Securing Workstation Documents				
	Standard No	ITS-2021-S	Rev	--
	Owner	Security and Compliance		
	Approved by	Sheryl Okuno, Director Security and Compliance		
	Issued	2/15/17 – Interim as ITS-1034-G	Revised	6-22-17
				Page 1 of 6

Table of Contents

1. Purpose 2
2. Related California State University Policies and Standards 2
3. Entities Affected by These Standards 2
4. Definitions 3
5. Standards 4
   5.1 Responsibilities 4
      5.1.1 IT Security and Compliance 4
      5.1.2 Employees 4
      5.1.3 Vice Presidents 4
   5.2 Reporting 4
6. Contacts 5
7. Applicable Federal and State Laws and Regulations 5

Securing Workstation Documents	Standard No ITS-2021-S	Rev --
	Owner Security and Compliance	
	Approved by Sheryl Okuno, Director Security and Compliance	
	Issued 2/15/17 – Interim as ITS-1034-G	Revised 6-22-17
		Page 2 of 6

1. Purpose

Cal State LA must protect all information assets it owns based on the data classification and the risk to the University of exposure from inappropriate or undesired access, disclosure or destruction. The degree of protection that must be provided to Levels 1 and 2 Confidential Data correlates directly with the risk of exposure, regardless of the media on which the data resides. The degree of protection afforded confidential data must be consistent from creation to destruction, including handling and transmitting.

Before any actions can occur to secure confidential data on computers, the information must first be identified. Cal State LA provides a tool on all Baseline computers and non-Baseline computers managed by ITS to identify possible confidential data. This information security tool scans computers searching for protected data within electronic files. The University recognizes the need for a tool to assist users in quickly and automatically identifying files with Levels 1 and 2 Confidential Data and providing a convenient means for all employees to secure or remove unnecessary data.

2. Related California State University Policies and Standards

The following documents of the latest issue in effect represent the criteria against which University information security audits shall be based and shall apply to the extent specified herein. Standards provide detailed supporting and compliance information for policies.

ID/Control #	Description	Title
8020.0	**Policy**	**Information Security Risk Management**
8020.S000	*Standard*	*Information Security Risk Management – Exception Standard*
8020.S001	*Standard*	*Information Security Risk Management – Risk Assessment Standard*
8065.0	**Policy**	**Information Asset Management**
8065.S001	*Standard*	*Information Security Asset Management*

In support of the CSU policies and standards, the University publishes **standards** (define the minimum requirements necessary to meet CSU policy) and **user guidelines** (provide general recommendations and instructions for users to comply with the policy). These supporting documents are available on the IT Security website under the policy title noted above.

3. Entities Affected by These Standards

This standard pertains to all University employees.

4. 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 violation has occurred.

b. Level 1 Confidential Data: Confidential data 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 data 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 data 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.

c. Level 2 Internal Use Data: Internal use data 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.

d. 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

e. 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.

f. User: Users are one or more of the following:
   - Anyone or any system that accesses Cal State LA information assets.
   - Individuals who need and use University data as part of their assigned duties or in fulfillment of assigned roles or functions within the University community.
   - Individuals who are given access to sensitive data, have a position of special trust and as such are responsible for protecting the security and integrity of those data.

5. Standards

5.1 Responsibilities

5.1.1 IT Security and Compliance

IT Security and Compliance is responsible for:

- Evaluating and implementing an information security scanning tool capable of identifying and managing confidential information on workstations.
- Performing an automated monthly scan of all University Baseline-issued computers.
- Preparing a quarterly status report of employee actions taken and distributing the report to all divisional vice presidents.

5.1.2 Employees

All employees are responsible for:

- Reviewing the results of the monthly scan.
- Performing the appropriate action to remediate findings as soon as reasonably possible using the online instructions at IT Security and Guidelines.

5.1.3 Vice Presidents

Vice presidents are responsible for:

- Reviewing the quarterly reports and designating authorized individuals to complete remediation actions.
- Signing the Chancellor's Office annual Risk Assessment Report attesting that quarterly reviews were conducted and accepting risk associated with any incomplete remediations.

5.2 Reporting

Under CSU Information Security Policy, the University is required to ensure the integrity and security of all information assets, and evidence of this action may be requested during routine information security audits by the Board of Trustees auditors. To meet this requirement, IT Security and Compliance will:

- On a quarterly basis, create a report of all user computers that have not secured confidential data and distribute the report to each divisional vice president for review and action.
- At the end of each academic year, request that all vice presidents submit a certification that they have reviewed all quarterly reports. In the event some documents and files have not been secured, the vice president must sign his or her acceptance of the risk associated with any non-secured data within their divisions.

6. Contacts

a. For questions regarding this standard, contact the director for IT Security and Compliance at (323) 343-2600 or itsecurity@calstatela.edu.

b. For assistance with the information security scanning tool or managing results, contact the division ITC or the ITS Help Desk at (323) 343-6170.

7. 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.
Federal Privacy Act of 1974	**Federal Privacy Act of 1974** http://www.usdoj.gov/opcl/privacyact1974.htm This is a federal act that establishes a code of fair information practices governing the collection, maintenance, use and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies.
Gramm-Leach-Bliley Act 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 non-public 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.
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.

Securing Workstation Documents				
	Standard No	ITS-2021-S	Rev	--
	Owner	Security and Compliance		
	Approved by	Sheryl Okuno, Director Security and Compliance		
	Issued	2/15/17 – Interim as ITS-1034-G	Revised	6-22-17
				Page 6 of 6

State	Title
California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.85	**California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.8** http://www.leginfo.ca.gov/.html/civ_table_of_contents.html This is a state law that, as amended by SB 1386 (2003), AB 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.