Note to Merchants:

This is a generalized template, and many of these policies may not apply to your organization. Your department can also create their own security policy as long as it addresses key aspects of PCI security.

Please contact merchantservices@ucsc.edu or call 831-459-1686 for assistance in editing this document or creating one to suit your organization.

**Information Security Policy**

**for the**

**University of California Santa Cruz**

The enclosed IT security policies have been developed to protect [Department Name] critical operations, partners, assets, staff and customers. Compliance to these policies is mandatory. If you have any questions regarding any of the policies or your responsibilities in implementing them, please contact your supervisor.

*Version 3.2*

*Approval Date: [Date]*

Primary Contact: [PCI Coordinator or Department Head]

**TABLE OF CONTENTS**

[1. Introduction 3](#_Toc416032783)

[2. Roles and Responsibilities 7](#_Toc416032784)

[3. Risk Assessment 7](#_Toc416032785)

[4. Logical Access Control 8](#_Toc416032786)

[5. Physical Access Control 9](#_Toc416032787)

[6. Security Training and Awareness 11](#_Toc416032788)

[7. Employee Technologies 11](#_Toc416032789)

[8. Data Retention and Disposal 12](#_Toc416032790)

[9. Transmission of Data 13](#_Toc416032791)

[10. Malicious Software Protection 13](#_Toc416032792)

[11. Patch Management 13](#_Toc416032793)

[12. Change Control 13](#_Toc416032794)

[13. Network Security 14](#_Toc416032795)

[14. Security Incident Response 15](#_Toc416032796)

[15. Logging and Auditing 16](#_Toc416032797)

[16. Information System Configuration 16](#_Toc416032798)

[17. Personnel Vetting 17](#_Toc416032799)

[18. Information Security Testing 17](#_Toc416032800)

[19. Service Provider Management 18](#_Toc416032801)

[20. Policy Distribution and Review 18](#_Toc416032802)

[21. Compliance 18](#_Toc416032803)

[22. Policy Acknowledgment 19](#_Toc416032804)

###

# Introduction

The data that resides at [Department Name] is of great value to The University of California, Santa Cruz (UCSC). Due to the increasing value of the data we collect, store, process, and share with our partners, it is a high priority for [Department Name] to protect such data. [Department Name] information security policy is consistent with security efforts and practices already in place across the University of California system and [UCSC ITS General Practices for Protecting Electronic Restricted Data](http://its.ucsc.edu/policies/rdpp-general.html#sanction).

The management of [Department Name] is committed to developing, adopting, and maintaining appropriate information security policies, standards and procedures to ensure integration of information security with [Department Name] mission, business strategy, risk posture and in accordance with applicable regulatory guidelines.

This will be accomplished by active UCSC management oversight, effective management and monitoring of information security risks, delineation of clear accountability for information security and establishing appropriate organizational processes to ensure that information security risks are appropriately and regularly identified, monitored and controlled.

This policy applies to all [Department Name] relevant employees (including vendors and business partners). Additionally, this policy is supported by daily operational security procedures that have been developed in conjunction with this policy and existing UCSC security policies.

This policy is necessary in order to maintain [Department Name] compliance with applicable laws and standards, protect the [Department Name] from liability and protect the confidentiality, integrity and availability of [Department Name] information systems, data and network resources.

[Department Name] information security policy represents the combined efforts [Department Name]. UCSC’s Information Technology Services(ITS), Human Resources Department (HR), Finance and user communities. While this policy does refer to local UC Santa Cruz policies, it is the merchant’s responsibility to review those policies on an annual basis and modify polices at the merchant level to ensure PCI compliance.

[Department Name] may at any time, make changes to this policy.

*Reference: PCI DSS v3.2 requirements 12.2, 12.4*

**Document Approval**

|  |  |
| --- | --- |
| **Date of Last Review** | **Name and Title of Approver** |
|  |  |
|  |  |
|  |  |

