User Guidelines for Information Security Contract Language	Guidelines No.	ITS-1022-G	Rev:	A
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director IT Security and Compliance		
	Issued:	8-4-11	Revised:	5-27-15
				Page 1 of 14

Table of Contents

1 Purpose 2
2 Entities Affected by these Guidelines 2
3 Definitions 2
4 Guidelines 4
4.1 General Service Provider Responsibilities 4
4.1.1 Third-party Service Providers with Direct Access to Protected Data 4
4.1.2 Third-party Service Providers with Indirect Access to Protected Data 5
4.2 Data at Rest 5
4.3 Data in Transit 6
4.4 Data in Use 6
4.5 Return or Destruction of Data 6
4.6 Protected Data 7
4.7 Laws and Regulations Compliance 7
4.8 Third-party Service Provider Personnel and Subcontractors 8
4.9 Information Security Breach 8
4.9.1 Pre-Breach 8
4.9.2 Breach Notification 9
4.9.3 Breach Report 9
4.10 Contract Termination 10
5 Contacts 10
6 Applicable Federal and State Laws and Regulations 10
7 Related Documents 12
8 Appendices 14
8.1 Information Security Contract Language Templates 14
8.1.1 ITS-2827 Information Security Contract Language for Third-party Service Providers with Direct Data Access 14
8.1.2 ITS-2828 Information Security Contract Language for Third-party Service Providers with Indirect Data Access 14

1 Purpose

A significant step Cal State L.A. must take to safeguard information security is to define by agreement the security procedures its third-party service providers are required to uphold. Outsourced services provided by third-party service providers inherently increase the level of risk within an organization. It is critical to Cal State L.A. that each third-party service provider protects the integrity and security of University protected data.

The purpose of these guidelines is to define the information security responsibilities and procedures that apply to all third-party service providers. In addition to these guidelines, forms *ITS-2827 Information Security Language for Third-party Service Providers with Direct Data Access* and *ITS-2828 Information Security Language for Third-party Service Providers with Indirect Data Access* provide templates with the specific language that can be included in all agreements with third-party service providers to ensure appropriate safeguards and processes are in place to protect the University's information and that, if needed, the third-party service provider is prepared to respond to an information security incident.

2 Entities Affected by these Guidelines

These guidelines are a tool for all University employees who are responsible for preparing, evaluating, administering and terminating contracts, agreements, service orders, purchase requisitions or other procurement documents with third-party service providers who may directly or indirectly come in contact with Cal State L.A. protected data.

These guidelines apply to all third-party service providers working on or for the Cal State L.A. campus.

3 Definitions

a) Confidential Information: See Level 1 Confidential Data and Level 2 Internal Use Data. Confidential information must be interpreted in combination with all information contained on the computer or electronic storage device to determine whether a security violation has occurred.

b) Data at Rest: All data recorded on storage media that is not traversing the network or in use.

c) Data in Transit: All data being transferred.

d) Data in Use: All data not at rest.

e) Electronic Storage Media**:** Electronic or optical data storage media or devices including, but not limited to, the following: computer hard drives, laptops, smartphones, tablets, magnetic disks, CDs, DVDs, flash drives, memory sticks, tapes and any emerging technology capable of processing or storing data. Also called memory devices.

f) Health Insurance Information: An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

g) Information Security Breach: According to California Senate Bill (SB) 1386: A situation where "…unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

h) Level 1 Confidential Data: Confidential information is information maintained by the University that is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws. Its unauthorized use, access, disclosure, acquisition, modification, loss or deletion could result in severe damage to the CSU, its students, employees or customers. Financial loss, damage to the CSU's reputation and legal action could occur if data is lost, stolen, unlawfully shared or otherwise compromised. Level 1 information is intended solely for use within the CSU and limited to those with a "business need-to-know." Statutes, regulations, other legal obligations or mandates protect much of this information. Disclosure of Level 1 information to persons outside of the University is governed by specific standards and controls designed to protect the information. Confidential information must be interpreted in combination with all information contained on the computer or electronic storage device to determine whether a violation has occurred.

i) Level 2 Internal Use Data: Internal use information is information that must be protected due to proprietary, ethical or privacy considerations. Although not specifically protected by statute, regulations or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification, loss or deletion of information at this level could cause financial loss, damage to the CSU's reputation, violate an individual's privacy rights or make legal action necessary. Non-directory educational information may not be released except under certain prescribed conditions.

