DOCUMENT INFORMATION

VCSATS Policy Number:	**VCSATSP 100-010**
Title:	**Policy Guidance**
Policy Owner:	**Director Technology Services**
Effective Date:	**2/1/2014**
Revision:	**2.0**

Table of Contents

1. PURPOSE

This policy provides the overall guidance on the approach to the VCSA Division Information Security Framework. Additionally, this policy:

- Provides specific definitions for terms used throughout VCSA policies and VCSATS Work Instructions.
- Addresses UCOP, UCR, regulatory and contractual requirements for information security [PCI DSS 12.1, PCI DSS 12.4].
- Details specific tools, techniques and addresses other matters that are required to consistently implement and use the VCSA Polices, VCSATS Work Instructions and VCSATS Guides.
- Provides the method of obtaining an exception to Policy or Work Instruction.
- Addresses privacy and monitoring.

2. SCOPE

This policy applies to the Vice Chancellor Student Affairs Division.

3. RESPONSIBILITIES

TABLE 1 - ROLES AND RESPONSIBILITIES

Role	Responsibility
Director Technology Services (DTS)	Review and approve changes to this document

4. REFERENCES

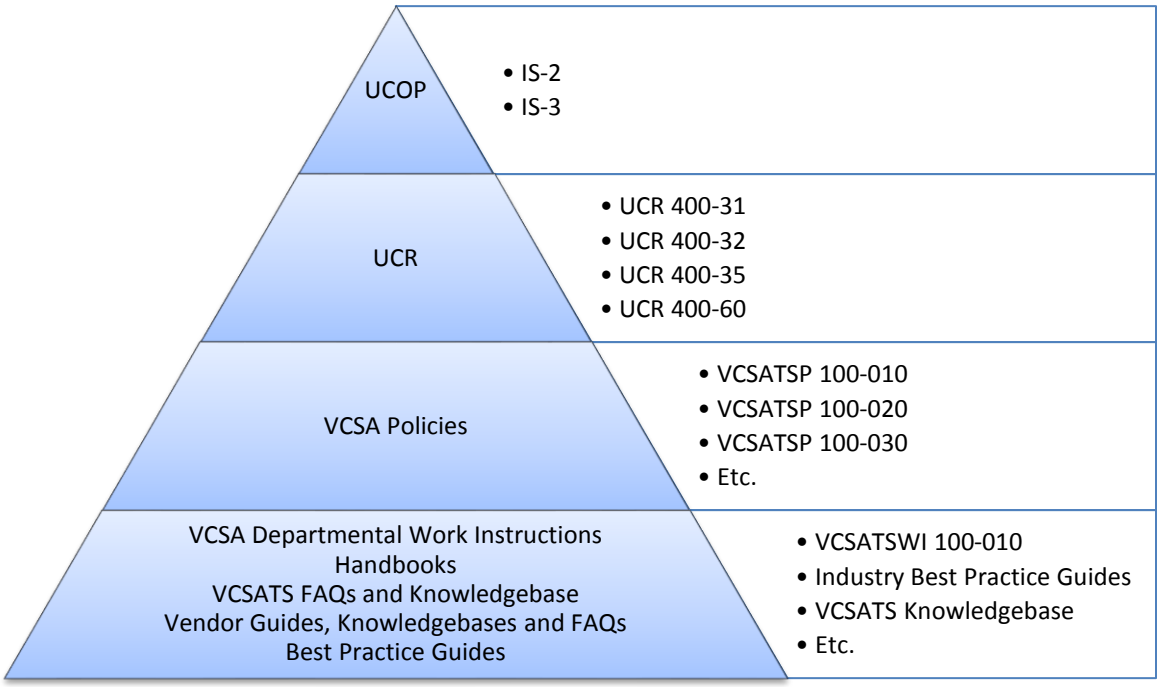
TABLE 2 - REFERENCES

Reference	Location
Policy Framework	VCSATS Policy Center
State of California Information Practices Act of 1977	http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/StateInformationPracticesAct.aspx
VCSATS SharePoint Industry Best Practice Guide Center	http://students894.ucr.edu/sites/Software/InfoSecPolicies/IndustryBPGuides
VCSATSP 100-090 Data Retention Policy	VCSATS Policy Center – Published Policies and Work Instructions Library
UCOP IS-2	http://policy.ucop.edu/
UCOP IS-3	http://policy.ucop.edu/
UCR 400-31	http://fboapps.ucr.edu/policies/index.php?path=viewPolicies.php&policy=400-31
UCR 400-32	http://fboapps.ucr.edu/policies/index.php?path=viewPolicies.php&policy=400-32
UCR 400-35	http://fboapps.ucr.edu/policies/index.php?path=viewPolicies.php&policy=400-35
UCR 400-60	http://fboapps.ucr.edu/policies/index.php?path=viewPolicies.php&policy=400-60

5. POLICY HEIRARCY

For the purposes of complying with regulatory and contractual obligations, this policy defines the policy hierarchy for the VCSA division.

- Policies are tied to good security practice, laws, UCOP or UCR umbrella policies or contractual requirements (PCI). VCSATS policies define standards required for compliance with the described objectives.
- VCSATS work instructions detail how to implement policies. Work instructions establish a repeatable process to produce repeatable results.