**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. |
| **Contractor** | A person, or company, that undertakes a contract to provide materials or labor to perform a service or do a job. Also known as “Vendor” or “service Provider” |
| **DMZ** | Demilitarized zone. Network added between a private and a public network to provide an additional layer of security. |
| **Employee** | People employed within the UC system. |
| **Emergency Change** | A change which, due to urgency or criticality, needs to occur outside of the departments 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).  |
| **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 attempted or successful unauthorized access, use, disclosure, modification, or destruction of data or services used or provided by the department.  |
| **Sensitive Data** | Sensitive data is an informal term used to describe information with some level of sensitivity. At the University of California, sensitive data is typically called "Confidential Data". Highly sensitive confidential data is called "Restricted Data".The term confidential information applies broadly to information for which access or disclosure may be assigned some degree of sensitivity, and therefore, for which some degree of protection or access restriction may be warranted. Unauthorized access to or disclosure of information in this category could result in a serious adverse effect, cause financial loss, cause damage to the University’s reputation and loss of confidence or public standing, constitute an unwarranted invasion of privacy, or adversely affect a partner, e.g., a business or agency working with the University.Restricted data or information [1]: Any confidential or personal information that is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transit. The term should not be confused with that used by the UC-managed national laboratories where federal programs may employ a different classification scheme.At UCSC, restricted data includes, but is not necessarily limited to Personal Identity Information (PII), Electronic protected health information (PHI), personally identifiable information (PII), bank account numbers and tax ID numbers that are stored, processed or transmitted on or by information systems or network resources.ePHI) protected by Federal HIPAA legislation, Credit card data regulated by the Payment Card Industry (PCI), Information relating to an ongoing criminal investigation, Court-ordered settlement agreements requiring non-disclosure, Information specifically identified by contract as restricted, Other information for which the degree of adverse effect that may result from unauthorized access or disclosure is high. |
| **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 the department. |
| **Multi-Factor Authentication** | The use of two, or more, independent mechanisms for authentication. For example, a security token and a password. |
| **User** | Anyone who accesses the departments information systems, data or network resources. |
| **Visitor** | A vendor, guest of an employee, service personnel, or anyone who needs to enter a secure or sensitive facility containing information systems, data or network resources for a short duration, usually not more than one day. |

# Roles and Responsibilities

While responsibility for information security on a day-to-day basis is every [Department Name] employee’s duty, specific guidance, direction, and authority for information security is the responsibility of Division of Graduate Studies Security Committee. The Security Committee is comprised of Departmental Head, Business and Systems Analyst, PCI Coordinator, and IT staff and has been assigned the day-to-day responsibilities for information security to [Department Name] Information Technology Services (ITS) Department. Accordingly, this Department will:

* Establish, document and distribute information security policies, standards and procedures.
* Monitor and analyze security alerts & information and distribute to appropriate [Department Name] 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*

*Reference: PCI DSS v3.2 requirement 12.5 (12.5.1 – 12.5.5*)

# Risk Assessment

The [Department Name] has incorporated PCI specific risk assessment policies and processes into their official procedures, which are consistent with UC Santa Cruz campus procedures located at <http://its.ucsc.edu/policies/breach-procedures.html>

[Department Name] must regularly identify, define, and prioritize risks to the confidentiality, integrity, and availability of its information systems, network resources and data. [Department Name] must conduct an annual formal, documented risk assessment of its information systems, data and network resources. The assessment must identify and prioritize the threats and vulnerabilities to [Department Name] information systems, data and network resources and define the likelihood and impact of risks.

The risk assessment must be used in conjunction with [Department Name] risk management process to identify, select, and implement appropriate and reasonable controls to protect the confidentiality, integrity, and availability of [Department Name] information systems, network resources, and data.

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

Annually, [Department Name] PCI Coordinator must submit an information security risk management report to appropriate [Department Name] management. The report must identify the significant risks to [Department Name] 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.

*Reference: PCI DSS v3.2 requirement 12.1.2*

# Logical Access Control

In conjunction with the [UCSC Campus Password Policy](http://policy.ucsc.edu/policies/its/it0002.html), the following is required for PCI compliance.

[Department Name] employees, contractors, council members, service providers and vendors must not attempt to gain logical access to [Department Name] information systems, data or network resources for which they have not been given proper authorization.

Logical access to [Department Name] information systems and media containing sensitive data must be denied until specifically authorized by appropriate [Department Name] personnel.

Appropriate [Department Name] information system owners and/or data custodians or their designated delegates must define and approve logical access to [Department Name] information systems and media containing sensitive data.

Logical access to [Department Name] information systems and media 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.

[Department Name] will follow the formal [UCSC Local Procedures](http://shr.ucsc.edu/procedures) that documents the user management process which enables the controlled addition, change, and termination of logical access rights on [Department Name] information systems, data and network resources. The process must be capable of granting different levels of access to [Department Name] information systems, data and network resources.

A unique user name must be used by all persons accessing [Department Name] information systems and media containing sensitive data. Along with the unique user name, one of the following authentication methods must be used:

* Password
* Token devices
* Biometrics

Multi-factor authentications must be used by employees, contractors, service providers and vendors for remote access to [Department Name] information systems and media containing sensitive data. [Department Name] employees who telecommute must take all precautions necessary to secure any and all sensitive [Department Name] data in their homes and prevent unauthorized access to any [Department Name] information system or data.

