Information Security
CC260

Last Reviewed: April 2018

Intent

UCLA Extension's information security policy ensures that its critical operations, assets and customers are properly protected. Due to the increasing value of the data we collect, store and process, we are committed to its protection, the enforcement of applicable regulatory guidelines and routine assessment of security risks.

This policy applies to all employees, vendors and business partners with whom data is shared or to whom data is accessible. This policy mandates employment of daily operational security procedures.

This policy ensures compliance with applicable laws and standards, protects the University from liability and protects the confidentiality, integrity and availability of our information systems, data and network resources.

A copy shall be provided to contractors, vendors, service providers and business partners who have access to data. Third party persons (i.e. vendors, service providers) who do not comply with this policy may be subject to appropriate actions as defined in their contractual agreements.

Per *Payment Card Industry* (PCI) *Data Security Standards* (DSS) this policy must be substantively reviewed annually by the managing cashier in Student & Alumni Services Department and the Director of Information Technology Services (ITS). Revisions driven either by security incidents discovered during the year or by revisions and updates to the card industry's data security standards will be proposed to the Dean for incorporation and approval.

This policy meets the requirements for having a policy on *Information Security* as required by the PCI DSS. This policy will be superseded by any provision of UC or UCLA policy or California law regarding information security should any conflict be found and amended as needed to align with these higher authorities.

Definitions

- **Availability.** Ensuring that information systems, data and network resources are available and ready for use when they are needed.
- **Confidentiality.** The protection of data from unauthorized disclosure.
- **DMZ.** Demilitarized zone. Network added between a private and a public network to provide an additional layer of security.
- **Emergency Change.** A change which, due to urgency or criticality, needs to occur outside of Extension's formal change management process.

- **Encryption.** Process of converting data into an unintelligible form except to holders of a specific cryptographic key.
- **Information System.** Information systems include, but are not limited to, laptop computers, workstations, servers, mainframe computers, routers, switches, cell phones, telephones, fax machines and personal digital assistants (PDAs).
- **ITS.** UCLA Extension's *Information Technology Services* department.
- **Integrity.** The accuracy, completeness and validity of information.
- **Logical Controls.** Controls that limit logical access to information systems and/or electronic data, for example, passwords, user accounts, firewall rules.
- **Malicious software.** Software designed to damage or disrupt information systems, data or network resources.
- **Network Resource.** Communication links and network bandwidth.
- **Physical Controls.** Controls that are physically implemented, for example, surveillance cameras, motion alarms, door locks, security guards.
- **Risk.** The likelihood of a given threat exercising a particular potential vulnerability, and the resulting impact of that adverse event on an organization.
- **Security Incident.** The unauthorized access, attempted or successful, to use, disclosure, modification, or destruction of data or services used or provided by UCLA Extension.
- **Sensitive Data.** Sensitive data includes but is not limited to, passwords, Social Security numbers, credit card information, protected health information (PHI), personally identifiable information (PII), bank account numbers and tax ID numbers that are stored, processed or transmitted on or by Extension information systems or network resources.
- **Strong Cryptography.** A cryptographic algorithm or protocol that makes it very difficult for an unauthorized person to gain access to encrypted data.
- **Threat.** Condition that may cause information or information processing resources to be intentionally or accidentally lost, modified, exposed, made inaccessible, or otherwise affected to the detriment of UCLA Extension.
- **Two Factor Authentication.** The use of two independent mechanisms for authentication. For example, a security token and a password.
- **User.** Anyone who accesses information systems, data or network resources.
- **Visitor.** A vendor, guest of an employee, service personnel, or anyone who needs to enter a UCLA Extension facility containing information

systems, data or network resources for a short duration, usually not more than one day.

Roles and Responsibilities

Extension's Information Technology Department (ITS) will:

- Establish, document and distribute information security standards and procedures.
- Monitor and analyze security alerts and information, and distribute to appropriate employees.
- Establish, document, and distribute security incident response and escalation procedures.
- Administer user accounts, including additions, deletions, and modifications.
- Monitor and control all access to sensitive data.