- Guidelines or Guide Books are suggested methods, best practices, or clarifications to assist with the implementation of technology.



6. POLICY FRAMEWORK

The Policy Framework is a document that maps regulatory and contractual requirements such as HIPAA and PCI to University, Campus and VCSA documentation such as that listed in section 5 POLICY HEIRARCY.

7. DEFINITIONS

Term, Abbreviation, Acronym	Definition
Anti-Virus	Software used to prevent, detect, and remove malware, including computer viruses, worms, and trojan horses. For the purposes of VCSA, this will typically be Sophos Endpoint Security and Control.
Antivirus	Synonymous with Anti-Virus
Audit and Logging Client	Software used to allow timely detection of and response to unauthorized information processing activities, including but not limited to event tracking, recording user activities and recording system activities.
Case	A record in FogBugz, similar to a ticket in other systems. It is used to track work and communication associated with work. Cases are considered formal recordings of work items, approvals, rejections, and configuration items. All cases entered for a project are considered part of the project record.
Change Review Board (CRB)	Comprised of the Services Manager, Software Manager, Business Analysis Manager, SME, and Infrastructure Manager. The CRB also has as a permanent member, at least one Director or their designee.
Code Review Tool	A tool which facilitates systematic examination of computer source code, interpreted code (script) or configuration/rule files and is intended to find and fix mistakes in these files. For the purposes of VCSA, the Code Review Tool is often Kiln.
Configuration Management	A process for establishing and maintaining consistency of a product's performance and functional and physical attributes with its requirements, design and operational information throughout its life.
CP	Control Point: Used in flowcharts, diagrams, and other Visio-based artifacts to denote a check on the process which ensures effective operation. This usually takes the form of one performer checking the work of another performer.
Closed	FogBugz status applied to a case to show that the work is completed. This is usually applied by the original opener of the case and usually comes after Resolved status, though it may also be applied simultaneously with Resolved status. Closing a case is the action of setting the status of the ticket to Closed.
CRB	Change Review Board
Critical Data	For policy purposes, Critical Data should be considered synonymous with Restricted Data.