j) Medical Information: Any information regarding an individual's medical history, mental or physical condition or medical treatment or diagnosis by a health care professional.

k) Node: In networks, a processing location. A node can be a computer or some other device, such as a printer.

l) Personal Information: California Civil Code 1798.29 defines personal information as: An individual's first name or first initial and last name in combination with any one or more of the following data elements:
   - Social Security number
   - Driver's license or California Identification Card number
   - Account number or credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account
   - Medical information
   - Health insurance information

m) Proprietary Information: Information that an individual or entity possesses, owns or for which there are exclusive rights. Examples include: faculty research, copyrighted or patented materials, white papers, research papers, business continuity and other business operating plans, email messages, vitae, letters, confidential business documents, organization charts or rosters, detailed building drawings and network architecture diagrams. Proprietary information, if lost or stolen, could compromise, disclose or interrupt operations or embarrass the individual or the University.

n) Protected Data: An all-encompassing term that includes any information defined herein as confidential, personal, proprietary, health insurance or medical information. See Level 1 Confidential Data and Level 2 Internal Use Data.

o) Security Breach: Unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information maintained on it.

p) Third-party Service Providers: Refers to an entity that is undertaking an outsourced activity on behalf of the University or is performing system administrator duties on their offsite system that contains University protected data (e.g., vendors, vendor's subcontractors, business partners, consultants, etc.).

4 Guidelines

Third-party service providers generally fall into two categories:

- Providers with **direct** access to protected data – e.g., system designers; equipment or system installers; maintenance technicians; application developers; consultants; student service providers that require the use of Cal State L.A. protected data; recipients of Cal State L.A. protected data for reporting purposes; and the like. These providers are generally granted access to the equipment or protected data to perform the specific tasks and responsibilities detailed in the approved Purchase Requisition, service contract, scope of work or other official procurement document. They must submit an Information Confidentiality/Non-disclosure Agreement found at http://www.calstatela.edu/its/services.php under Third-party Service Providers.
- Providers with **indirect** access to protected data – e.g., office equipment installers or maintenance personnel; painters; electricians; plumbers; carpet installers or cleaners; furniture delivery or assembly personnel and the like. These providers may come in contact indirectly with protected data in the work area, such as that visible on a computer screen, in use at a desk or laying on a file cabinet, copier or fax machine.

4.1 General Service Provider Responsibilities

4.1.1 Third-party Service Providers with Direct Access to Protected Data

All third-party service providers with direct access to protected data shall agree to:

- Not use or disclose University information or remove from an office where it is maintained any official record or report or copy thereof, whether paper or electronic, except as permitted or required by the Agreement or as otherwise authorized in writing by the University.
- Not make University information available to any employees, contractors or agents of the third-party service provider except those with a need to know and agreed by the Agreement.
- Attest that its employees, agents and associates involved in the performance of the Cal State L.A. Agreement are bound by its terms.
- Not distribute, repurpose or share data across other applications, environments or business units of third-party service provider.
- Implement appropriate measures to ensure the security and confidentiality of all University information, including protecting against unauthorized access of or use of the University information that could result in substantial harm or inconvenience to the University.

- Regularly review the compliance of information processing within the area of responsibility with the appropriate security policies, standards and any other security requirements. If non-compliance is found as a result of the review:
  - Determine the cause of the non-compliance.
  - Evaluate the need for actions to ensure that non-compliance does not recur.
  - Determine and implement appropriate corrective action for all non-compliance issues.
  - Conduct a periodic review of the correction action taken in all non-compliance issues.

4.1.2 Third-party Service Providers with Indirect Access to Protected Data

All third-party service providers with indirect access to protected data shall agree to:

- Not use or disclose University information or remove from an office where it is maintained any official record or report or copy thereof, whether paper or electronic.
- Not make University information available to any employees, contractors or agents of the third-party service provider.
- Attest that its employees, agents and associates involved in the performance of the Cal State L.A. Agreement are bound by its terms.
- Not distribute, repurpose or share data across other applications, environments or business units of third-party service provider.
- Implement appropriate measures to ensure the security and confidentiality of all University information, including protecting against unauthorized access of or use of the University information that could result in substantial harm or inconvenience to the University.