Risk Assessment

UCLA Extension will regularly identify, define, and prioritize risks to the confidentiality, integrity, and availability of its information systems, network resources and data. Extension's ITS will conduct a formal, documented risk assessment of its information systems, data and network resources on an annual basis. The assessment must identify and prioritize the threats and vulnerabilities to Extension's information systems, data and network resources and define the likelihood and impact of risks.

The risk assessment will be used in conjunction with the University's risk management process to identify, select, and implement appropriate and reasonable controls to protect the confidentiality, integrity, and availability of Extension's information systems, network resources, and data. The risk assessment will follow established methodologies such as OCTAVE, ISO 27005 or NIST SP 800-30.

Extension must conduct risk management on a regular basis and select and implement reasonable, appropriate, and cost-effective controls to manage, mitigate, or accept identified risks. All such controls must be commensurate with identified risks.

Annually, the Director of ITS must submit an information security risk management report to the Dean's Office. The report must identify the significant risks to information systems, data and network resources that have been identified during the past year, the risks that have been accepted and which risks have been mitigated.

Logical Access Control

Logical access to information systems and media containing sensitive data will be denied until specifically authorized by appropriate personnel. Appropriate information system owners and/or data custodians or their designated delegates will define and approve logical access to Extension's information systems and media containing sensitive data.

Logical access to Extension's information systems and media is provided only to those having a need for specific access in order to accomplish a legitimate task and must be based on the principles of *need to know* and *least possible privilege*.

Extension supports a formal, documented user-management process which enables the controlled addition, change and termination of logical access rights on information systems, data and network resources. The process is capable of granting different levels of access to information systems, data and network resources. An automated access control system is in place to control access to information systems.

A unique user name will be used by all persons accessing Extension information systems and media containing sensitive data. Along with the unique user name, a password is required.

Multi-factor authentication will be used by employees, contractors, service providers and vendors for remote access to Extension's information systems and media containing sensitive data. Extension employees will also use multi-factor authentication for UCLA Logon (Bruin Online). Extension employees who telecommute must take all precautions necessary to secure any and all sensitive data in their homes and prevent unauthorized access to any Extension information systems or data.

Vendor maintenance accounts and ports on Extension information systems that contain sensitive data must be disabled until the specific time they are needed by the vendor. After appropriate use by the vendor, they must again be disabled. All vendor access shall be monitored while in use.

Group, shared or generic accounts or passwords may not be used on Extension information systems that store, process or transmit sensitive data. The following requirements must be met for passwords on such systems:

- User passwords must be changed at least every 90 days.
- Passwords must be at least 7 characters long and include both numeric and alphabetic characters.
- First time passwords must be unique for each user and must be changed upon first use.
- Password reuse must be restricted to no more than once every 4 uses.

- Via the use of strong cryptography, all passwords must be unreadable during transmission and storage on all information systems that store, process or transmit sensitive data.
- User accounts must be locked after six failed login attempts. The lockout must be for at least 30 minutes or until authorized personnel unlock the account.

Extension employees must not use passwords that are also used for non-Extension accounts, such as accounts for Federal Government systems (e.g. SEVIS) also employed in the course of business.

Activation of information system locking software or log off will occur when a user session on an Extension information system is inactive for more than 15 minutes.

User identity will be appropriately verified before any password, which enables access to an Extension information system or network resource, is reset.

User accounts that are inactive for more than 90 days on information systems that store, process or transmit sensitive data must be disabled or removed. Annually, appropriate system owners and/or data custodians or their designated delegates will review and verify logical access rights to information systems and media containing sensitive data. Such rights will be revised as necessary. Inactive accounts over 90 days old will be either removed or disabled.

Extension employees and contractors experiencing a change in status (e.g. termination, position change) will have their logical access rights promptly reviewed, and if necessary, modified or revoked.