Term, Abbreviation, Acronym	Definition
Critical System	For policy purposes, Critical Systems are synonymous with Essential Systems.
Confidential Data	As defined in IS-2, Appendix A – Definitions: "The term confidential information applies broadly to information for which disclosure or access may be assigned some degree of sensitivity, and therefore, for which some degree of protection or restricted access may be identified. Unauthorized access to or disclosure of information in this category could seriously or adversely affect the University and cause financial loss, damage to the University's reputation, loss of confidence or public standing, or adversely affect a partner, e.g., a business or agency working with the University. Information in this category may have limited, moderate, or severe impact on University functions, which must be determined through risk assessment or business impact analysis." Confidential data may or may not include Restricted data. It may also be or not be Essential data.
Confidential System	Any system that deals with Confidential Data and is not identified as a HIPAA or PCI system.
Data Owner	Individual who reviews and authorizes data access requests.
Diagram	This is a flowchart, usually created in Visio. Normally, the flowchart is created to show the roles and steps in a Work Instruction.
Dormant	Inactivity for a period of over 1 year.
DTS	VCSATS Senior Director Technology Services or Director of Security, Services and Infrastructure. Based on the context in which it is used, this can either be the office or specifically the Director/Sr. Director.
Encrypted Archive	Encryption protected file containing one or more files. For the purposes of VCSA, unless specifically noted otherwise, the Encrypted Archive is TrueCrypt. A typical use of the Encrypted Archive is storage of sensitive keys which must be retrieved using unique, identifiable credentials.
Endpoint Protection	Hardware, software, or firmware controls at each endpoint within the network that protect against intrusion, malware, etc. Endpoints can include but are not limited to servers, work stations, phones and POS terminals.

Term, Abbreviation, Acronym	Definition
Essential Data	As defined in IS-3. The classification of Essential notes a financial impact. It does not necessarily have a direct correlation to privacy or confidentiality concerns.
Essential System	A system dealing with Essential Data. Essential classification is not exclusionary. Therefore, Essential Systems may also be classified as HIPAA, PCI, etc.
FogBugz	Integrated web-based project management system featuring bug/issue tracking, work tracking, discussion forums, wikis, customer relationship management, and evidence based scheduling.
IDS	Intrusion Detection System - a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a Management Station
IM	VCSATS Infrastructure Manager Based on the context in which it is used, this can either be the office or specifically the Infrastructure Manager.
Industry Best Practice Guide	Often referenced in Work Instructions. A Best Practice is a method or technique that has consistently shown results superior to those achieved with other means, and that is used as a benchmark. Best practices are used to maintain quality in addition to mandatory legislated standards and can be based on self-assessment or benchmarking. Various entities exist which establish and influence Best Practices for any number of industries. These include, but are not limited to: • Vendor Consortiums (PCI) • Work Groups (W3C) • Standards Organizations/Bodies (ISO) • Governmental bodies (NIST) • Vendors (Microsoft, Cisco, VMWare.) VCSA Industry Best Practice Guides are found in the VCSATS SharePoint Industry Best Practice Guide Center.
IPS	Intrusion Prevention System - also known as intrusion detection and prevention systems (IDPS), are network security appliances or software that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about said activity, attempt to block/stop activity, and report activity.

Term, Abbreviation, Acronym	Definition
Kiln	Source code control management system and code review tool. It also allows for a variety of other digital assets to be placed into version control. Kiln is a primary facilitator of the VCSA Configuration Management system.
Logging Method	System for tracking activity such as accessing a restricted area or server room. This may take the form of a ticket, keycard scan record, or similar. In most cases, the ticket will take the form of a FogBugz case.
Media Destruction	This refers to the disposal of media that still contains Restricted Data. With regard to electronic media, it is the process rendering unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise by physically destroying the media (for example, degaussing), so that the data cannot be reconstructed [PCI DSS 9.10.2]. With regard to non-electronic media, Media Destruction is the process of rendering physical data unrecoverable through normal means. Approved methods of destruction are limited to cross-cut shredding, pulping, or incineration [PCI DSS 9.10.1 (a)]. Vendors must be certified by the National Association for Information Destruction (NAID).
Media Destruction Container	This is a secured container for shredding, incinerating, or pulping media including but not limited to hard drives, print outs, receipts, or DVDs. Media Destruction Containers must be secured from tampering, regardless of the destruction method. Minimally, the container must be locked closed to prevent removal of material by anyone other than the approved destruction vendor [PCI DSS 9.10.1 (b)].
OGC	Office of General Counsel. UCR and UCOP both have this department and OGC is the acronym used to refer to them in singular or collectively based on context.

