VISC Incident Response Guideline

REVISION CONTROL

Document Title:	VISC Incident Response Guideline
Author:	Click here to enter author.
File Reference:	VISC Incident Response Guideline Draft.docx

Revision History

Revision Date	Revised By	Summary of Revisions	Section(s) Revised
10/07/11	Danita Leese	Copy and paste to new template	All

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
2/7/2012	VISC Governance	Approved

Table of Contents

Page

1.0 INCIDENT RESPOSE PROCEDURES

1.1 Purpose

The purpose of this document is to outline the procedures that VISC Member Campuses will use for addressing and reporting security incidents as well as procedures the VISC will use for responding to security incidents. This procedure allows for a coordinated response from the VISC, the VISC Computer Security Incident Response Team (CSIRT), as well as others involved in investigations.

1.2 Scope

The procedures outlined in this document apply to all VISC Member Campuses.

2.0 VISC MEMBER CAMPUS CONTACT REQUIREMENTS

Each VISC Member Campus will be required to set up a list of contact resources. These resources will act as a liaison between the VISC CSIRT and the VISC Member Campuses. Depending on the type of incident that the VISC CSIRT responds to will determine how these resources will be used. These resources should be appointed and in place well in advance of any requests for response from the VISC CSIRT.

- **Campus Chief Information Officer (CIO):** The Campus CIO, or a designee, should make a determination if an incident is Low Severity and if so, handle the incident internally. If the Campus CIO determines that the incident is a higher than a Low Level Severity Incident, the incident will be forwarded to the VISC for handling. If notifications need to be made as a result of an incident, the Member Campus CIO will be contacted in order to start the notification process. That Campus CIO would then make notifications to Campus upper-level management (See Appendix 2: VISC Security incident Response Procedure – Notification Tree).
- **Help Desk**: Depending on the type of incident reported, the VISC CSIRT may require the resources of the reporting Campus' Help Desk. These resources may include:
    1. Creation of Administrative credentials for VSIC CSIRT.
    2. Deployment of forensic client to assets that require forensic response.
- **Network Team**: Depending on the type of incident reported, the VISC CSIRT may require the resources of the reporting Campuses Network Team. These resources may include:
    1. Segregation of compromised hosts from the network to prevent further damage.
    2. Enabling of ports /IP addresses required for forensic response.
- **Server Team**: Depending on the type of incident reported, the VISC CSIRT may require the resources of the reporting Campuses Server Team. These resources may include:
    1. Access to tape backups.
    2. Access to Campus Exchange/Mail Servers.

3.0 INCIDENT SEVERITY LEVELS

3.1 High Severity Levels

The VISC Director and campus liaison will assign an incident a High Severity Level (Level 1) if it meets the following criteria:

- Incidents that could have long term effects on the Campus community.
- Incidents that affect critical systems or have a Campus-wide effect.
- Incidents that could damage the reputation of the University.
- Incidents that are a violation of State and/or Federal law.

Examples of incidents that would be rated as High Severity include:

a. Security compromise on Campus enterprise systems or applications

b. Cyber-stalking

c. Patriot Act violations

d. Loss or theft of Level 1 (Confidential) information

e. International, Federal, State, or Local law violations including:

I. HIPPA

II. FERPA

III. Child Pornography

The VISC will immediately contact the individual that reported the incident in order to obtain a clear understanding of the scope of the incident. If necessary, the VISC will activate the CSIRT and determine the appropriate steps to be taken to rectify the incident. The reporting Campuses CIO will be notified so they may determine if other notifications (legal counsel, law enforcement, etc.) will need to be made.

For High Severity Level Incidents, the owner(s) or /operator(s) of the affected hosts will typically be directed to disconnect the device/system from the network and not to use or modify the device/system in any way until the VISC CSIRT has contacted them and provided instructions.

3.2 Medium Severity Incidents

The VISC Director and campus liaison will assign an incident a Medium Severity Level (Level 2) if it meets the following criteria:

- Incident indicates a threat of a future attack (network reconnaissance).
- Incident has a strong possibility of affecting a large portion of the Campus network.
- If there is imminent danger of modification of the public's perception of the VISC Member Campus due to information security reasons other than disclosure of personal and sensitive information or disruption of service (i.e. main web page has been modified in an unauthorized manner, but orders can still be processed), then assign the incident Medium Severity.