Physical Access Control

At least annually, Extension directors and managers will review all of its physical areas that must be protected from unauthorized physical access. The assessment must take into consideration areas where sensitive data is stored, processed, or transmitted as well as the location of any supporting assets or critical infrastructure.

Extension's information systems and electronic and non-electronic media containing sensitive data must be located in physically secure areas ("limited access area"). Information systems located in unrestricted, public access areas must be physically secured to prevent theft.

Access to limited-access areas must be denied until specifically authorized by appropriate personnel. Such access must be provided only to those having a need for specific access in order to accomplish a legitimate task and must be based on the principles of need to know and least possible privilege. Access privileges to limited access areas must be reviewed at least annually.

Cameras or other access control mechanisms must monitor the entry and exit points of physical areas containing information systems that store, process or transmit sensitive data or electronic and non-electronic media containing sensitive data and must be protected from tampering or disabling. Camera data must be stored for at least three (3) months unless otherwise restricted by law.

Extension's ITS will either disable or control and restrict physical access to publicly accessible network jacks; it must also restrict physical access to wireless access points (WAPs), gateways and handheld devices, networking/ communications hardware and telecommunications lines located at Extension facilities.

Backup media, both paper and electronic, that contains sensitive data will be stored in a secure location. The location's security will be reviewed at least annually. An inventory of all such media will be conducted at least annually. Where appropriate, shred bins will be maintained with a lock preventing access to its contents. All such media, when no longer needed for business or legal reasons, will be destroyed in such a way that there is reasonable assurance that the media cannot be reconstructed (i.e. crosscut shredding, pulping or incinerating of hardcopy materials and degaussing, securely overwriting or physically destroying electronic media).

Extension's electronic and non-electronic media containing sensitive data will be classified so that it can be identified as "confidential." Distribution of such media outside Extension must be tracked and logged. Such media will only be distributed outside Extension via a delivery method that can be tracked (such as secure courier).

The designated manager or director must approve the movement of any media containing sensitive data from a limited access area.

Extension will have a formal, documented process in place that clearly identifies and distinguishes between employees, contractors, and visitors in high security or limited access areas.

Visitors to limited access areas will be formally authorized by supervisorial staff managing access to such areas. Visitors to limited access areas will be given a physical token (i.e., a badge or access device) that has an expiration date and that identifies a visitor as a non-employee. Visitors must return their physical token upon leaving a limited access area or at the expiration date.

Visitors will sign a visitor's log prior to being granted physical access to limited access areas. The log will document the visitor's name, the company represented, the authorizing employee, and the date and time of entrance and departure. Unless otherwise restricted by law, visitor logs must be retained for at least three (3) months.

Security Training and Awareness

UCLA Extension will ensure that all personnel are provided with sufficient training and supporting reference materials to enable them to appropriately protect information systems, network resources, and data. Security information and awareness is provided via web-based training, instructor-led training, memos and periodic meetings.

Security information and awareness training will include but is not limited to:

- Presentation of this and other job-related policies at point-of-hire for all Extension employees.
- Announcements of any significant revisions to this or other related policy, security controls or processes will be made as they are implemented.
- Announcements by ITS of any significant new security threats to information systems, network resources, or data will be made as they become known.
- For those who have access to grades and other sensitive data stored in student records, attendance at training regarding the federal *Family Educational Rights and Privacy Act*, *California Information Practices Act*, and other law and policies affecting privacy will be completed.
- For those who participate in or manage enrollment and payment process (Student & Alumni Services and Cashier & Financial Services), or who have ancillary access to credit card data (ITS), mandatory annual engagement in structured training provided by UCLA regarding payment card industry compliance and security expectations will be completed. The Enrollment Manager will coordinate and ensure the training is completed by each employee.
- For those who have the ability to amend records, attendance at identity theft alert and fraud sensitivity training per the Federal Trade Commission *Red Flags Rule* will be required annually. The Enrollment Manager in Student & Alumni Services will conduct this training, and will post on its intranet site the current *Red Flags Control Matrix* and update it following each annual meeting.