Term, Abbreviation, Acronym	Definition
Personal Information	California Senate Bill 1386 and Assembly Bill 700, effective July 1, 2003, added a new provision to the California Information Practices Act - Civil Code 1798.29, 1798.82. This new provision requires any state agency (including the University of California) with computerized data containing personal information to disclose any breach of security of a system containing such data to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The Civil Code defines "personal information" to be an individual's first and last name in combination with any of the following (see other definitions): • Social security number and/or • Driver's license number or CA identification card number and/or • Financial account number, credit or debit card number, in combination with any security code, access code, or password that would permit access to the individual's account and/or • Medical information (medical history, mental or physical condition, medical treatment or diagnosis) and/or • Health insurance information (policy number, subscriber information number, individual's application and claims history including appeal records)

Term, Abbreviation, Acronym	Definition
Protected Data	1. As defined in 45 C.F.R. § 160.103, below (HIPAA/HITECH), it is concerned with Electronic Protected Health Information: Protected health information means individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium. (2) Protected health information excludes individually identifiable health information in: (i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and (iii) Employment records held by a covered entity in its role as employer. (This is provided as a reference. However, the latest version of the C.F.R. should always be used.) 2. As defined by UCR and UCOP policy, Protected Data is the data comprising personal information governed by these guidelines is defined as protected data. This protected data includes an individual's first and last name in combination with any of the following: • social security number AND/OR • driver's license number AND/OR • financial account or credit card number in combination with any password that would permit access to the individual's financial account

Term, Abbreviation, Acronym	Definition
Public Data	If data is not considered Restricted, it is considered Public. There are no regulatory or policy restrictions on sharing or protecting Public data. However, measures may be taken to protect the data as deemed appropriate. This definition is for Policy understanding and does not alter responsibilities to consult with campus counsel, FERPA officer, HIPAA officer or other appropriate campus executive/officers.
Public System	Public systems are those which do not host restricted data. Public systems may still be hardened as deemed appropriate.
Resolved	FogBugz case status indicating that the work listed in the case is believed to be completed. There are various forms of Resolved status, all variations of which list different descriptions of why the work is completed (Completed, Duplicate, etc.) Resolved status is not the same as Closed.
Restricted	Dealing with Restricted Data, including but not limited to hosting, creating or accessing.
Restricted Data	As defined in UCR 400-32 II.C. See section 9 of this document for more detail. Data which, if made available to unauthorized persons, may adversely affect UCR, its programs, or participants served by its programs. Examples include, but are not limited to, personal identifiers, treatment records, Protected Information as defined in this policy, student records (see section 8 DATA CLASSIFICATION for more detail) and financial information.
Restricted Information	See Restricted Data
Risk	Risks are potential events, either positive or negative, that could have an impact on a project or system. They are not in effect today but they could be realized if a triggering action occurs. Trigger events for Risks always have a mathematical probability of less than 1. If the probability is equal to 1, then the Risk has become an Issue.
Risk Based Approach	Used by an organization to focus on the threats that matter to its business – mission, operational, financial, environmental and so on -- and implements the controls and processes required to protect against those risks. The impact costs of the risk occurring are evaluated against the costs of mitigation to find the right balance. The rationale is documented to support the outcome.