Vendor maintenance accounts and ports on [Department Name] 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 must not be used on [Department Name] 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 [Department Name] personnel unlock the account.
* [Department Name] employees must not use passwords that are also used for non-[Department Name] accounts.

Activation of information system locking software or log off must occur when a user session on a [Department Name] workstation information system is inactive for more than 15 minutes.

User identity must be appropriately verified before any password, which enables access to a [Department Name] information system or network resource, is reset.

User accounts that are inactive for more than 90 days on [Department Name] information systems that store, process or transmit sensitive data must be disabled or removed.

At least every 6 months, appropriate [Department Name] information system owners and/or data custodians or their designated delegates must review and verify logical access rights to [Department Name] information systems and media containing sensitive data. Such rights must be revised as necessary. Inactive accounts over 90 days old must be either removed or disabled.

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

*Reference: PCI DSS v3.2 requirements 7.1 (7.1.1 – 7.1.4), 7.2 (7.2.1 – 7.2.3), 8.1, 8.2, 8.3 (8.3.1-8.3.2), 8.5 (8.5.1 - .16)*

# Physical Access Control

At least annually, [Department Name] must identify 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.

[Department Name] information systems and electronic & non-electronic media containing sensitive data must be located in physically secure areas (“limited access area”). Typically, such areas have a defined security perimeter such as a card controlled entry door or a staffed reception desk. [Department Name] 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 [Department Name] 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.

Access to controlled network areas are managed by Information Technology Services per local [UCSC ITS Facilities Policy](http://its.ucsc.edu/internal/facilities.html).

Cameras or other access control mechanisms must monitor the entry and exit points of [Department Name] physical areas containing information systems that store, process or transmit sensitive data or electronic & 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.

[Department Name] must 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 [Department Name] facilities.

Backup media, both paper and electronic, that contains sensitive [Department Name] data must be stored in a secure location. The location’s security must be reviewed at least annually. An inventory of all such media must 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, must 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).

[Department Name] electronic and non-electronic media containing sensitive data must be classified so that it can identified as “confidential.” Distribution of such media outside the [Department Name] must be tracked and logged. Such media must only be distributed outside [Department Name] via a delivery method that can be tracked (such as secure courier).

Appropriate [Department Name] management must approve the movement of any [Department Name] media containing sensitive data from a limited access area.

[Department Name] must have a formal, documented process in place that clearly identifies and distinguishes between employees, contractors, and visitors.

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

*Reference: PCI DSS v3.2 requirements 9.1 (9.1.1 – 9.1.2), 9.2, 9.3 (9.3.a – 9.3.c), 9.4, 9.5, 9.6, 9.7, 9.8 (9.8.1 – 9.8.2), and 9.9*

# Security Training and Awareness

[Department Name] must ensure that employees and contractors are provided with sufficient training and supporting reference materials to enable them to appropriately protect [Department Name] information systems, network resources, and data. [Department Name] must provide [information security awareness](https://financial.ucsc.edu/Pages/PCI_DSS_Print.aspx) to its employees and contractors upon hire and then at least annually.

[Department Name] must provide regular security information and awareness to its employees and contractors via methods such as log-in banners, posters, web-based training, memos and periodic meetings. Such information and awareness must include, but is not limited to:

* Any significant revisions to [Department Name] information security policies
* Significant new [Department Name] information security controls or processes
* Significant changes to [Department Name] information security controls or processes
* Significant new security threats to [Department Name] information systems, network resources, or data
* Information security best practices

Employees must acknowledge, at least annually, that they have read and understood [Department Name] information security policy.

*Reference: PCI DSS v3.2 requirements 12.6 (12.6.1 – 12.6.2), 12.7*

# Employee Technologies

Employee technologies (i.e., remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, PDAs) that access sensitive [Department Name] data must only be used by employees and contractors if the following controls are in place:

* Appropriate [Department Name] management approval for the use of the technologies
* Appropriate authentication with ID and password 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
* [Department Name] maintains a regularly updated list of approved devices

When payment card data on [Department Name] information systems is remotely accessed, the data must 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 [Department Name] 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 [Department Name] information systems containing sensitive data must be turned off when not in use by the vendors.

*Reference: PCI DSS v3.2 requirements 12.3 (12.3.1 – 12.3.4, 12.3.6 – 12.3.10*)

# Data Retention and Disposal

[Department Name] must keep the storage of sensitive data to the minimum necessary required for business, legal and/or regulatory purposes. When no longer required for such purposes, sensitive data on [Department Name] information systems or on [Department Name] electronic and non-electronic media must be appropriately disposed of. The following disposal methods must 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 on [Department Name] electronic media and information systems must be securely and thoroughly erased before such items can be re-used

[Department Name] information systems and electronic & 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 [Department Name] data retention requirements.

