DOCUMENT INFORMATION

VCSATS Policy Number:	**VCSATSP 100-020**
Title:	**Removable Media Policy**
Policy Owner:	**Infrastructure Manager**
Effective Date:	**2/1/2014**
Revision:	**5.0**

TABLE OF CONTENTS

DOCUMENT INFORMATION 1
TABLE OF CONTENTS 1
1. PURPOSE 2
2. SCOPE 2
3. RESPONSIBILITIES 2
4. REFERENCES 2
5. DEFINITIONS 3
6. POLICY 3
7. ENFORCEMENT 4
8. COMPLIANCE REFERENCE INDEX 4
9. HISTORY 5

1. PURPOSE

- Minimize the risk of loss or exposure of restricted data maintained by the VCSA division based on how removable electronic media is used.
- Reduces the risk of acquiring malware infections on computers operated by the VCSA division by prohibiting the movement of removable media to and from non-VCSA computing devices.

2. SCOPE

This policy covers all computers and servers operating in the Vice Chancellor Student Affairs division.

3. RESPONSIBILITIES

TABLE 1 - ROLES AND RESPONSIBILITIES

Role	Responsibility
Infrastructure Manager	• Ensure this document remains current and is updated whenever changes to this policy occur • Review and approve changes to this document
Director Technology Services	• Review and approve changes to this document
Privacy Officer, FERPA	• Ensure the policy is communicated to organizations handling data subject to FERPA
Privacy Officer, HIPAA	• Ensure the policy is communicated to organizations handling data subject to HIPAA and HITECH

4. REFERENCES

TABLE 2 - REFERENCES

Reference	Location
VCSATSP 100-010 Policy Guidance	VCSATS Policy Center
VCSATSP 100-040 Restricted Data Encryption Policy	VCSATS Policy Center
VCSATSP 100-070 Restricted Data Protection Policy	VCSATS Policy Center

5. DEFINITIONS

The definitions found in Terms and Definitions, 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	A procedure used to convert data from its original form to a format that is unreadable and / or unusable to anyone without the tools and / or information needed to reverse the encryption process.
Malware	Software of malicious intent and / or impact such as viruses, worms, and spyware.
Removable Media	Device or media that is readable and / or writeable by the end user and is able to be moved from computer to computer without modification to the computer. This includes, but is not limited to, flash memory devices such as thumb drives, cameras, MP3 players and PDAs; removable hard drives (including hard drive-based MP3 players); optical disks such as CD and DVD disks; mobile devices such as smart phones and tablets; floppy disks and any commercial music and software disks not provided by VCSA.

6. POLICY

6.1 Explicit approval shall be obtained from DTS and/or Privacy Officer to use removable media with Restricted data and/or systems [PCI DSS 12.3.1].

6.2 Copy, move, and storage of Restricted data onto local hard drives and removable electronic media is prohibited unless explicitly authorized for a defined business need [PCI DSS 12.3.10 (a)] or when explicitly authorized to provide information required by other state or federal agencies.

6.3 When Restricted data is stored on removable media, it must be encrypted in accordance with VCSATSP 100-040 Restricted Data Encryption Policy [PCI DSS 3.4.1 (c)].

6.4 Media backups containing Restricted data must be stored in a secure location, preferably in an off-site facility, such as an alternate or backup site, or a commercial storage facility [PCI DSS 9.5 (a)].

6.5 Removable media containing Restricted data must be physically secured to prevent unauthorized viewing, copying, or scanning [PCI DSS 9.6].

6.6 Strict control shall be maintained over the internal or external distribution of removable media, including [PCI DSS 9.7 (a)]:

6.6.1 Removable media containing Restricted data shall be labeled in a manner as to make it easily discernible that Restricted data is contained on the media per VCSATSP 100-070 Restricted Data Protection Policy [PCI DSS 9.7.1].

6.6.2 Delivery of removable media containing Restricted data shall be performed in accordance with VCSATSP 100-070 Restricted Data Protection Policy [PCI DSS 9.7.2, PCI DSS 9.8].

6.6.3 For removable media containing Restricted data, a record shall be created to track all media that is moved from a secured area [PCI DSS 9.8].

6.6.3.1 The record shall be vaulted in a manner consistent with VCSATSP 100-010 Policy Guidance [PCI DSS 9.8].

6.6.3.2 Management approval must be recorded in the record prior to moving the media [PCI DSS 9.8].

6.7 Removable media containing Restricted data shall be stored in a manner as to prevent unauthorized access [PCI DSS 9.9].

6.8 Stored removable media containing Restricted data shall be logged [PCI DSS 9.9.1]. Inventories shall be conducted at least annually [PCI DSS 9.9.1].

6.8.1 When no longer needed for business or legal reasons, Restricted data stored on removable media shall be destroyed as follows [PCI DSS 9.10, PCI DSS 9.10.1, PCI DSS 9.10.2].

7. ENFORCEMENT

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

8. COMPLIANCE REFERENCE INDEX

PCI DSS 12.3.1 3
PCI DSS 12.3.10 (a) 3
PCI DSS 3.4.1 (c) 3
PCI DSS 9.10 4
PCI DSS 9.10.1 4
PCI DSS 9.10.2 4
PCI DSS 9.5 (a) 3
PCI DSS 9.6 3
PCI DSS 9.7 (a) 3
PCI DSS 9.7.1 3
PCI DSS 9.7.2 4
PCI DSS 9.8 4
PCI DSS 9.9 4
PCI DSS 9.9.1 4

9. HISTORY

FogBugz Case	Description of Changes
1499	Create initial version of this policy.
3201	Identified error with Effective Date before requesting approval for version 1.0 of this Policy. Forgoing approval request for version 1.0 and requesting approvals for version 2.0
3813, 3815	Approval requested for version 2.0 of this policy.
4910	Updated document number and references within to match the approved naming convention.
1540, 8503	Added support for PCI DSS Requirements 9.x and 12.x.
8748, 8749	Approval requested for version 3.0 of this policy.
10924	Added smart phones and tablets to Table-3 in Section 5 as examples of removable media to clarify that explicit approval must be obtained to use these with Restricted data and systems.
11693, 11694	Approval requested for version 4.0 of this policy.
15517	Section 6.6.2 was missing the word “media.” Corrected the omission.
15851, 15852	Approval requested for version 5.0 of this policy.