Encryption Policy

Policy Contents

I. POLICY STATEMENT
II. REASON FOR POLICY
III. SCOPE
IV. AUDIENCE
V. POLICY TEXT
VI. PROCEDURES
VII. RELATED INFORMATION
VIII. DEFINITIONS
IX. FREQUENTLY ASKED QUESTIONS
X. REVISION HISTORY
XI. COMPLIANCE
XII. POLICY EXCEPTION PROCESS
XIII. APPENDICIES

Effective Date: 03-01-2015
Last Updated: 03-04-2015

Responsible University Officer:
Vice President, Chief Information Officer

Policy Owner:
Associate Director, Client Support Services

Policy Contact:
ITS Help Desk
I. POLICY STATEMENT
A. Schools, departments and business functions are required to apply University-approved encryption solutions to preserve the confidentiality and integrity of, and control accessibility to, University of San Francisco (USF) data classified as “Confidential” or “Highly Confidential” where this data is processed, stored or transmitted.

II. REASON FOR POLICY
A. The purpose of this policy is to establish:
   1. the types of data, devices and media that need to be encrypted
   2. when encryption must be used
   3. and the minimum standards of the software and techniques used for encryption.

III. SCOPE
A. This policy applies to all university data classified as USF “Confidential” or “Highly Confidential” where this data is processed, stored or transmitted.

IV. AUDIENCE
A. All Employees, Faculty and Staff.
B. Student workers including interns whose job function falls within scope of this policy by virtue of the types of data access which they are granted, either explicitly or implicitly (such as access to network shares or documents containing data covered by the scope of this policy.
C. All contractors, vendors and any other 3rd parties entrusted with University Sensitive, Confidential or Highly Confidential Data.

V. POLICY TEXT
A. Policy Requirements:
   1. Devices and Media Requiring Encryption:
      a. All ITS managed databases that contain USF “Confidential or Highly Confidential” must encrypt the data at rest, with the exception of those Enterprise resources housed in approved restricted-access facilities such as ITS Data Centers. All databases, application servers and file systems that contain USF “Confidential or Highly Confidential” data must leverage appropriate access control, per the Access Control Policy, to
ensure that access to the data is limited to those whose job functions require access.

2. Electronic Data Transfers:
   a. Any transfer of unencrypted USF “Confidential or Highly Confidential” data must take place via an encrypted method. Encrypted USF “Confidential or Highly Confidential” data may be transmitted via encrypted or unencrypted methods.
   b. All email communications outside of USF Google Secure Messaging must use an encryption technique, and therefore requires that messages containing USF “Confidential or Highly Confidential” data must be encrypted.
   c. Approved methods of encrypting electronic data transfers are listed in the “Standards” Section below.
   d. If encryption method used for electronic data transfer includes a password to access the data, that password must be transferred through an alternative method - i.e. such as calling the individual recipient to provide the passphrase or password. Email messages containing encrypted data may never include the password via email. Individuals who are unsure if they are correctly encrypting electronic data transfers should contact the ITS Help Desk.

3. Physical Transfer of Electronic Data:
   a. The physical transfer of USF “Confidential” or “Highly Confidential”, is not allowed. If there is a business need to perform a physical transfer of USF “Confidential” or “Highly Confidential”, a request for an exception to the policy must be granted. See “Policy Exception Process” below - If approved, physical transfers of USF “Confidential” or “Highly Confidential” data must be encrypted.
   b. Archiving USF “Confidential or Highly Confidential” data to a physical medium is not recommended, but is permitted if the data is encrypted. All archiving should be done electronically, so that it is stored in a controlled data center and backed up by ITS.
4. Software:
   a. ITS will install software that is capable of encrypting the entire hard drive on all ITS supported USF computers and electronic devices subject to this Policy in alignment with the ITS service offerings.
   b. Users who require encryption software should contact ITS to arrange installation of encryption software.