4.2 Data at Rest

If the third-party service provider has responsibility for storing Cal State L.A. information, the third-party service provider shall agree to:

- Use strong encryption for all protected data in any format whatsoever regardless of the electronic storage media and ensure that the password is not present on the media itself or on the node associated with the media.
- Store any and all Cal State L.A. data solely on designated target servers.
- Not store Cal State L.A. data at any time on any portable or laptop computing device or any portable storage medium, unless the storage medium is in use as part of the third-party service provider's designated backup and recovery process and has been approved for use by the University.
- Implement the following security controls on each server, workstation or portable (e.g., laptop computer) computing device that stores protected data:
  - Network-based firewall or personal firewall.
  - Continuously update anti-virus software.
  - Patch-management process including installation of all operating system/software third-party service provider security patches.
  - Upgrade and maintain at the current release level any middleware, operating systems and other software used by the service provider of Cal State L.A. applications.
- Maintain an inventory of the records being retained.
- Prohibit, directly or indirectly, the inclusion of any false, inaccurate or misleading entries into any records.

4.3 Data in Transit

If the third-party service provider has responsibility for the transit of Cal State L.A. information, the third-party service provider shall agree to:

- Limit remote access rights to on-demand situations, subject to Cal State L.A.'s current information security and access policies (e.g., type of secure connection to be used, coordination with information security personnel, etc.).
- If a connection is to be used for rendering support, the third-party service provider shall use the connection only for that purpose and is responsible for the security of the connection on the third-party service provider's side.
- Clearly identify exactly what, how and when information will be transmitted from their systems.
- Encrypt all files in transit containing protected information between the third-party service provider's off site location and Cal State L.A. The University will work with the third-party service provider to establish mutually accepted encryption standards.
- Ensure that a third host cannot eavesdrop on a communication between the third-party service provider and Cal State L.A.
- Not use a fax to transmit protected information because of the insecurity of the transmission.

4.4 Data in Use

If the third-party service provider has responsibility for the use of Cal State L.A. information, the third-party service provider shall agree to:

- Implement the following security controls on each server, workstation or portable (e.g., laptop computer) computing device that processes protected data:
    - Network-based firewall or personal firewall.
    - Continuously update anti-virus software.
    - Patch-management process including installation of all operating system/software third-party service provider security patches.
    - Upgrades and maintain at the current release level any middleware, operating systems and other software used by the third-party service provider for Cal State L.A. applications.
- Any and all Cal State L.A. data will be processed solely on designated target servers.
- Prohibit, directly or indirectly, the inclusion of any false, inaccurate or misleading entries into any records or reports.

4.5 Return or Destruction of Data

Upon termination, cancellation, expiration or other conclusion of the Agreement, the third-party service provider shall agree to:

- Return all data to the University, unless the University requests that the data be destroyed. This provision shall also apply to all University data that is in the possession of subcontractors or agents of the third-party service provider.
- Provide evidence of destruction if the University has requested the data be destroyed. The destruction of the data shall be completed within 30 days of the termination of the Agreement and evidence of the destruction of the data shall be provided to the University in writing.
- Not retain a copy of the data.

4.6 Protected Data

A third-party service provider who stores, transmits or uses Cal State L.A. protected data as required in the Agreement or has physical access to facilities or computer systems and such access presents the potential for incidental access or inadvertent disclosure of protected data, shall agree to:

- Acknowledgment that its Agreement with Cal State L.A. may allow the third-party service provider access to confidential University information including, but not limited to, personal information, student records, health care information or financial information, which is subject to federal and state legal standards and obligations as well as CSU and Cal State L.A. policies that restrict the use and disclosure of such information (see Section 4.7 below).
- Not disclosing to third parties any protected data except as required by law or with the express written consent of Cal State L.A. The University shall be immediately notified in writing of any subpoena, court order or other legal process seeking or purporting to compel disclosure of Cal State L.A. protected data and shall have the opportunity to challenge, oppose or appeal any such subpoena, order or legal process to the extent deemed appropriate by the University.
- Holding protected data in strictest confidence, protected and accessed only for the explicit business purpose agreed upon with the University.
- Use strong encryption for all protected data.