After a payment card transaction is authorized, the following types of data must never be stored in electronic or non-electronic form at a [Department Name] facility:

* Magnetic stripe data
* CVC2/CVV2/CID/CAV2
* PIN/PIN Block

Unless otherwise authorized, credit card primary account numbers (PANs) on [Department Name] information systems must be masked; the first six (6) and the last four (4) digits of the PAN are the maximum that can be displayed.

PANs stored electronically on [Department Name] information systems or portable storage devices must be made unreadable. One of the following methods must be used:

* Strong one-way hash functions
* Truncation
* Index tokens and pads
* Strong cryptography

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.

*Reference: PCI DSS v3.2 requirements 3.1, 3.2 (3.2.1 – 3.2.3), 3.3, 3.4, 3.5, 3.6, 9.10*

# Transmission of Data

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

If a [Department Name] 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).

*Reference: PCI DSS v3.2 requirements 4.1, 4.2*

# Malicious Software Protection

[Department Name] must deploy anti-virus software on its information systems commonly affected by malicious software. Such software must be capable of detecting, removing and protecting against 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.

Additional information regarding UCSC Information technology anti-virus policy can be found on the OCS website [Information Technology Services](http://its.ucsc.edu/vpn/security.html).

*Reference: PCI DSS v3.2 requirements 5.1, 5.2, 5.3.*

# Patch Management

[Department Name] must 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. [Department Name] 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.

*Reference: PCI DSS v3.2 requirements 6.1, 6.2***.**

# Change Control

[Department Name] abides by the UCSC ITS, documented change control process for information system and software configuration changes list in the formal [ITS change management documentation](http://its.ucsc.edu/change-mgmt/index.html). 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 [Department Name] information systems, data or network resources. Such emergency changes must be appropriately documented and promptly submitted, after the change, to [Department Name] normal change management process.

*Reference: PCI DSS v3.2 requirements 6.4 (6.4.1 – 6.4.4)*

# Network Security

[Department Name] will utilize documented standards, set by UCSC ITS for its firewalls and routers. Such standards must include:

* A formal process for approving and testing all network connections and changes to [Department Name] firewall and router configurations.
* Current diagram(s) of [Department Name] computer network. The diagram must show all connections to [Department Name] 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 [Department Name] network connects to the Internet and between any demilitarized zone (DMZ) and [Department Name] internal network(s).
* A description of groups, roles, and responsibilities for logical management of [Department Name] network components.
* Documentation and business justification of all services, protocols, and ports allowed by [Department Name] firewalls and routers, including documentation of security features implemented for insecure protocols (e.g. Telnet, FTP).
* A requirement to review [Department Name] firewall and router rule sets at least every six (6) months.

[Department Name] firewalls must perform stateful inspection and must restrict connections between untrusted networks (i.e. the Internet) and [Department Name] information systems that process, transmit or store sensitive data. The firewalls must 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 [Department Name] routers must be secured and regularly synchronized.

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

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

All [Department Name] databases that store sensitive data must be placed in the [Department Name] internal network(s) and be segregated from any [Department Name] DMZ.

Personal firewall software must be installed and active on any mobile and/or [Department Name] employee-owned computers with direct connectivity to the Internet that are used to access the [Department Name] 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 [Department Name] internal network(s).

*Reference: PCI DSS v3.2 requirements 1.1 (1.1.1 – 1.1.7), 1.2 (1.2.1 – 1.2.3), 1.3 (1.3.1 – 1.3.7), 1.4*.

# Security Incident Response

[Department Name] security incident response is driven by UCSC ITS Security Breach Response Plan and the [Department Name] Business Continuity Plan. The plan must 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
* Data back-up processes
* Legal requirements for reporting security incidents and compromises
* Coverage and responses for all critical [Department Name] 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.

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

*Reference: PCI DSS v3.2 requirements 12.10 (12.10.1 – 12.10.6)*

# Logging and Auditing

Appropriate logging and monitoring controls must be implemented on [Department Name] information systems, data and network resources consistent with the [campus log policy](http://policy.ucsc.edu/policies/its/it0005.html) and [procedures](http://its.ucsc.edu/policies/log-procedures.html).

