data, and data explicitly made available to the public (e.g., data available on open, public web pages, or in other publications and venues).

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.

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

Payment Card Industry Data Security Standard (PCI-DSS) is a set of security requirements defined by the credit card industry.

Personal computers are comprised of desktops, laptops, tablets, 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, optical disks, 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. See the three levels of data classification at CSU (Private Data, Restricted Data, and Public Data).

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.

# POLICY STATEMENT

CSU's IT Security policies are presented hereinafter in five 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 the use of Cloud resources to store CSU data. Section V defines the governance of these policies. A short reference to additional resources concludes this document.

# POLICY PROVISIONS

## 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.

### Principle of Least Privilege

Least Privilege is a well-established concept in information security. Expressed simply, it is the notion that information and resources should be made available only to those people, processes, or technologies that need them for a legitimate purpose. As a guiding principle for designing and operating information systems, Least Privilege leads to careful system access control, strong authentication, data confidentiality, and default-deny network access control. In particular, 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.

## 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. Departments owning the servers are responsible for ensuring that their servers containing sensitive information are secured in accordance with these policies. Servers shall be protected as follows:

a. Such servers shall be housed in a physically secure facility where access is audited and limited to only those individuals requiring access to perform routine or emergency maintenance on the system.
b. To the degree practicable, only operating systems and applications that provide high levels of security shall be used, system security features shall be enabled, and security updates (patches) shall be applied in a timely manner. Acceptable versions of operating systems and applications for web servers are listed at https://www.acns.colostate.edu/media/sites/100/2016/08/Web-Server-Standards.pdf
c. Server-side computer virus protection should be implemented and kept up to date.
d. 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.
e. 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.
f. 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 hardware firewall.
g. 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.
h. 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, and these archives should be secured physically to the degree warranted by the amount and nature of the sensitive information archived.
i. 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.
j. 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.

k. 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 (e.g. the campus VPN). This policy is particularly relevant when allowing access from external (non-CSU) networks.
l. To the degree practicable, remote access to the server that would potentially allow root or system-level control shall use encrypted protocols, shall use strong authentication, and should limit access to authorized source addresses and users (ideally through a separate, central service such as a load-balancer, proxy, or VPN).
m. 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.
n. 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.
o. Servers shall be scanned for operating system and application vulnerabilities on a regular schedule. Vulnerabilities detected shall be addressed in a timely manner.
p. 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.
q. To prevent the inadvertent release of sensitive information stored on hard drives when systems or components are decommissioned, all storage media must be sanitized in accordance with the guidelines in NIST 800-88 Revision 1 (http://dx.doi.org/10.6028/NIST.SP.800-88r1) prior to release to other agencies. Surplus Property will either sanitize or destroy disk drives for a nominal fee.

**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:

a. 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. Acceptable versions of operating systems and applications for personal computers connecting to the University network are listed at https://www.acns.colostate.edu/computer-standards
b. Computer virus protection shall be implemented and kept up to date.
c. Services and applications offered shall be the minimum necessary to accomplish the desired business/academic functions.
d. Network traffic shall be limited to only those services and ports considered essential and required for legitimate business/academic purposes.
e. 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.
f. To prevent the inadvertent release of sensitive information stored on hard drives, all drives must be sanitized in accordance with the guidelines in NIST 800-88 Revision 1 (http:// dx.doi.org/10.6028/NIST.SP.800-88r1) prior to release to other agencies, or disposal. Surplus Property will either sanitize or destroy disk drives for a nominal fee.
g. 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, optical disk, etc.

**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://policylibrary.colostate.edu/policy.aspx?id=704.

The best security model addresses vulnerabilities at multiple levels, a concept known as "defense in depth". This document focuses primarily on securing systems and data, 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--to expose system and application vulnerabilities, to assess adequate patching levels, and to assess the adequacy of information protection--is a fundamental IT security measure, and will be employed as a regular practice. 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**

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:

a. Password strength (length and/or complexity)
b. Good password choice (avoiding common, easily guessed passwords)
c. Limited password lifetime (periodic refresh/reset)
d. Limited number of guesses over the password's lifetime (lockout for consecutive failures)

System configuration choices that help protect passwords from theft include:

a. Up-to-date anti-malware
b. Current operating system and application patches
c. Limiting the use of administrator-level accounts
d. Not allowing the operating system or browser to remember (or "cache") passwords

Users can help protect their passwords by avoiding:

a. Responding to "phishing" emails asking for personal information in reply emails or web links
b. Posting passwords in plain view
c. Sharing account information with others
d. 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 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. Furthermore, sensitive information that is old and not needed in the normal course of academic/business operations should be removed and securely archived elsewhere.