Employee Technologies

Employee technologies, i.e. remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, PDAs. Email and internet usage, that access sensitive data will only be used by personnel if the following controls are in place:

- The Dean's Office has approved the use of the technologies
- Appropriate authentication is used

- A regularly updated inventory of devices, approved network locations for their use, and list of the persons authorized to access the devices
- Devices are labeled with owner name, contact information, and a description of the device's purpose
- Devices are appropriately used and placed in appropriate network locations
- The ITS Department maintains a regularly updated list of approved devices

When payment card data is remotely accessed, the data will not be copied, moved, or stored onto local hard drives or removable electronic media unless explicitly authorized for a defined business need.

Remote access sessions to information systems containing sensitive data must be disconnected after twenty (20) minutes of inactivity. Remote access technologies used by vendors or business partners to access information systems containing sensitive data must be turned off when not in use.

Data Retention and Disposal

Departments that must keep and store sensitive data will do so to the minimum necessary required for business, legal and/or regulatory purposes. Full social security numbers required for tuition payment reporting to the Internal Revenue Service will be retained only for the period that a taxpayer may file an amended return to either the State of California or the federal government.
When no longer required for such purposes, sensitive data on information systems or on electronic and non-electronic media must be appropriately disposed. The following disposal methods will be used:

- Non-electronic media must be cross-cut shredded, incinerated or pulped.
- Electronic media must be purged, degaussed, shredded or otherwise destroyed so that sensitive data cannot be reconstructed.

Sensitive data electronic media and information systems must be securely and thoroughly erased before such items can be re-used.

Information systems and electronic and non-electronic media that contain sensitive data must be inventoried and audited on a quarterly basis to ensure that the stored data does not exceed defined data retention requirements.

Electronic storage of any credit/payment card information is prohibited.

Cryptographic keys must be securely stored and comply with the following key management procedures:

- Generation of strong keys
- Maintenance of an inventory of encryption keys

- Secure key storage and distribution
- Periodic key changes
- Destruction of old keys
- Split knowledge and dual control of keys
- Prevention of unauthorized substitution of keys
- Replacement of known or suspected compromised keys
- Revocation of old or invalid keys

Key custodians must sign a form specifying that they understand and accept their key-custodian responsibilities.

Credit Card Data & Payment Handling

Processing cash, cash equivalents, and credit card payments must be processed only by authorized agents who have completed campus provided PCI DSS Security Awareness Training, Cash Handling Safety and Security Training, and CASHNet Cashier Training, after initial hire and annually thereafter, and who have completed a background check in accordance with *PPSM Policy 21* at the time of hire or at the time they assume payment handling responsibilities. Payments may be remitted by online website, mail, telephone, in person or at an Extension open house event. Credit card payments are not to be made by email or fax.

Non-cash payments received outside any enrollment system must be conducted and verified by two employees in the Cashier's office. Cash payments may not be collected at offsite locations or non-approved cash handling sites. The content must be documented in a log, and the supervisor must verify that the posted transactions processed correspond to the payments log. A quarterly audit of the log must be conducted and the log must be retained for 2 years. Credit card information collected on the paper form for enrollments/payments must be redacted after data entry and verification by the bank processor prior to storage.

In accord with UC/UCLA policy, *UC Business and Finance BUS-49*, *UCLA Policy 360* and *361*, all non-cash payments taken off site require that a police/armed escort be present during the processing of payments or enrollments and during the transport of collected payments.

Transmission of Data

If sensitive data must be sent over an open, public network (i.e., the Internet), strong cryptography such as TLS, SSH, or IPSEC must be used to encrypt the data.

If an Extension wireless network is used to transmit sensitive data, strong encryption (i.e. WPA2, IPSEC) must be used.