[Department Name] must implement automated audit trails on its information systems that store, process or transmit sensitive data. The audit trails must 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 [Department Name] information systems that store, process or transmit sensitive data must be reviewed daily. Such logs and audit trails must be monitored by file integrity or change detection software. Log reviews must include intrusion detection and authentication, authorization and accounting (AAA) servers.

Information generated by logging and monitoring controls implemented on [Department Name] information systems, data and network resources must be protected from unauthorized access. Access to such information must 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 [Department Name] external-facing technologies (i.e., firewalls, DNS, email) must be copied onto a log server on the [Department Name] internal network. Unless otherwise restricted by law, audit and log file information must be retained for at least one year.

[Department Name] information systems must have their system clocks and times synchronized with a master time source (e.g. network time protocol [NTP]). Internal [Department Name] time servers must not all receive time signals from external sources. Specific Internet time servers must be designated from which time updates will be accepted.

*Reference: PCI DSS v3.2 requirements 10.1, 10.2 (10.2.1 – 10.2.7), 10.3 (10.3.1 – 10.3.6), 10.4, 10.5 (10.5.1 – 10.5.5), 10.6, 10.7, 10.8, 10.9.*

# Information System Configuration

[Department Name] must develop and implement formal, documented configuration standards for its information systems. Such standards must be consistent with system hardening best practices as defined by organizations such as SANS, NIST and CIS. At a minimum, the standards must require the following:

* One primary function for servers that process, transmit or store sensitive data
* Disabling of unnecessary and/or insecure services and protocols aligns with part of campus minimum [network connectivity requirements policy](http://policy.ucsc.edu/policies/its/it0004.html).
* 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 [Department Name] information systems storing, transmitting or processing sensitive data must be encrypted.

[Department Name] must have a formal, documented process to identify newly discovered security vulnerabilities and update [Department Name] configuration standards to address new vulnerabilities. Configuration standards must be updated to reflect any newly discovered vulnerabilities.

*Reference: PCI DSS v3.2 requirements 2.1, 2.2 (2.2.1 – 2.2.4), 2.3, 2.4, 6.2*

# Personnel Vetting

As determined necessary by [Department Name] risk assessment, new [Department Name] employees must be subject to the guidelines of the UCSC Staff Human Resources “Back Ground Check” Policy. Such vetting can include, but is not limited to, background checks, credit checks and/or personal references. Such vetting is especially important for positions that involve access to sensitive data.

New employees who will access sensitive data must sign a confidentiality (non-disclosure) agreement. This agreement must be renewed on an annual basis.

Reference: PCI DSS v3.2 requirements 12.7

# Information Security Testing

[Department Name] must 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 must include both network and application layer tests.

At least quarterly, a wireless analyzer must be used at [Department Name] facilities 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 [Department Name] facilities and alerting appropriate personnel upon discovery of devices.

[Department Name] must conduct appropriate quarterly external vulnerability scans against all of its information systems that are Internet reachable. [Department Name] must 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, [Department Name] must implement and maintain network IDS, host based IDS and/or IPSs to monitor all traffic to [Department Name] information systems that process, transmit or store sensitive data.

[Department Name] must 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.

*Reference: PCI DSS v3.2 requirements 11.1, 11.2, 11.3 (11.3.1 – 11.3.2), 11.4, 11.5*.

# Service Provider Management

If [Department Name] shares sensitive data with service providers, then [Department Name] must develop and maintain a service provider management program that meets, at minimum, the following requirements:

* + Maintenance of a list of service providers.
	+ Written acknowledgement from each service provider that they are responsible for the security of the sensitive data the service provider possesses or has access to.
	+ 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.

*Reference: PCI DSS v3.2 requirement 12.8 (12.8.1 – 12.8.5)*

# Policy Distribution and Review

This policy must be published and distributed to all appropriate [Department Name] parties (employees, contractors, vendors, service providers and business partners).

This policy must be reviewed at least annually and revised as necessary.

*Reference: PCI DSS v3.2 requirements 12.1, 12.1.1*

# Compliance

Per the UCSC ITS [Sanctions Policy](http://its.ucsc.edu/policies/sanction.html); [Department Name] employees and contractors must comply with all applicable parts of this security policy. Compliance is necessary to ensure the confidentiality, integrity and availability of [Department Name] information systems, data and network resources.

[Department Name] employees and contractors who do not comply with all applicable [Department Name] security policies may be subject to disciplinary actions, up to and including termination of employment.

Third party persons (i.e. vendors, service providers) who do not comply with this policy may be subject to appropriate actions as defined in contractual agreements.

**Policy Acknowledgment**

I have received a copy of [Department Name] Information Security Policy and I have read and understand the policy. I agree to observe the terms and conditions of this policy.

Signed Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_