All types of physical IT media (disks, tapes, optical disks, 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**

The University funds and operates wireless networks for University business as well as for visitors. In general, these networks are subject to the same requirements as the University's wired network (see section I.3 and II.2: "Network Security"). Due to the nature of wireless networking, devices using the WiFi spectra (2.4GHz and 5GHz) are subject to additional restrictions in order to maintain a functional campus network, therefore unauthorized wireless devices shall not be

connected to the University's network. Furthermore, devices that interfere with the University's use of these spectra are not permitted. Approved classes of devices, and recommended configurations, are posted at https://www.acns.colostate.edu/wireless. University business conducted via wireless devices shall use the encrypted, authenticated wireless networks provided for students, faculty, staff, and visitors from eduroam member institutions.

**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.

**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 Central Help Desk at 970.491.7276. 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 has 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, optical disks, 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' website (http://www.acns.colostate.edu/Security).

**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 https://www.acns.colostate.edu/Security). 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 web servers. To keep the list of exceptions current and relevant, thereby minimizing the possibility of inadvertent exposure of internal resources to attack, exception requests will need to be re-confirmed each year. 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.

**3. Anti-malware**

Where applicable, all client computers shall deploy University-standard software for protection against various forms of malicious software ("malware", including viruses, spyware, etc.). Anti-malware software shall be configured to automatically update malware definition files. Other means of providing equivalent levels of protection against malware may be used, provided an exemption has been approved (see https://www.acns.colostate.edu/Security) by ACNS.

**4. Passwords**

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 practicable; the requirements below are suggested as a combination of strength and guessing protection that meets current government and industry standards:

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)
b. 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).
c. Passwords shall not be derived from a user's name or login ID.
d. Passwords shall not be derived from system-specific information such as hostname, aliases or entries in users' files.
e. 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*).
f. Default passwords supplied by vendors shall always be changed before production implementation.
g. 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.
1. Passwords shall be changed at least once per year.
2. 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.

h. 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.

6. **Web Browser Security**
    a. **Browser Version:** Browsers should be set to automatically apply security updates (patches).
    b. **Plugins and Extensions:** Utility programs that run within the browser also need to be kept updated so they do not become vectors for attack.
    c. **Cookies, History, and Temporary Files:** Because browser cookies and files that exist on computers as a result of web browsing (including browsing history and temporary files) may contain sensitive information and are subject to access via spyware, malware and other illicit means of access, their existence on IT systems should be minimized whenever possible. Periodically, and at least once a week if significant amounts of sensitive information may exist in browser cookies on computers, users should delete these cookies and files.
    d. **Additional Protection:** For instructions on keeping each of the major browsers securely configured, and for additional steps to increase a computer's protection, see https://www.us-cert.gov/publications/securing-your-web-browser.

## SECTION III Protection of Credit Card Information

The University is required to comply with the Payment Card Industry Data Security Standard (PCI-DSS; see https://www.pcisecuritystandards.org/security_standards/). The requirements in this section are mandatory, minimum requirements that shall be implemented on all University systems that process, store, 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 (disks or other storage devices). In order to maintain University-wide compliance with these standards, all credit card activity will be coordinated by a PCI Team comprised of members from Academic Computing and Networking Services and Business and Financial Services (BFS). The PCI Team shall post and maintain standards and procedures documentation, meet regularly with all credit card merchants, and provide annual compliance reporting.

### 1. Credit Card Information Stored in Non-electronic Form

Credit card information that is stored in non-electronic form is subject to PCI-DSS, as well as 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. The PCI-DSS prohibits the storage of some kinds of card information after card authorization.

### 2. Credit Card Information Stored in Electronic Form

Computers shall not store credit card information in any form, unless approved in writing by BFS. If so approved, credit card information that is stored in electronic form is also subject to PCI-DSS, as well as policies contained in the latest version of the "CSU Personal Records Privacy and Security Policy."

**3. Systems that Support Credit Card Authorization**
To maintain appropriate internal controls and compliance with both card industry and University policies, departments that wish to process credit cards shall coordinate the establishment of their vendor agreements and merchant accounts with the Banking Services unit of BFS. All systems that process credit cards shall use a University-approved authorization provider, and be configured such that no credit card information traverses University networks or systems. To prevent credit card fraud, all use of these vendors' systems shall be configured to comply with PCI Team procedures regarding fraud detection suites and use of the Card Verification Value (CVV) number (found on the back of credit cards). Systems involved in credit card activity shall be segmented from the main University network as specified by the PCI Team, and shall be reviewed at least annually for compliance with the PCI DSS and University policies.

