User Guidelines for Encryption Security	Guideline No.	ITS-1027-G	Rev:	B
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director IT Security and Compliance		
	Issued:	8-4-11	Updated:	12-11-14
				Page 1 of 11

Table of Contents

1 Purpose 2
2 Entities Affected by These Guidelines 2
3 Definitions 2
4 Guidelines 4
4.1 General 4
4.2 Approved Encryption Algorithms 4
4.3 Managing Encryption Keys 5
5 Recommended Products 5
6 Encryption Tools and Practices 7
6.2 Remote Access 7
6.3 Digital Certificates for Web-based Applications 7
6.4 Laptops 7
6.5 Individual Files 8
6.6 Microsoft Office 2010 8
6.7 Microsoft Documents, Workbooks and Presentations 8
7 Contracts with Third-Party Service Providers 8
8 Contacts 8
9 Applicable Federal and State Laws and Regulations 9
10 Related Documents 10

1 Purpose

University protected data is a valuable asset but one that must be protected from acquisition by unauthorized individuals. Federal and state laws can subject organizations to fines and penalties for failure to protect its constituents' confidential data.

Protected data can be "captured" as it traverses unsecured wireless and wired networks. Email attachments can be misdirected or re-sent by the original recipient to unauthorized recipients. In some instances, data can be compromised when computers, laptops or electronic storage media are lost or stolen. The most effective way to prevent protected data from being compromised is to always encrypt protected data – both at rest and in transit.

These guidelines provide information on approved encryption algorithms, recommended encryption products and specific encryption tools and practices that can be used by the University community.

2 Entities Affected by These Guidelines

The general aspects of these guidelines apply to all faculty, staff, Auxiliary Services, University-Student Union (U-SU), Associated Students, Inc. (ASI), third-party service providers and any others entrusted with University protected data.

The technical aspects of these guidelines apply to all ITS Baseline Services personnel and campus Information Technology Consultants (ITCs) who are responsible for the encryption product evaluation, procurement, installation, user training and assistance and encryption key management.

3 Definitions

a. Asymmetric Key Method: This method uses a pair of keys, one private and one public. The keys are related mathematically, but the private key cannot be practically derived from the public key. A message encrypted with the public key can be decrypted only with the corresponding private key. Public key methods assume that the communications medium between sender and recipient is not secure (e.g., the Internet).

b. Ciphertext: In cryptography, ciphertext is the result of the process (known as encryption) of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. This result is also known as encrypted information. The process to read ciphertext is known as decryption.

c. Data Encryption: Process of disguising information as 'ciphertext,' or data that will be unintelligible to an unauthorized person.

d. Digital Signature: A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender and that it was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery and tampering.

e. Encryption: A procedure used to convert data from its original form to a format that is unreadable and/or unusable to anyone without the tools/information needed to reverse the encryption process.

f. Encryption Keys: Used to decrypt encrypted data and communication.

g. Hash Functions: Hash function is a function associated with a table that computes hash code. Hash functions are mostly used to speed up table lookup or data comparison tasks — such as finding items in a database, detecting duplicated or similar records in a large file, finding similar stretches in DNA sequences and so on.

h. 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. Confidential data is information whose unauthorized use, access, disclosure, acquisition, modification, loss or deletion could result in severe damage to the CSU, its students, employees, alumni, donors 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.

i. Level 2 Internal Use Data: Internal use information is data 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. 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.

k. Secure Socket Layer (SSL): A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a private key to encrypt data that's transferred over the SSL connection. Both Netscape Navigator and Internet Explorer support SSL and many websites use the protocol to obtain sensitive information, such as credit card numbers. By convention URLs that require a SSL connection start with "https" instead of "http."

l. Symmetric Key Method: This method uses a single key for encryption and decryption, which is shared between sender and recipient. Secret key methods assume that the communications medium between sender and recipient is secure and that the secret key is not subject to compromise in transit. Most stand-alone encryption products use this method.

m. Wi-Fi Protected Access 2 (WPA2): Security protocol for wireless local area networks that indicates a product has successfully completed testing under the Wi-Fi Alliance's Wi-Fi Protected Access 2 certification program and meets the criteria established to ensure stronger data protection for multiple users and large managed networks. These criteria prevent unauthorized network access by verifying network users through an authentication server.

4 Guidelines

4.1 General

Not all encryption algorithms provide the same level of protection. This is a function of the algorithm used and the length of the encryption key. The use of weaker encryption or the practice of encrypting only short fields (which is inherently weak) may allow ciphertext data to be cracked in hours or even minutes using a fast computer. Only encryption algorithms that are well-tested may be used and Information Technology Consultants (ITCs) should be consulted prior to installation of any encryption tool in departments.

4.2 Approved Encryption Algorithms

There are three basic classes of cryptographic algorithms: symmetric key algorithms, asymmetric key algorithms and hash algorithms. The classes are defined by the number of cryptographic keys that are used in conjunction with the algorithm.