Term, Abbreviation, Acronym	Definition
Vulnerability Management Guidance Source	Recommended sources for finding or subscribing to updates regarding the most current developments with regard to threats, vulnerabilities, and related practices. • National Vulnerability Database - nvd.nist.gov • Open Source Vulnerability Database – osvdb.org • SecurityFocus weekly newsletters – www.securityfocus.com • Security Alert Consensus by Neohapsis, Network Computing, and SANS – http://archives.neohapsis.com/ appears • ISS Monthly Security Alert Summary – www.iss.net/threats/ThreatList.php • National Cyber Alert System - www.us-cert.gov/referral_pg/
Sensitive Information	Synonymous with Restricted Data.
Server Hardening Guide	A type of Industry Best Practice Guide used to reduce risks and areas that can be exploited by threats.
SME	Subject Matter Expert or domain expert is a person who is an expert in a particular area or topic.
Threat	The combination of an actor, motivation for that actor to do harm, and a vulnerability which that actor can exploit to do harm. Threat can also exist from an actor who may unintentionally and/or unknowingly do harm.
Ticket	Either a Web Help Desk ticket or FogBugz case.
Ticketing System	Either FogBugz or Web Help Desk based on the context in which the term is used.
TrueCrypt	Disk encryption software providing On The Fly Encryption (OFTE) of for data at rest. TrueCrypt does not encrypt data in transit. Users require uniquely assigned A-accounts in order to access the TrueCrypt archive.
Vault	Vaulting is the act of placing an object into storage. Within VCSA, Vaults can take several forms based on the context in which the term is used: **SharePoint**: Vault for documents such a Project Plans, policies, status reports, etc. **Kiln**: Vault for code, binary objects, or any other type of digital asset as necessary. **FogBugz**: Vault for correspondence, project records, work requests, etc.

Term, Abbreviation, Acronym	Definition
VCSA	Vice Chancellor Student Affairs. Based on the context in which it is used, this can either be the organization, the office, or specifically the Vice Chancellor.
VCSA Download Site	VCSA portal for obtaining approved software.
VCSATS	Vice Chancellor Student Affairs Technology Services – an information technology unit operating as a division wide resource.
VCSATS Industry Best Practice Guide Center	SharePoint repository containing guides referenced in various work instructions. • Guides are placed directly into the "Industry Best Practice Guide Center." • Guides do not require formal approval and are updated directly in the "Industry Best Practice Guide Center."
VCSATS Policy Center	SharePoint repository containing Policies, Work Instructions, and Guides. • Policies and Work Instructions are created and approved in the "Documents" Library • Approved Policies and Work Instructions have copies placed into "Published Policies and Work Instructions"
Version Control	Also known as source control or configuration management it is the management of changes to a configuration item. Management of configuration items includes but is not limited to the ability to store and retrieve multiple revisions of a configuration item with a history of changes from revision to revision. For the purposes of VCSA, Version Control is facilitated by Kiln or SharePoint as appropriate.
Vulnerability	As defined by NIST SP 800-30, it is a flow or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.
Work Instruction	Outlines how to perform a process with the goal of repeatable execution that conforms to policy.
Work Product	Documents, configurations, rule sets, security settings, diagnostic output, architecture, data flow, use case, error case, source code, database schemas, scripts, or any other items created for the University. Typically, these are to achieve project objectives or support ongoing activities.

8. DATA CLASSIFICATION

8.1 Restricted

Data classified and protected by regulatory, University and contractual obligations such as Electronic Protected Health Information covered by HIPAA/ HITECH, Cardholder Data as covered by PCI, and other protected information such as but not limited to Social Security Numbers, addresses, etc.

8.2 FERPA

A subset of Restricted data. It differs from other Restricted data in that it is used campus wide and outside of the scope of VCSATS. Instead, it is managed according to policies set by the FERPA privacy officer and/or by the campus. FERPA data is protected on VCSATS servers with similar technical controls to Restricted data though incidental or occasional transfer of information is not covered.

8.3 Non-Restricted

All other data that does not fall into the Restricted and FERPA categories. Typically this is public data.