4.7 Laws and Regulations Compliance

Third-party service providers must abide by all state and federal legal standards and obligations as well as CSU policies and Cal State L.A. standards and guidelines when storing, transmitting, using, disposing and disclosing University information, working in areas where protected data may be in use by others or otherwise exposed. These documents include, but are not limited to:

- California Civil Code (Sections 1798.29, 1798.82, 1798.84, 1798.85), as amended by SB 1386 (2003), 1298 (2007) and SB 24 (2011). This code requires that any breach of unencrypted personal information must be disclosed to the affected individuals whose information was disclosed or that is reasonably believed to have been disclosed and requires notification to the Attorney General if more than 500 residents are involved. The University interprets the Code to include both electronic and written information.
- FERPA - The Family Education Privacy Rights Act (Title 20, United States Code, Section 1232g) is applicable to student records and information from student records.
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- The California Information Practices Act of 1977
- Payment Card Industry Data Security Standard (PCI DSS)
    - Third-party service provider must provide a certificate of compliance with the Payment Card Industry Data Security Standard prior to engagement and must provide an updated certificate of compliance to Cal State L.A. annually thereafter for the duration of the Agreement.
    - Any changes in third-party service provider's certification require prompt written notification to Cal State L.A.
    - If applicable, third-party service provider agrees that their electronic check processing functionality will comply with the appropriate NACHA - The Electronic Payment Association's provisions. Applications purchased from a third-party that will be used by a Merchant to store, process or transmit sensitive cardholder data must be Payment Application Best Practices (PABP) certified. This certification ensures that the application is compatible with PCI requirements.

- Americans with Disabilities Act of 1990, as amended
- Gramm-Leach-Bliley Act (Title 15, United States Code, Section 6801(b) and 6805(b)(2) applicable to financial transactions.
- CSU policies, and
- University standards and guidelines.

4.8 Third-party Service Provider Personnel and Subcontractors

If a third-party service provider has personnel or has subcontractors who may store, transmit or use University information or may have physical access to facilities or computer systems and such access presents the potential for incidental access or inadvertent disclosure of protected data, the third-party service provider and its subcontractors shall agree to:

- Identify in writing the person who will be responsible for overall security for the third-party service provider.
- Not allow the substitution of personnel assigned to work when "regular, full time company employees" in the technical positions are not available, without knowledge or permission of the University.
- Perform appropriate background investigations of all team members and certify that all individuals who will be involved have cleared the background investigation.
- Use reasonable measures to ensure information security compliance by employees who assist in the performance of functions or activities under this Agreement. Such measures shall include informing each employee or agent who receives protected data of the obligations associated with that information.
- Implement appropriate authentication methods to ensure information system access to protected data is only granted to properly authenticated and authorized persons, including the use of strong passwords.

4.9 Information Security Breach

4.9.1 Pre-Breach

If the Cal State L.A. administrator entering into an agreement with a third-party service provider determines that the outsourced function is critical to Cal State L.A. processes, appropriate business continuity planning by the third-party service provider is needed to ensure the availability of the function.

If a third-party service provider's function is deemed to be critical to Cal State L.A. processes, the third-party service provider shall agree to:

- Guarantee that a disaster recovery plan exists, including off-site storage of data in a secure location. Cal State L.A. must approve the off-site storage of the data and the University retains the right to reject the location for security reasons and to recommend another location.
- Provide a copy of the plan to the University.
- Identify the timeframe that any services considered mission critical are to be restored.
- Test the plan annually with results provided to Cal State L.A.
- Provide Cal State L.A. with operating procedures the service provider and the University are to implement in the event business resumption contingency plans are implemented.
- Assume notification expenses including the University's out-of-pocket costs if the security breach has occurred due to the third-party service provider's negligence.

4.9.2 Breach Notification

When the third-party service provider discovers that there may have been a breach in security, which has or may have resulted in compromising protected data, it shall agree to:

- Immediately (within two hours of discovery) notify Cal State L.A.
- Assume responsibility for informing all individuals whose information may have been compromised in accordance with applicable law.
- Indemnify, hold harmless and defend California State University System and its trustees, officers and employees and Cal State L.A. and its officers and employees from and against any claims, damages or other harm related to such notification.
- Not notify those whose data have been or may have been exposed without prior discussion with Cal State L.A.

The third-party service provider shall notify:

Mr. Peter Quan
Vice President for Information Technology Services and Chief Technology Officer
California State University, Los Angeles
323-343-2700
ITSecurity@calstatela.edu

4.9.3 Breach Report

The third-party service provider shall agree to provide a report regarding the breach to the University information security officer. The report shall identify:

- The nature of the unauthorized use or disclosure.
- The University protected data used or disclosed.
- Who made the unauthorized use or received the unauthorized disclosure.
- What has been done or shall be done to mitigate any harmful effect of the unauthorized use or disclosure.
- What corrective action has been taken or shall be taken to prevent future similar unauthorized uses or disclosures.
- Other information, as reasonably requested by the University.