Strong cryptography must be used whenever sensitive data is sent via end-user messaging technologies (e.g., email, instant messaging, chat).

Malicious Software Protection

ITS will deploy anti-virus software on its information systems commonly affected by malicious software. Such software must be capable of detecting, removing and protecting against all known types of malicious software including spyware and adware.

Anti-virus software must be kept actively running and capable of generating audit logs. Anti-virus software must be enabled for automatic updates and conduct periodic scans.

Patch Management

ITS will have a formal, documented process for regularly identifying and prioritizing relevant and necessary security and functional patches for its information systems and applications that process, transmit or store sensitive data. ITS may use a risk based approach for prioritizing security patch installations. All critical new security patches must be applied within one (1) month of release. A process will be developed to identify and assign a risk ranking (based on security best practices such as CVSS) to newly discovered security vulnerabilities.

Change Control

ITS must develop and implement a formal, documented change control process for information system and software configuration changes. The process must include:

- Identification and documentation of significant changes
- Assessment of the potential impact, including security implications, of significant changes
- Appropriate approval of all changes by authorized parties
- Ability to terminate and recover from unsuccessful changes
- Testing procedures to ensure the change is functioning as intended
- Communication of completed change details to appropriate persons
- The updating of appropriate information system or software documentation upon the completion of a significant change

Only properly authorized persons may make an emergency change to information systems, data or network resources. Such emergency changes must be appropriately documented and promptly submitted, after the change, to ITS's normal change management process.

Network Security

ITS will have and maintain documented standards for its firewalls and routers. Such standards must include:

- A formal process for approving and testing all network connections and changes to firewall and router configurations.
- A current diagram(s) of Extension's computer network. The diagram must show all connections to information systems that process, transmit or store sensitive data. Changes to the diagram(s) must be appropriately documented.
- Requirements for a firewall at each logical point where Extension's network connects to the Internet and between any demilitarized zone (DMZ) and Extension's internal network(s).
- A description of groups, roles, and responsibilities for logical management of network components.
- Documentation and business justification of all services, protocols, and ports allowed by firewalls and routers, including documentation of security features implemented for insecure protocols (e.g. Telnet, FTP).
- A requirement to review Extension's firewall and router rule sets at least every six (6) months.

Extension's firewalls must perform stateful inspection and must restrict connections between untrusted networks (i.e. the Internet) and information systems that process, transmit or store sensitive data. The firewalls will prohibit direct access from the Internet to such information systems, must restrict inbound and outbound traffic to that which is documented as necessary for organizational purposes, and explicitly deny all other traffic.

Configuration files on routers must be secured and regularly synchronized.

A firewall(s) must be installed between any wireless networks and information systems that process, transmit or store sensitive data. Such firewalls will deny or control traffic from any wireless networks to these information systems.

Outbound traffic from payment card applications will be sent to IP addresses within a DMZ; such traffic will not be sent directly to the Internet. Inbound Internet traffic to payment card applications must be limited to IP addresses within the DMZ.

All databases that store sensitive data will be placed in the internal network(s) and be segregated from any DMZ.

Personal firewall software must be installed and active on any mobile and/or employee-owned computers with direct connectivity to the Internet that are used to access the Extension's internal network. The personal firewall software must be configured to specific standards and prevent unauthorized users from altering or disabling it.

IP masquerading (e.g., port address translation [PAT] or network address translation [NAT]) must be used for information systems on Extension's internal network(s).

Security Incident Response

ITS will have a formal, documented security incident response plan that will be reviewed annually by the Dean's Office. The plan will include:

- Roles, responsibilities, and communication strategies in the event of a security incident including notification of appropriate parties
- Specific incident response procedures
- Business recovery and continuity procedures (Cf. policy FA600)
- Data back-up processes
- Legal requirements for reporting security incidents and compromises (e.g. California Information Practices Act);
- Coverage and responses for all critical information systems
- Reference or inclusion of payment card brand incident response procedures
- Procedures for responding to alerts from intrusion detection (IDS), intrusion prevention (IPS) and/or file integrity monitoring systems

The security incident response plan must be tested annually and must designate specific personnel to be available on a 24/7/365 basis in order to respond promptly to information security alerts. The plan must be reviewed regularly and modified as necessary. Lessons learned will be documented.