8.4 System Classification

The system classification shall be documented in the Risk Assessment for the system. If a component of the system is listed as restricted, the entire system shall be considered to be restricted unless:

- Restricted components are isolated from non-restricted and FERPA components.
- The isolation of the restricted components is demonstrable.
- The Risk Assessment lists the isolated components.
- Evidence of the isolation is vaulted.

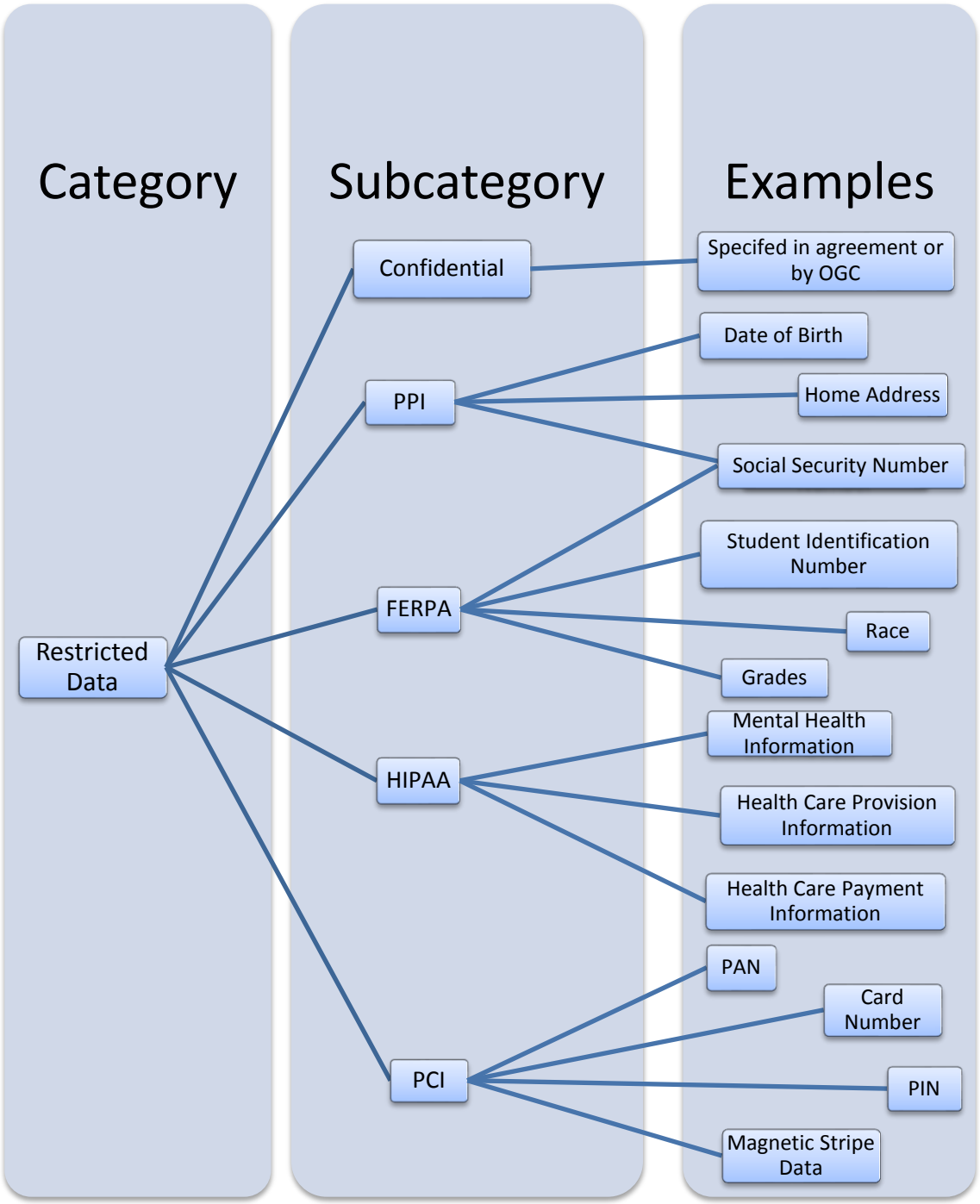
8.5 Questions on determining classification

For questions and guidance on determining classification, contact the following individuals:

- HIPAA – contact the HIPAA Privacy Officer.
- FERPA – contact the FERPA Privacy Officer.
- All other questions – contact the Director of Technology Services.

