DOCUMENT INFORMATION

VCSATS Policy Number:	**VCSATSP 100-070**
Title:	**Restricted Data Protection Policy**
Policy Owner:	**Infrastructure Manager**
Effective Date:	**5/1/2013**
Revision:	**4.0**

TABLE OF CONTENTS

1. PURPOSE

This policy defines the rules for ensuring the protection of Restricted Data used and stored within Vice Chancellor Student Affairs (VCSA) systems.

2. SCOPE

This policy applies to all resources maintained or controlled by Vice Chancellor Student Affairs Technology Services (VCSATS) and all media within VCSA.

3. RESPONSIBILITIES

TABLE 1 - ROLES AND RESPONSIBILITIES

Role	Responsibility
Infrastructure Manager	• 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

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 100-100 Restricted Data Access Policy	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
External	In the context of this policy, External refers to any entity outside of the University of California. Including but not limited to Vendors and Consultants.

6. POLICY

6.1 Restricted Data Handling

A. Permanent deletion of PCI cardholder authentication data

1) For authentication or authorization data which is received, processes must be in place to securely delete the data and to verify that the data is unrecoverable.

B. Storage of PCI cardholder authentication data

1) All systems must adhere to the following requirements regarding storage of sensitive authentication data after authorization (even if encrypted):
   a) The full contents of any track from the magnetic stripe must not be stored under any circumstance.
      i. The magnetic stripe is located on the back of a card. This also applies to equivalent data contained on a chip, or elsewhere.
      ii. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.
      iii. If required for business purposes, the following data elements from the magnetic stripe may be retained and if retained, must be encrypted at rest:
         a) The cardholder's name
         b) Primary account number (PAN)
         c) Expiration date
         d) Service code

b) The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) may not be stored under any circumstance.
c) The personal identification number (PIN) or the encrypted PIN block may not be stored under any circumstance.

C. Masking

1) The PAN shall be masked so that only the first six and last four digits may be displayed.
   a) This includes but is not limited to electronic display such as within systems, so that masking is applied when data is displayed or retrieved.
   b) This includes but is not limited to physical media, so that the PAN is appropriately masked on any physical copy.
   c) This requirement does not apply to employees and other parties with a specific need to see the full PAN, though they may not share the full pan except as authorized by the Director Technology Services.
   d) This requirement does not relax requirements at the UCOP or UCR level.
2) The PAN shall be rendered unreadable anywhere it is stored (including but not limited to data repositories, portable digital media, backup media, and in audit logs) by one of the following approaches:
   - One-way hashes based on strong cryptography (hash must be of the entire PAN)
   - Truncation (hashing cannot be used to replace the truncated segment of PAN)
   - Index tokens and pads (pads must be securely stored)
   - Strong cryptography with associated key management processes and procedures.

   a) Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.

D. Permanent destruction of Restricted Information

1) For Restricted data that is stored, processes must be in place to securely delete the data and to verify that the data is unrecoverable when media or storage devices are disposed of or when the data is no longer needed.
2) All media containing Restricted data shall be destroyed when it is no longer needed for business or legal reasons in accordance with the definition of Media Destruction found in VCSATSP 100-010.
3) Devices and media containing restricted data shall have the data destroyed prior to any repair, maintenance, or disposal in accordance with the definition of Media Destruction found in VCSATSP 100-010. This includes but is not limited to hard drives or other storage in printers, spoolers, faxes, x-ray machines, lab equipment, EKG machines, phones, tablets, etc.

E. Remote-access of Restricted Data

1) Restricted data accessed via remote-access technologies shall not be copied, moved, or stored onto local hard drives and/or removable electronic media, unless explicitly authorized by the appropriate officer for a defined business need [PCI DSS 12.3.10 (a)].
2) Where the officer is not identified, Restricted data accessed via remote-access technologies shall not be copied, moved, or stored onto local hard drives and/or removable electronic media, unless explicitly authorized by the data owner for a defined business need [PCI DSS 12.3.10 (a)].

6.2 Distribution of Restricted Data

A. Use, Disclosure, and Request of Restricted Data

1) When using or disclosing Restricted data or when requesting Restricted data from another Covered Entity (as defined by HIPAA), reasonable efforts shall be made to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request [45 C.F.R. § 164.502(b)(1)].
2) Disclosure shall be performed in accordance with VCSATSP 100-100 Restricted Data Access Policy.

B. De-identification and Re-identification of Restricted Data

1) De-identification and/or re-identification of Restricted data shall be done with the approval, and under the direction of the appropriate officer [45 C.F.R. §164.514(b), 45 C.F.R. § 164.514(c)].
2) Where an officer is not identified, de-identification and/or re-identification of Restricted data shall be done with the approval, and under the direction of the data owner.

C. Classification of Information and Labeling

1) All internally or externally distributed Restricted Data must be classified according to VCSATSP 100-010 Policy Guidance.
2) All media or portable devices containing Restricted Data must be labeled to clearly indicate that Restricted Data is or may be on the device.

D. Internal and External Distribution of Restricted Information via Electronic Methods

1) VCSATSP 100-040 Restricted Data Encryption Policy shall be applied to Restricted Information internally or externally distributed in electronic format.

E. Internal Distribution of Restricted Data via Non-Electronic Methods

1) Distributing Restricted Data via hard copy is strongly discouraged and should be avoided in any case where it can be it can be delivered electronically.
2) Restricted Data that is internally distributed shall be clearly labeled as containing Restricted Data.
3) In the case of hard copy with multiple pages, every page must be labeled as containing Restricted Data, such as in the header or footer.
4) A ticket must be opened to note the nature of the Restricted Data, the sender of the Restricted Data, the intended recipient, the date of delivery, the method of delivery, and the reasonable steps taken to protect the data during transport.
5) The ticket is to be updated with the actual recipient, the date of receipt, and any other relevant information regarding the security of the Restricted Data, such as a suspected breach of privacy during delivery, failure to deliver, etc.

F. External Distribution of Restricted Data via Non-Electronic Methods

1) Restricted Data sent to external recipients by non-electronic methods shall be sent by secured courier or other delivery method that can be accurately tracked.

G. Exceptions

1) Health Care Providers, University officers or their designees, or UCOP officers or their designees are exempt from this policy when adherence would prevent execution of normal duties. For example, pharmacists may print labels to affix to medication and give that label to the intended patient without encrypting the data, opening a ticket, or noting "Restricted Information" on the label. This exception does not override federal or state law.

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
1517	Initial creation
2611, 2612	Requested approval for version 1.0 of this policy
4910	Updated document number and references within to match the approved naming convention.
1915	Changed document title from Cardholder Data Protection Policy to Restricted Data Protection Policy. Added sections for distribution of Restricted Data.
5319, 5320	Requested approval for version 2.0 of this policy
7647	Updated to support PCI SAQ-D, clarify Purpose and Scope, add clarification to 6.1.D
7649, 7650	Requested approval for version 3.0 of this policy
8258, 8263, 8502 8281 1750	Added support for 45 C.F.R. §§ 164.502(b)(1), 164.514(b), 164.514(c) and PCI DSS 12.3.10 (a). Added reference to VCSATSP 100-100 Restricted Data Access Policy for disclosures. Added
8913, 8914	Requested approval for version 4.0 of this policy