ITS employees who are responsible for responding to security incidents must receive regular and appropriate training in security incident response processes.

Logging and Auditing

Appropriate logging and monitoring controls will be implemented on information systems, data and network resources.

ITS will implement automated audit trails on its information systems that store, process or transmit sensitive data. The audit trails will be able to reconstruct the following events:

- Individual accesses to sensitive data
- Actions taken by any individual with root or administrative privileges
- Access to all audit trails
- Invalid logical access attempts
- Use of identification and authentication mechanisms
- Initialization of audit logs
- Creation and deletion of system-level objects

For each of the above events, the following must be recorded:

- User identification
- Type of event
- Date and time
- Success or failure indication
- Origination of event
- Identity or name of affected data, system component, or resource

Logs and audit trails on information systems that store, process or transmit sensitive data must be reviewed daily. Such logs and audit trails will be monitored by file integrity or change detection software. Log reviews will include intrusion detection and authentication, authorization and accounting (AAA) servers.

Information generated by logging and monitoring controls implemented on information systems, data and network resources will be protected from unauthorized access. Access to such information will be limited to only those individuals with a need-to-know. Such information must be promptly backed up to a centralized log server and/or media that is difficult to alter. Logs for external-facing technologies (i.e., firewalls, DNS, email) must be promptly copied onto a log server on the internal network. Unless otherwise restricted by law, audit and log file information must be retained for at least one year, with 3 months of log file information being immediately restorable.

UCLA Extension must synchronize with at least one of the following UCLA Campus time servers:

time1.ucla.edu - 164.67.62.194 (stratum 1)

time2.ucla.edu - 164.67.62.212 (stratum 1)

time3.ucla.edu - 164.67.62.198 (stratum 2)

time4.ucla.edu - 164.67.62.213 (stratum 2)

Software Application Development

When Extension develops software applications that store, process or transmit sensitive data, such applications will be developed using a formal, documented software development life cycle and be based on information security best practices.

Security patches and system and software configuration changes on developed applications must be tested before being deployed. Testing must include at least:

- Validation of all input
- Validation of proper error handling
- Validation of secure cryptographic storage
- Validation of secure communications
- Validation of proper role based access control

ITS will have separate development, test and production environments for developed applications that process, transmit or store sensitive data. There must be clear separation of duties between the three environments. Real sensitive data must not be used or must be sanitized for testing or development of developed applications.

Test data and accounts must be removed before developed applications are placed into the production environment. Custom code used in internally developed applications must be reviewed for vulnerabilities before the code is used in the production environment.

Applications developed by ITS that process, transmit or store sensitive data must be based on secure coding best practices such as the Open Web Application Security Project (OWASP) guidelines, SANS CEW Top 25 or CERT Secure Coding. Internally developed Web applications must be protected against the following vulnerabilities:

- Injection flaws (such as SQL Injection)
- Buffer overflow
- Insecure cryptographic storage
- Insecure communications
- Improper error handling
- All “High” vulnerabilities identified during patch management risk ranking process
- Cross-site scripting (XSS) attacks
- Improper access control
- Cross-site request forgery (CSRF)

All Internet accessible Web applications that process, transmit or store sensitive data must be protected against known attacks by either: having an organization specializing in application security review the applications at least annually using manual or automated application vulnerability security assessment tools or methods; or by installing a web-application firewall in front of the applications.