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.

## SECTION IV Cloud Computing

Cloud computing is becoming commonplace, even for institutions that continue to maintain extensive internal computing and network services. Cloud-based services enable convenient storage or synchronization of a consistent set of files on one or more computers and mobile devices, sharing data with a large variety of external users, and leveraging externally hosted processing resources. Such services make cloud resources an attractive option, and it is accepted that all members of the University community, including the institution itself, utilize cloud services in CSU's everyday business affairs.

However, these services vary widely as to their integrity and reliability, as well as the contractual terms and conditions they impose upon their users (often with little or no understanding by those users). Some cloud providers, for instance, mine data for marketing purposes and make no effort to determine whether such data is subject to privacy laws that the University must obey (such as FERPA, protecting the privacy of students' education records, and HIPAA, protecting the privacy of personal health information, among others).

The purpose of this Policy, therefore, is to define cloud computing as it applies to the University, and to establish certain prudent rules and practices to be followed when utilizing the cloud.

### Policies for Cloud Computing

It is the policy of Colorado State University to permit and encourage the use of cloud-based services that enhance productivity, convenience, and creativity, provided that the institution and its employees, agents and contractors must take reasonable measures to protect the integrity, security, and privacy of data, and to prevent damage to and unauthorized use of its systems, when utilizing such services.

1. **General Cloud Policy**

The University endorses the use of cloud computing services for University business, including file storing and sharing, when:

a. The cloud services vendor provides appropriate levels of protection and recovery for University information;
b. The vendor accepts and is contractually bound to implement explicit restrictions on storage of Sensitive Information (defined as both Private Data and Restricted Data); and
c. The use of such service does not place the University at an unreasonable risk of experiencing data breach, data loss/non-recovery, or degradation of its computing and network services.

2. **Use of Non-Contracted Vendors for Cloud Computing**

The University, its departments and other business units, and persons acting for the University, may use cloud computing services for University data only if (i) there is an approved University Contract authorizing such use; (ii) there is no University Contract, but the service has been approved by -the VP for IT for use by the University; or (iii) the use is limited to the exchange or storage of Public Data. **Cloud-based services provided by non-contracted or non-approved vendors may not be used to store, transmit or share Private Data or Restricted Data.**

3. **Contracted Vendors for Cloud Computing**

When contracting with a cloud computing vendor, the University must specify particular data protection terms in a contract so as to provide a level of security that ensures that the University data is kept confidential, is not changed inappropriately, and is available to the University as needed. The level of confidentiality, security and integrity that is required varies depending on the type of data for which the service will be used, but, in general, must meet or exceed all applicable laws, rules and regulations, as well as other applicable University policies, concerning the use and protection of such data. At a minimum, such contracts must provide:

a. Explicit, enforceable promises by the vendor to utilize encryption, password protection, firewalls, and other such technologies to protect the data at all times, without regard to interruption of service;
b. An indemnification by the vendor protecting CSU from claims, damages and expenses that may occur as a result of the vendor's negligence in providing the service, or its breach of the agreement; and
c. A requirement that the vendor report any breach, loss, or corruption of University data to the responsible University administrator within a reasonable time (which may be immediate) after determining that such event may have occurred.

Additionally, the University should consider the following contract terms to ensure a minimum level of information security protection: Data transmission and encryption requirements; Authentication and authorization mechanisms; Intrusion detection and prevention mechanisms; Logging and log review requirements; Security scan and audit requirements; and Security training and awareness requirements.

All contracts entered into by or on behalf of CSU with any cloud services provider must be approved by the Director of ACNS before being signed on behalf of CSU by an authorized contract signatory.

Data restrictions for contracted vendor services:
**Cloud services provided by a University-contracted vendor may not be used to store, transmit or share Private Data or Restricted Data unless the VP for IT has first approved such use for the University.**

4. **Support**

Many cloud-based services require the install of a third-party application on the device that will access the service. Use of these services under this policy does not imply that the applications will be supported by ACNS or other information technology service areas. Individuals using these services and applications should contact their local IT support personnel to discuss support options. Support options provided by the vendor should also be considered when contracting.

## 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 Advisory Committee (STAC), 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.

## 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/.