This report will be provided as soon as possible but no later than 48 hours of breach notification. The report shall be updated weekly as more information becomes available.

The third-party service provider shall notify:

Ms. Sheryl Okuno
Director, IT Security and Compliance
California State University, Los Angeles
323-343-2600
ITSecurity@calstatela.edu

4.10 Contract Termination

The University shall have the right to immediately terminate a contract if the third-party service provider has violated an information security standard or procedure.

5 Contacts

a) To report an information security breach, contact the vice president for Information Technology Services and chief technology officer, 323-343-2700, Library PW 1070 or ITSecurity@calstatela.edu.

b) To submit an information security breach report, contact the director of IT Security and Compliance, 323-343-2600, Library PW 1070 or ITSecurity@calstatela.edu.

c) Address questions regarding this standard to: ITSecurity@calstatela.edu.

d) Address questions regarding purchase requisitions, service orders and procurement contracts to: director of Procurement, 323-343-3480, ADM 503.

6 Applicable Federal and State Laws and Regulations

Federal	Title
Family Educational Rights and Privacy Act (FERPA)	**Family Educational Rights and Privacy Act (FERPA)** http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html This is a federal law that protects the privacy of student education records.
Gramm-Leach-Bliley Act Title 15 USC, Subchapter I, Sec. 6801-6809	**Gramm-Leach-Bliley Act** http://www.ftc.gov/privacy/glbact/glbsub1.htm This is a federal law on the disclosure of nonpublic personal information.
Health Insurance Portability & Accountability Act (HIPAA), 45 C.F.R. parts 160 & 164	**Standards for Privacy of Individually Identifiable Health Information** http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/prdecember2000all8parts.pdf This is a federal law that protects the privacy of health records.
U.S. Copyright Office	**United States Digital Millennium Copyright Act** For a comprehensive summary, visit: http://www.copyright.gov/legislation/dmca.pdf The legislation implements two 1996 World Intellectual Property Organization (WIPO) treaties: the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty. The DMCA also addresses a number of other significant copyright-related issues.

Federal	Title
Federal Privacy Act of 1974	**Federal Privacy Act of 1974** http://www.usdoj.gov/opcl/privacyact1974.htm Establishes a code of fair information practices that governs the collection, maintenance, use and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies.
Sarbanes-Oxley Act of 2002 (Public Law 107-204)	**Sarbanes-Oxley Act of 2002** http://www.sec.gov/about/laws/soa2002.pdf Protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws.
Fair Credit Reporting Act (FCRA)	**Fair Credit Reporting Act (FCRA), U.S. Code, Title 15 § 1681 et seq.** For the complete text as amended September 2012, visit: http://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0111-fair-credit-reporting-act.pdf This is the federal law that protects consumer credit and credit reporting.
Fair and Accurate Credit Transactions Act of 2003 (FACTA)	**Fair and Accurate Credit Transactions Act of 2003 (FACTA), the Red Flag Rules** http://www.gpo.gov/fdsys/pkg/PLAW-108publ159/pdf/PLAW-108publ159.pdf This is a federal law that requires financial institutions and creditors to develop and implement written identity theft prevention programs.
Americans with Disabilities Act	**Americans with Disabilities Act of 1990** http://www.ada.gov/pubs/ada.htm The current text of the Americans with Disabilities Act of 1990 [ADA], including changes made by the ADA Amendments Act of 2008 (P.L. 110-325), which became effective on January 1, 2009

State	Title
Information Practices Act of 1977	**Information Practices Act of 1977** http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798-1798.1 This Act established California Civil Code, (sections 1798 et seq.), which requires government agencies to protect the privacy of personal information maintained by state agencies.

State	Title
California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.85	**California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.85** http://www.leginfo.ca.gov/.html/civ_table_of_contents.html This is a state law that, as amended by SB 1386 (2003), SB 1298 (2007) and SB 24 (2011), provides information on safeguarding personal information, requires notification to California residents whose personal information was or is reasonably believed to have been acquired by unauthorized individuals and requires notification to the Attorney General if more than 500 residents are involved.
Government Code Sections 14740-14769	**State Records Management Act** http://www.leginfo.ca.gov/.html/gov_table_of_contents.html This is a state law that provides information on the administration of state records.