9. RESTRICTED DATA BREAKDOWN

The following diagram provides a visual depiction to help create a clear understanding of the relationships of the elements of Restricted Data.



10. EVIDENCE BASED COMPLIANCE

An evidence-based approach to work is the accepted Best Practice within VCSA as the organization is subject to internal and external audit. The following activities comprise the key components of the Best Practice to support compliance:

- All work must be associated with a ticket. This is commonly referred to as "No ticket, no work."
- Sufficient detail regarding the work associated with the ticket must be recorded. For example, initiation, tasks completed, approvals, and final disposition should be clearly recorded and explained in a manner such that they could be used to demonstrate compliance.
- Work under the assumption that all work done will come into the scope of an audit in the distant future.
    - Has the work been recorded?
    - Is it able to be understood years from now?
    - Is it able to stand on its own?
    - Is it able to be understood without explanation from the author?

11. APPROVED TOOLS

VCSA approved tools support Best Practices relevant to security, project management, configuration management, and audit support. They facilitate collaboration, production of consistent work products, and evidence-based compliance. VCSA approved tools include:

- FogBugz
- Kiln
- Web Help Desk
- SharePoint

12. SYSTEMS OF RECORD

Any and all components of an approval record must be kept in a system of record.

- Approved systems of record are SharePoint, Kiln, FogBugz and Web Help Desk.
- Email is not an approved system of record. Any email that constitutes part or all of an approval record must be vaulted in one of the approved systems of record listed above.

13. INFORMATION SECURITY MONITORING AND PRIVACY DISCLOSURE

Vice Chancellor Student Affairs Technology Services (VCSATS) is charged with operating technology to support the division and maintaining security. In order to minimize risk and provide the needed safeguards to protect operations and information resources, VCSA requires that the security of every computing system or device connected to the network be established and maintained. To ensure the integrity and reliability of systems, VCSATS uses various techniques that include routine monitoring of electronic communications.

This section explains the techniques used to monitor VCSA electronic communications exclusively as well as the limitations of that monitoring. It may not include different practices and requirements implemented by UCR's Computing and Communication on other systems or other segmented networks.

13.1 Practices

I. Intrusion Detection

VCSATS uses a combination of automated technology and manual review to identify systems that are attacking campus information resources, may be infected with malware, or fail to meet minimum security requirements. The automated systems use a combination of pre-determined signatures and traffic analysis to collect and store a relevant portion of electronic communications for systems or user accounts identified as a potential threat to the campus network. Security staff may manually review these stored collected electronic communications, in accordance with University and UCOP privacy policies as well as the law, to validate the findings or tune the automated systems.

The information collected may include: source and destination IP addresses, source and destination ports, URLs, and user names.

II. Logs

VCSATS stores and utilizes a variety of logs. Logs that have been "red-flagged" as identified by a pre-determined system algorithm may be manually or automatically reviewed in accordance with applicable policies and law to verify incident reports.

III. Network and System Logs

Network and System logs are created and stored for all network traffic to and from VCSA servers and the internet. Logs are created and stored for devices sending electronic communication within VCSA managed environments.

The information may include: source and destination IP addresses, source and destination ports, packet counts, and byte counts.

IV. Authentication Logs

Authentication logs are created and stored for access to VCSA resources, such as logon, VPN, etc. VCSA system owners may also create and store their own logs.

The information may include: source and destination IP addresses, URLs, and user names.