The following cryptographic algorithms are currently approved for use by Federal Information Processing Standards (FIPS) and, therefore, are to be used with University protected data:

Algorithm	Type	Federal Information Processing (FIPS) Standard
Advanced Encryption Standard (AES)	Symmetric	FIPS 197
Digital Signature Algorithm (DSA)	Asymmetric	FIPS 186-3
RSA (Algorithm developed by Rivest, Shamir and Adelman)	Asymmetric	FIPS 186-3

Algorithm	Type	Federal Information Processing (FIPS) Standard
Elliptic Curve Digital Signature Algorithm (ECDSA)	Asymmetric	FIPS 186-3
Secure Hash Standard • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512	Hashing	FIPS 180-3
Keyed-Hash Message Authentication Code (HMAC)	Hashing	FIPS 198-1

The use of encryption algorithms that do not meet the Federal Information Processing Standards must be reviewed on a case-by-case basis and approved in writing by the director of IT Security and Compliance.

4.3 Managing Encryption Keys

Encryption keys are critically important since without them, it would be impossible to decrypt encrypted data. If each user retained his or her encryption keys, keys could easily be misplaced or lost. In the event disaster recovery or business continuity measures must occur, encryption keys would be scattered throughout the division. Therefore, central management of encryption keys within the department or division is highly recommended. It is further recommended that the vice president or other high-level MPP designee retain the encryption keys in the event immediate access is required to protected data on the computer or electronic storage device of an individual who is unavailable or no longer employed by the University.

Departments may delegate responsibility for encryption key management to ITS if technical management is not feasible for the department. Requests for ITS encryption key management should be directed to IT Security and Compliance: itsecurity@calstatela.edu. Requests must be approved by the department chair, manager or divisional vice president.

5 Recommended Products

At the time of this document preparation, the following products meet the required standard and may be used for protecting University protected data. However, the products may need to be configured to use “strong encryption” and meet the standards above.

The products listed below are not all inclusive and departments may utilize other products as long as they document that the product used meets Federal Information Processing Standards.

Whole Disk Encryption	Algorithm To Be Used	Platforms
Bitlocker	AES	Microsoft Windows 7 and 8.1
FileVault	AES	Mac OS X
Pointsec for Linux	AES	Linux
Linux Unified Key Setup (LUKS)	SHA-1 in HMAC mode	Linux
Data at Rest	**Algorithm To Be Used**	**Platforms**
AXCrypt	AES	Microsoft Windows
GPG	AES	Microsoft Windows, Mac OS X, Linux
TrueCrypt	AES	Microsoft Windows, Mac OS X, Linux
Loopback Encrypted File System	AES	Linux
Data in Transit	**Algorithm To Be Used**	**Platforms**
SSH (Version 2)	AES	All
SSL/TLS	AES/ECDSA	All
IPSEC or SSL VPN	SHA-1; HMAC; AES	All
Access	**Algorithm To Be Used**	**Platforms**
Wi-Fi Protected Access 2 (WPA2)	AES	Windows, MAC OS X, Linux
File Encryption	**Algorithm To Be Used**	**Platforms**
WinRAR	AES	Windows, MAC OS X, Linux
WinZip	AES	Windows

This information is also available at: http://www.calstatela.edu/its/services/software/encryptiontools.php. The online list is continually updated as products and recommendations change.

6 Encryption Tools and Practices

6.1 Common Management Systems (CMS)

The Common Management System (CMS) consists of three distinct parts: (1) the Common Financial System (CFS), where the "books" of the University are maintained, and the Human Capital Management System (HCM) comprised of (2) the Human Resources System, which contains job, salary and benefits information for all employees of the University, and (3) the Student Administration System where all academic records of the University are maintained for catalog, curriculum, class schedules and student academic progress. CMS has in place enhanced network and administrative system security measures including encryption of data at rest and in transit.

6.2 Remote Access

The University approved method of remote access is based on Virtual Private Network (VPN) technology, which forces all traffic through an encrypted tunnel. Therefore, all remote access traffic passed between the University network and the end users is fully encrypted. Outlook Web Access (OWA) is also encrypted with SSL. Where SSL is used, like OWA, VPN is not required.

6.3 Digital Certificates for Web-based Applications

A digital certificate for web-based applications must meet the X.509 standard. The certificates installed on servers should be acquired from Certificate Authorities (CA) that have a WebTrust seal. WebTrust is a recognized Certificate Authority standards organization and their seal indicates that a Certificate Authority has undergone an audit by a WebTrust accredited auditor. Since these certificates expire after a specified period of time, a department must have in place a process to renew expiring certificates.

6.4 Laptops

Some laptops are delivered with a built-in encryption functionality that renders all the data on the hard disk unusable if the disk is removed from the computer. If this technology is unavailable and protected data is stored on the laptop, software to encrypt the protected data on the laptop must be installed.