7 Related Documents

The following documents, forms and logs of the latest issue in effect shall apply to the extent specified herein.

Campus	Title
ITS-2524	**Cal State L.A. Information Security Program** http://www.calstatela.edu/sites/default/files/groups/Information%20Technology%20Services/security/campus_information_security_plan_2012.pdf This document establishes the University's Information Security Program in support of its obligation to protect the technology resources and information assets entrusted to it.
ITS-1013-G	**User Guidelines for Data Center/Communication Room Access** http://www.calstatela.edu/sites/default/files/groups/Information%20Technology%20Services/security/its-1013-g_userguidelinesfordatacenteraccess.pdf These guidelines outline the requirements for obtaining authorized access to data centers and communication rooms.
ITS-2018-P	**Electronic Security Incident Reporting Procedure** http://www.calstatela.edu/sites/default/files/groups/Information%20Technology%20Services/security/its_2018_electronic_security_incident_reporting_-_final.pdf This procedure provides information to guide users in reporting electronic security incidents.
ITS-2808	**Information Confidentiality/Non-Disclosure Agreement** http://www.calstatela.edu/its/services.php (Third-party Service Providers or Information Security and Compliance) This form is for vendors, consultants and agency employees who work in areas, on systems or in proximity to Levels 1 and 2 confidential data.

ITS-2827	**Information Security Contract Language for Third-party Service Providers with Direct Data Access** http://www.calstatela.edu/its/services.php (Procurement) This form is required for inclusion in all procurements involving service providers who will have direct access to the University's protected data.
ITS-2828	**Information Security Contract Language for Third-party Service Providers with Indirect Data Access** http://www.calstatela.edu/its/services.php (Procurement) This form is required for inclusion in all procurements involving service providers who may indirectly access the University's protected data during the execution of routine activities.
Chancellor's Office	**Title**
CSU Information Security Policy	**The California State University Information Security Policy** http://www.calstate.edu/icsuam/sections/8000/8000.0.shtml This document provides policies and standards governing CSU information assets.
CSU Third Party Security Standard 8040.S001	**Third Party Security** http://www.calstate.edu/icsuam/documents/Section8000.pdf#page=21 This document provides the minimum requirements for third-party contract language when the procurement of goods or services involves CSU and campus information assets.
CSU Executive Order 1031	**System-wide Records/Information Retention and Disposition Schedules Implementation** http://www.calstate.edu/EO/EO-1031.html This Executive Order provides for the implementation of the California State University (CSU) System wide Records/Information Retention Schedules.
Miscellaneous	**Title**
PCI DSS	**Payment Card Industry Data Security Standards** https://www.pcisecuritystandards.org/pdfs/pci_audit_procedures_v1-1.pdf These procedures are designed to conduct reviews to validate compliance with Payment Card Industry (PCI) Data Security Standard (DSS) requirements.

8 Appendices

8.1 Information Security Contract Language Templates

ITS has designed two forms with approved information security contract language that meets the requirements of this user guideline. These electronic forms are available for insertion in contracts, scopes of work, service orders or any other procurement documents that define tasks and responsibilities related to the access and use of protected data.

8.1.1 ITS-2827 Information Security Contract Language for Third-party Service Providers with Direct Data Access

This form must be included in all contracts and service orders that provide the third-party service provider with access to or use of any Cal State L.A. protected data. Sections should not be excluded even if the section does not appear to fit the immediate contract work requirements. For example, the third-party service provider may not have a contractual requirement to transmit protected data, however, future circumstances or technological changes may require the vendor to access the system remotely and download information or require the campus to provide information electronically. Leaving the contract language intact prevents consequences from unforeseen conditions.

This form is available for downloading at: http://www.calstatela.edu/its/services.php (Procurement)

8.1.2 ITS-2828 Information Security Contract Language for Third-party Service Providers with Indirect Data Access

This form must be included in all contracts and services orders not covered by Section 7.1.1. All third-party service providers may come in contact with Cal State L.A. protected data as they perform their contracted services. This template outlines the general information security requirements of **all** third-party service providers working on the campus.

This form is available for downloading at: http://www.calstatela.edu/its/services.php (Procurement)