

DOCUMENT INFORMATION

| | |
|------------------------------|----------------------------------------------|
| VCSATS Policy Number: | VCSATSP 100-090 |
| Title: | Data Retention and Destruction Policy |
| Policy Owner: | Infrastructure Manager |
| Effective Date: | 5/1/2013 |
| Revision: | 4.0 |

Table of Contents

| | |
|----------------------------|---|
| DOCUMENT INFORMATION | 1 |
| 1. PURPOSE | 2 |
| 2. SCOPE | 2 |
| 3. RESPONSIBILITIES..... | 2 |
| 4. REFERENCES | 2 |
| 5. DEFINITIONS..... | 3 |
| 6. POLICY | 3 |
| 7. ENFORCEMENT | 4 |
| 8. HISTORY | 4 |

1. PURPOSE

This policy provides rules and instructions regarding data retention and destruction to ensure compliance with University policy, regulatory requirements and contractual obligations.

2. SCOPE

This policy applies to the Vice Chancellor Student Affairs Division, including vendors and business partners, as defined by HIPAA, who store or manage VCSATS data.

3. RESPONSIBILITIES

TABLE 1 - ROLES AND RESPONSIBILITIES

| Role | Responsibility |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Infrastructure Manager | <ul style="list-style-type: none"> • Ensure this document remains current and is updated whenever changes to the policy occur. • Review and approve changes to this document. • Review and approve changes to VCSATSG 100-020 Data Retention Guide. |
| Data Owner | <ul style="list-style-type: none"> • Review and approve changes to this document. • Review and approve retention changes to VCSATSG 100-020 Data Retention Guide. |
| Counsel | <ul style="list-style-type: none"> • Give legal advice or guidance. • Advise on additional retention or destruction needs. |

4. REFERENCES

TABLE 2 - REFERENCES

| Reference | Location |
|--------------------------------------|----------------------|
| VCSATSG 100-020 Data Retention Guide | VCSATS Policy Center |
| 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 |
|-----------------------------|------------|
| None | |

6. POLICY

- 1) Data shall be reviewed on a quarterly basis and retained per the published retention schedule..
- 2) Data retention periods shall comply with all of the following ^{45 C.F.R. § 164.316(b)(2)(i)} PCI DSS 9.1.1 (c) PCI DSS 10.7 (a) , ^{PCI DSS 10.7 (b)} . Where standards differ, the longer retention period shall be used.
 - a) Regulatory requirements
 - b) Contractual obligations
 - c) University policy
- 3) The Data Retention Guide may be modified by the Data Owner and Infrastructure Manager per VCSATSP 100-010 Policy Guidance to ensure compliance as outlined in this policy.
- 4) This policy and shall be reviewed annually to ensure compliance with University policies, regulatory requirements and contractual obligations.
- 5) Data may be destroyed under the direction of the Infrastructure Manager once it has met the retention obligation of this policy and VCSATSG 100-020 Data Retention Guide.
- 6) Where not specified in the guide, Restricted data shall be retained for a period of 8 years, after which it may be destroyed per a published retention schedule.
- 7) In the event UCR is served with a subpoena or request for documents or any employee becomes aware of a governmental investigation or audit concerning UCR or the commencement of any litigation against or concerning UCR, such employee shall inform the Infrastructure Manager. The Infrastructure Manager, in conjunction with the Data Owner, and with the advice of counsel, shall suspend destruction of relevant data until such time as the Infrastructure Manager, in conjunction with the Data Owner, and with the advice of counsel, determine otherwise. The Infrastructure Manager shall take such steps as is necessary to promptly inform all staff of any suspension in the further destruction of relevant data.

7. ENFORCEMENT

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

8. COMPLIANCE REFERENCE INDEX

| | | | |
|-----------------------------------|---|------------------------|---|
| 45 C.F.R. § 164.316(b)(2)(i)..... | 3 | PCI DSS 10.7 (b) | 3 |
| PCI DSS 10.7 (a)..... | 3 | PCI DSS 9.1.1 (c)..... | 3 |

9. HISTORY

| FogBugz Case | Description of Changes |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| 1934 | Create initial version of this work instruction. |
| 4016, 4017 | Requested approval for version 1.0 of this Policy |
| 4910 | Updated document number and references within to match the approved naming convention |
| 6817 | Updated to support PCI DSS 3 |
| 6818, 6819 | Requested approval for version 2.0 of this Policy (Not Approved) |
| 4023, 6819, 6086 | Added Counsel role and other minor edits. Corrected references to the guide. Added section 6.8 as support for 45CFR §164.316 b 2 i |
| 8066, 8067 | Requested approval for version 3.0 of this Policy. (Not Approved) |
| 8805, 8806 | Requested approval for version 4.0 of this Policy |