B. Standards
1. The value of the data that requires protection and the system storing the data need to be considered carefully. Physical security refers to being able to control access to the system’s storage media. All encryption methods detailed in the standards below are applicable to desktop and mobile systems.
2. A defense in depth approach is recommended when evaluating and deploying encryption products. This typically involves a combination of full disk encryption and file/folder encryption - i.e. full disk encryption combined with file/folder encryption in order to provide two “layers” of encryption to protect data in the event the first layer is compromised.
3. USF Security Services leverages the recommendations of the NIST for contemporary encryption algorithm standards.
4. USF Security Services recommends the use of integrated encryption solutions in combination with recommended third-party products detailed in the following standards. Encryption methods which do not utilize ITS-provided solutions for centralized management must provide the encryption key or password to the Security Services Team of ITS for proper storage and escrow to allow compliance with investigatory or other approved or legal orders for access to encrypted data.
   a. Full Disk Encryption
      i. Scenario: Full disk encryption encrypts all data on a system, including files, folders and the operating system. This is most appropriate when the physical security of the system is not assured. Examples include traveling laptops or desktops that are not in a physically secured area.
      ii. Recommended Product(s): Sophos Encryption, Mac OS X FileVault
   b. Email Encryption
      i. Scenario: Email-specific products integrate encryption into the email client, allowing messages and attachments to be sent in an encrypted form transparent to the user. This is most appropriate for departments whose users require frequent and regular
encryption of email communications. Most departments can make use of a broader range of file/folder encryption products to encrypt individual files and folders.

ii. Recommended Product(s): Google Vault, Sophos Encryption

c. External Devices Encryption

i. Scenario: External devices such as hard drive and USB flash drives, can be encrypted in their entirety (similar to full disk encryption). Data on these systems can be considered secure without access to the key and encryption software.

ii. Recommended Product(s): Sophos Encryption

d. File//Folder Encryption

i. Scenario: Individual or multiple files can be encrypted separately from the host operating system. These encrypted archives can be stored in different locations such as network shares, external hard drives, DVDs, CDs, USB flash drives or be transmitted securely via email.

ii. Recommended Product(s): Sophos Encryption

e. Mobile Device Encryption

i. Scenario: Mobile devices such as PDAs, tablets and smartphones allow users to exchange, transfer and store information both within and beyond the USF network or properties. The extreme portability of these devices renders them susceptible to theft or loss. USF Security Services recommends the use of standardized devices such as laptops for storing, transmitting or processing Sensitive Data.

ii. Product(s): Android Encryption, iPhone Encryption, Sophos Encryption

f. Transport-Level Encryption

i. Scenario: Secure transport client/server products provide transport-level encryption to protect data in transit between the sender and recipient in order to ensure delivery without eavesdropping, interception or forgery. This scenario requires the appropriate configuration of a server in order to allow clients to connect in a secure manner.

ii. Product(s): FileZilla, PSFTP, SCP, WinSCP
VI. PROCEDURES
A. (None)

VII. RELATED INFORMATION
A. Technology Resources Appropriate Use Policy,
   http://myusf.usfca.edu/system/files/technology_resources_appropriate_use_policy.pdf
B. USF Information Security Policy,
C. NIST Standard, National Institute of Standards and Technology (NIST) - SP800-111- Guide to Storage Encryption Technologies for End User Devices,

VIII. DEFINITIONS
A. (None)

IX. FREQUENTLY ASKED QUESTIONS
A. (None)

X. REVISION HISTORY
A. 06-01-2013 – Final draft of policy
B. 11-12-2013 – Approved for publication
C. 03-01-2015 – Minor edits

XI. COMPLIANCE
A. Failure to follow this policy can result in disciplinary action in accordance with Human Resources Employment Handbook and Office of General Counsel employee and labor relations. Disciplinary action for not following this policy may include termination, as provided in the applicable handbook or employment guide.

XII. POLICY EXCEPTION PROCESS
A. A proposed exception request to ITS Policy requires a formal e-mail explanation related and in support of job function.
B. A proposed exception request to ITS Policy, mentioned in 'XII.A', must be approved via email by respective department or division supervisor, Dean, or VP, before submitted to ITS for review.
C. Forward approved email as stated in 'XII.B' to itshelp@usfca.edu for processing.
D. Evaluation of ITS Policy Exception will escalate internally, and as applicable may include further review by: UITC subcommittee(s), the Information Security Officer, and others as appropriate at the request of VP for IT.

XIII. APPENDICIES
A. (None)