V. Blocking

Users or systems that are "red-flagged" and determined to be a threat as described in section 13.1 may be blocked and denied network access until the issue is resolved. Blocked user accounts may also be denied access without additional information. VCSATS will make best efforts to directly contact the account or system owner by email, but this is not always possible.

13.2 Privacy

VCSA recognizes that principles of academic freedom and shared governance, freedom of speech, and privacy hold important implications for the use of electronic communications.

VCSATS employees who operate and support electronic communications resources regularly monitor transmissions for the purpose of ensuring reliability and security of University electronic communications resources and services, and in that process might observe certain transactional information or the content of those electronic communications. Except as provided in University and UCOP privacy policies or by law, VCSATS employees are not permitted to seek out transactional information or contents when not germane to system operations and support, or to disclose or otherwise use what they have observed.

In the process of such monitoring, any unavoidable examination of electronic communications (including transactional information) shall be limited to the least invasive degree of inspection required to perform such duties. This exception does

not exempt systems personnel from the prohibition against disclosure of personal or confidential information.

Network traffic may be inspected to confirm malicious or unauthorized activity that may harm the campus network or devices connected to the network. Such activity shall be limited to the least perusal of contents required to resolve the situation. User consent is not required for these routine monitoring practices.

The data of separated employees becomes the property of the University and, with DTS and Assistant/Associate Vice Chancellor approval, may be accessed to support University operations.

Except as provided above, systems personnel shall not intentionally search the contents of electronic communications or transactional information for violations of law or policy. However, if in the course of their duties, systems personnel inadvertently discover or suspect improper governmental activity (including violations of law or University policy), reporting of such violations shall be consistent with the Policy on Reporting and Investigating Allegations of Suspected Improper Governmental Activities (the "Whistleblower Policy").

14. THE FUNCTION OF ROLES WITHIN POLICIES AND WORK INSTRUCTIONS

Roles may be performed by different individuals as necessary. Role is not synonymous with title.

For example, a Business Analyst (BA) role could be performed by a business user or technical staff based on the scenario.

15. EXCEPTIONS TO POLICY AND WORK INSTRUCTIONS

The goal of VCSA is to follow UCOP, UCR, and VCSA policy. In addition, VCSATS has the goal of following approved VCSATS work instructions. In the event that a business, regulatory requirement, officer, etc. requires deviation, the following steps must be taken:

- Document and vault the rational for the deviation.
- Obtain written approval from the proper authority.
    - For policy deviation, obtain written approval from DTS, the Assistant or Associate Vice Chancellor and other campus officers as required. VCSA approval may also be required based on the nature of the exception.
    - For work instruction deviation, obtain written approval from DTS.
- Vault the written approval.
- Implement the deviation using a risk based approach and follow the rational.

16. DISCIPLINARY ACTION

All staff are expected to work based on UCR's Accountability Ethic: We will be accountable as individuals and members of this community for our ethical conduct and compliance with applicable laws and University policies and directives. This is a core job responsibility and is subject to campus performance management processes.

17. POLICY QUESTIONS AND SUPPORT

To submit questions or request support regarding policies, work instructions, or guides, follow the methods below:

- All staff may contact their manager, or;
- VCSATS staff are to open a FogBugz case to submit the question or support request.
- All other VCSA staff are to open a Web Help Desk ticket to submit the question or support request.

18. COMPLIANCE REFERENCE INDEX

19. HISTORY

FogBugz Case	Description of Changes
3202, 5045, 5547, 8460, 8997, 10294, 10536, 10776, 10777	Create initial version of this policy.
10789	Version 1.0 vaulted but not routed for approval.
10795	Created version 1.3 to produce a working copy while final reviews take place. The intent is that this document still provides definitive guidance with the expectation that minor changes will be made prior to formal issue.
15511	Added “Data Owner” to the definitions section and made formatting changes.
15848, 15849	Requested approval for version 2.0 of this document.