DOCUMENT INFORMATION

VCSATS Policy Number:	**VCSATSP 100-040**
Title:	**Restricted Data Encryption Policy**
Policy Owner:	**Infrastructure Manager**
Effective Date:	**4/22/2013**
Revision:	**4.0**

TABLE OF CONTENTS

1. PURPOSE

This policy defines the rules for encryption of Restricted Data within the VCSA division.

2. SCOPE

This policy applies to all systems within Vice Chancellor Student Affairs Technology Services that deal with Restricted data.

3. RESPONSIBILITIES

TABLE 1 - ROLES AND RESPONSIBILITIES

Role	Responsibility
Infrastructure Manager	• Oversee the performance of this process • Ensure this document remains current and is updated whenever changes to the process occur • Review and approve changes to this document
Director Technology Services	• Review and approve changes to this document
Data Custodian	• Ensure appropriate encryption strategies are in place for both transmission and storage of protected data.

4. REFERENCES

TABLE 2 - REFERENCES

Reference	Location
Risk Assessment Methodology Overview	UCOP (http://www.ucop.edu/information-technology-services/initiatives/resources-and-tools/risk-assessment-methodology-overview-.html)
VCSATSP 100-010 Policy Guidance	VCSATS Policy Center

5. DEFINITIONS

The terms and definitions found in VCSATSP 100-010 Policy Guidance, as referenced in section 4 references, shall apply, unless a term is expressly defined here. The scope of every term expressly defined in this section is limited to this document.

TABLE 3 - LOCAL DEFINITIONS

Term, Abbreviation, Acronym	Definition
Encryption	The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

6. POLICY

6.1 General Instructions

Select appropriate encryption methods for data and systems based on the output of the Risk Assessment dictated in the Risk Assessment Methodology Overview.

Logical access to encrypted file systems shall be managed independently of native operating system access control mechanisms (for example, by not using local user account databases).

6.2 Data at Rest

The use of encryption, for the purpose of access control of data at rest, shall be based upon a risk analysis as mentioned in section 6.1 General Instructions.

6.3 Data in Use

Encryption shall be applied to data in use in a manner commensurate with the associated risk or applicable industry requirement, such as HIPAA, PCI, HITECH, etc.

6.4 Data in Transit

6.4.1 Any Restricted data that is temporarily in electronic transition will be encrypted [45 CFR § 164.312.a.2.iv, PCI DSS 4.2 (a)]. This includes, but is not limited to transfer via end-user messaging technologies such as e-email, instant messaging, chat, etc. [PCI DSS 4.2 (a)].

6.4.1.1 The method and strength of encryption selected must be commensurate with the value of the data as identified in the Risk Assessment. The use of WEP is prohibited [PCI DSS 4.1.1].

6.4.1.2 Both the sending and receiving systems must be secured with access controls on both ends. For example, the receiver can only get data from sender, and the sender can only send data to receiver.

6.4.1.3 Vendor default keylengths must not be shortened.

6.4.1.4 Only trusted keys and/or certificates may be accepted [PCI DSS 4.1 (b)].

6.4.2 Restricted data in unencrypted form may not be transferred via end-user messaging technologies [PCI DSS 4.2 (b)].SSL/TLS implementations must show HTTPS as part of the browser Universal Record Locator (URL) [PCI DSS 4.1 (e)].

6.4.3 When requesting Restricted data, including but not limited to payment data, HTTPS must appear in the URL [PCI DSS 4.1 (e)].

6.5 Data in Transit Over Wireless

As physical access to wireless networks cannot be restricted, appropriate measures must be taken to offset this inherent risk.

6.5.1 6.4.16.4.1.1 The method and strength of encryption selected must be commensurate with the value of the data as identified in the Risk Assessment. The use of WEP is prohibited [PCI DSS 4.1.1PCI DSS 4.2 (a), PCI DSS 4.2 (b)].

6.6 Encryption Key Management

6.6.1 Cryptographic keys shall be stored securely (for example, stored on removable media that is adequately protected with strong access controls) [PCI DSS 3.4.1 (b)], [PCI DSS 3.6.3].

6.6.2 Cryptographic keys shall be stored in encrypted format [PCI DSS 3.5.2 (a)].

6.6.3 Key-encrypting keys shall be stored separately from data-encrypting keys [PCI DSS 3.5.2 (a)].

6.6.4 Access to the cryptographic keys shall be restricted to the fewest number of custodians necessary [PCI DSS 3.5.1].

6.6.5 Cryptographic keys shall be stored in the fewest possible locations and forms possible [PCI DSS 3.5.2 (b)].

6.6.6 Generated cryptographic keys must be strong per standards provided in the encryption software documentation [PCI DSS 3.6.1].

6.6.7 Cryptographic keys shall be changed when any of the following trigger conditions are met:

6.6.7.1 Key has reached the end of its defined cryptoperiod (for example, after one year has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57) [PCI DSS 3.6.4].

6.6.7.2 Key integrity has been weakened (for example, departure of an employee with knowledge of a clear-text key) [PCI DSS 3.6.5 (a)].

6.6.7.3 The key is suspected of having been compromised [PCI DSS 3.6.5 (b)].

6.6.7.4 Note: Retired or replaced cryptographic keys may only be retained, to be used for decryption/verification purposes (not used for encryption operations) [PCI DSS 3.6.5 (c)].

6.6.8 Split knowledge and dual control of cryptographic keys (for example, requiring two or three people, each knowing only their own key component, to reconstruct the whole key), shall be established for manual clear-text key-management operations [PCI DSS 3.6.6].

6.6.9 Any individual responsible for management or use of encryption keys must sign the Encryption Key Custodian Agreement.

7. ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action.

8. COMPLIANCE REFERENCE INDEX

9. HISTORY

FogBugz Case	Description of Changes
1514	Initial creation of this policy.
2601, 2602	Requested approvals for version 1.0 of this policy. (Not Approved)
2617, 2618	Requested approvals for version 2.0 of this policy.
4910, 7637	Updated document number and references within to match the approved naming convention. Added section 6.6 for PCI SAQ-D support. Changed “Sensitive” references to “Restricted.”
7639, 7640	Requested approvals for version 3.0 of this policy.
2540, 8363 6837	Added support for PCI DSS Requirement 4. Updated reference for Risk Assessment Methodology Overview to point to new location. Included link to make document easier to find.
8745, 8746	Requested approval for version 4.0 of this policy.