Information System Configuration

ITS will develop and implement formal, documented configuration standards for its information systems. Such standards must be consistent with system hardening best practices as defined by the Center for Internet Security (CIS). At a minimum, the standards will require the following:

- One primary function for servers that process, transmit or store sensitive data
- Disabling of unnecessary and/or insecure services and protocols
- Appropriate configuration of system security settings
- Removal of unnecessary functionality (e.g., scripts, Web servers, subsystems)
- Changing or removing vendor-supplied defaults (i.e., passwords, accounts, SNMP community strings)

All remote logins that enable administrator access to information systems storing, transmitting or processing sensitive data must be encrypted and use two factor authentication.

ITS will have a formal, documented process to identify newly discovered security vulnerabilities and configuration standards to address new vulnerabilities. Configuration standards must be updated to reflect any newly discovered vulnerability.

Personnel Vetting

All employees hired at the University are vetted as part of the recruitment process. Vetting includes background checks for criminal histories and the checking of references. To facilitate career mobility, all new *career* employees at UCLA Extension, whether or not they will have access to sensitive data on their first assignment, will have undergone a criminal background check. *Limited appointment* staff will undergo criminal background checks if hired into areas where they will have access to sensitive information (e.g. cashier, enrollment office).

Extension employees shall be notified of the process for data security, privacy access, and ownership during staff on-boarding. Additionally Extension employees who are authorized to use Extension-owned equipment, including portable devices, shall be made aware of the terms of use and expected due diligence during employment or at employment termination.

Information Security Testing

ITS will annually, or after any significant changes to its information technology environment, perform internal and external penetration tests of its information systems that process, transmit or store sensitive data. The penetration tests will include both network and application layer tests.

At least quarterly, a wireless analyzer will be used at the Extension Administration Building and at metro centers to identify all wireless devices in use or a wireless IDS/IPS must be deployed which is capable of identifying all wireless devices in use at facilities and alerting appropriate personnel upon discovery of devices.

ITS will conduct appropriate quarterly external vulnerability scans against all of its information systems that are Internet reachable. ITS will also run quarterly internal vulnerability scans against all of its information systems that process, transmit or store sensitive data. All internal and external scans must be run until passing results are obtained, or all "High" vulnerabilities are resolved (identified during patch management risk ranking process).

Per its risk assessment, ITS will implement and maintain network IDS, host based IDS and/or IPSs to monitor all traffic to information systems that process, transmit or store sensitive data. IDS/IPS signatures must be kept up-to-date at all times and configured to alert personnel of suspected compromise.

ITS will deploy file integrity monitoring software on its information systems that process, transmit or store sensitive data. The software must perform critical file comparisons at least weekly.

Service Provider Management

If UCLA Extension shares sensitive data with service providers, it will do so in a manner that conforms to UCLA's management practices and policy governing service contracts as well as UCLA Extension, requiring:

- ITS to maintain a list of service providers.
- Written acknowledgement and/or PCI DSS compliant evidence in order to show from each service provider that they are responsible for the security of the sensitive data the service provider possesses or has access to.
- Agreement prohibiting unauthorized disclosure of data to other parties.
- An established process for engaging service providers that includes proper due diligence prior to engagement.
- Development and maintenance of a program to monitor service providers' PCI DSS compliance.

References and Listing

This policy will be publically listed. Questions and comments are welcome by the Extension Director of ITS, (310) 825-4281.

See also:

- UC Business and Finance Policy BUS-49 for Cash and Cash Equivalents Received, September 2008.
- UC Personnel Policies for Staff Members PPSM 21: Selection and Appointment, Section E, December 2017.
- UCLA Policy 360: Internal Control Guidelines for Campus Departments, July 2001.
- UCLA Policy 361: Cash Handling Safety and Security, updated May 2013.
- UCLA Extension policy SA504 Confidentiality of Student and Client Records as amended, May 2016.
- UCLA Extension procedure SA504.1 Procedures Regarding Access to and Disclosure of Information about Students wherein references to all UC policy, California law and related federal law on the subject matter are listed.