An alternate recommendation for laptops that store protected data is that they have special laptop “tracking and recovery” software installed. This special software will track the location of a stolen laptop and can remotely delete all data on the stolen laptop’s hard drive as soon as the stolen device is connected to the Internet. One popular tracking and recovery software application is Computrace, available at http://www.computrace.com.

> **Note:** These recommendations require an action that may not take place immediately (i.e., removing the hard disk, connecting to the Internet). The best information security practice is to always encrypt the protected data on laptops.

6.5 Individual Files

WinZip software allows the encryption of individual files and offers strong AES encryption for securing protected data. WinZip does not automatically encrypt files. The WinZip file encryption process must be followed to encrypt a file. Instructions for WinZip file encryption are available at: http://www.calstatela.edu/encrypt.

6.6 Microsoft Office 2010

Microsoft Office 2010 has further simplified the process to password protect and encrypt documents.

- Click on the **File ► Info**. On the menu to the right, click **Protect Document ► Encrypt with Password**.
- The Encrypt Document dialog box will appear. Type in a **password ► OK** to finish.

6.7 Microsoft Documents, Workbooks and Presentations

Microsoft Office allows users to conveniently add passwords to Office documents, Excel workbooks and PowerPoint presentations to prevent others from opening or modifying the work. Passwords should meet campus password standards to ensure proper protection. Document encryption is recommended for all documents that will be stored in the OneDrive cloud and is required for all documents containing Levels 1 and 2 confidential data.

It's important to remember your password as Microsoft cannot retrieve forgotten passwords.

Instructions for protecting your work are available at: https://support.office.com/en-us/article/Protect-your-document-workbook-or-presentation-with-passwords-permission-and-other-restrictions-05084cc3-300d-4c1a-8416-38d3e37d6826

7 Contracts with Third-Party Service Providers

Commercial applications, including outsourced services, must protect the University data as required by law and abide by any relevant industry standards. Contracts with vendors, consultants and other third-parties must include language about protection of the University protected data and should specify where encryption will be used.
Refer to *ITS-1022-G User Guidelines for Information Security Contract Language* for specific vendor requirements and sample contract language for Third-party Service Providers with direct and indirect access to University protected data. User Guidelines are available at: http://www.calstatela.edu/its/policies. Information Security Contract Language templates can be downloaded at http://www.calstatela.edu/its/forms and attached to procurement documents.

8 Contacts

a. For questions regarding specific department procedures and assistance encrypting files, contact the department Information Technology Consultant (ITC).

b. Find an up-to-date list of recommended encryption tools at: http://www.calstatela.edu/its/services/software/encryptiontools.php.

c. Find up-to-date instructions for WinZip encryption and Microsoft Office file encryption at: http://www.calstatela.edu/encrypt.

d. Address questions regarding these guidelines to: ITSecurity@calstatela.edu.

9 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/guidd/fpco/ferpa/index.html This is a federal law that protects the privacy of student education records.
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 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.

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 resident are involved.

10 Related Documents

CSULA	Title
ITS-2524	**Cal State L.A. Information Security Program** http://www.calstatela.edu/its/itsecurity/guidelines/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.
Administrative Policy P008	**Policy for Technology and Information Security Compliance** http://www.calstatela.edu/univ/admfin/policies/008/008.pdf This University policy establishes the guidelines for implementation, access, use, disposal and legal compliance of technology resources and information assets.
ITS-1005-G	**User Guidelines for Portable Electronic Storage Media** http://www.calstatela.edu/its/policies/ These guidelines are intended to help students, faculty, and staff meet the University's accepted standards for protecting confidential information that is copied, downloaded, or stored on portable electronic storage media.
ITS-1006-G	**User Guidelines for Securing Offices, Workspaces, and Documents** http://www.calstatela.edu/its/policies/ These guidelines are intended to help the campus community protect offices, machines, devices, and documents from unauthorized access to confidential, personal, and proprietary information.
ITS-1007-G	**User Guidelines for Laptop Security** http://www.calstatela.edu/its/policies/ These guidelines outline the steps for securing laptops and the personal, confidential, and/or proprietary information contained on them.
ITS-1015-G	**User Guidelines for Wireless Access** http://www.calstatela.edu/its/policies These guidelines are to help users meet the University's accepted standards for wireless access.
ITS-1020-G	**User Guidelines for Mobile Computing** http://www.calstatela.edu/its/policies/ These guidelines establish an authorized method for controlling mobile computing devices that contain or access CSULA protected data.

CSULA	Title
ITS-1022-G	**User Guidelines for Information Security Contract Language** http://www.calstatela.edu/its/policies These guidelines define the information security responsibilities and procedures that apply to all Third-party Service Providers.

Chancellor's Office	Title
CSU Information Security Policy	**The California State University Information Security Policy** http://www.calstate.edu/icsuam/documents/Section8000.pdf This document provides policies governing CSU information assets.