Examples of incidents that would be rated as Medium Severity include:

a. Loss or theft of Level 2 (Sensitive) information

b. Web site defacement

c. Personal business operations using Campus resources

d. Unauthorized excessive resource utilization

e. Compromised Faculty/Staff accounts

3.3 Low Severity Incidents

The VISC Member Campus CIO will assign an incident a Low Severity Level (Level 3) if it meets the following criteria:

Low severity incidents are those incidents where there is no imminent threat to California State University, VISC Member Campus systems, or VISC Member Campus confidential and sensitive data. Low security level incidents can typically be handled by the VISC Member Campus IT Department and will rarely require VISC CSIRT response.

Examples of incidents that would be rated as Low Severity include:

- Malware/virus infected system connected to the Campus network
- Copyright infringement notifications (RIAS, MPAA, DMCA)
- Illegal sharing of copyrighted materials including music, movies, and software
- Compromised student accounts
- Unauthorized servers including:
    a. Game Servers
    b. Chat Servers
    c. File Servers
    d. DHCP servers

There may be cases where a Low Severity Incident is required to be escalated to a higher level incident based upon the findings of that incident. As an example, if a system is infected with Malware and it is determined that the system contains unprotected Level 1 (Confidential) data, that incident would be escalated to a High Severity Level incident and the VISC Director would need to be notified in order to activate the VISC CSIRT.

4.0 VISC INCIDENT RESPONSE PROCESS

VISC member campuses may receive notifications of an incident from several sources including:

- Help Desk
- Network Operations
- Campus Staff / Faculty
- External Agencies
- The Public

When a VISC Member Campus is notified of an incident that requires that may require VISC CSIRT be activated, the CIO, or a designee, of that Campus in conjunction with the VISC Director will make a determination as to the severity level of that incident. Low Severity Level incidents can typically be handled by the individual Campus IT Department. All other Incidents will be forwarded to the VISC Director for activation of the VISC CSIRT.

At that time, the VISC CSIRT will handle coordination of the incident including:

- Notification to the CIO or designee of the Campus reporting the incident. Depending on the severity of the incident, the CIO of the reporting Campus may need to make additional notifications to the upper-level management of the reporting Campus. Notification to Law Enforcement may also be required.
- If necessary, the VISC CSIRT will coordinate with the reporting Campuses Network Team to quarantine the system on which the incident took place to prevent further compromise. It may also be necessary for the Network Team of the reporting Campus to open ports to allow forensic tools to pass data back to the VISC CSIRT locate at California State University Fullerton.
- If necessary, the VISC CSIRT will coordinate with the reporting Campuses Help Desk to obtain administrative credentials for that Campus in order to perform the forensic response.
- The VISC CSIRT will perform a preliminary analysis of the incident which will include:
    - Identifying incident cause
    - Determine if personal and/or Campus information is at risk
    - Evidence collection
    - Remedial actions
    - Recommendations
- Coordinate additional assistance, if necessary, to provide and to preserve incident evidence.
- Investigate information on website defacements.
- Notify or alert campus users if newly reported vulnerabilities are identified on Operating Systems, server or services, applications, or network devices.

At the conclusion of an incident a report will be generated by the VISC CSIRT that will be signed off on by the VISC Director. Copies of these reports will be made available to the CIO, or a designee, of that Campus. All reports and evidence collected will be archived unless otherwise specified.

The VISC is available to assist member Campuses deal with security incidents that might affect their respective Campus.

An Information Security Incident is generally defined as any known or highly suspected circumstance that results in an actual or possible unauthorized release of information deemed confidential or sensitive by the University or subject to regulation or legislation, beyond the University's sphere of control.

Examples of an Information Security Incident may include but are not limited to:

- The theft or physical loss of computer equipment known to hold files containing SSNs.
- An unencrypted list of alumni contributors emailed to an unauthorized recipient.
- A server known to hold sensitive data is accessed or otherwise compromised by an unauthorized party.
- Printed copies of student loan applications are discovered in a publicly accessible dumpster.
- An outside entity is subjected to a DDoS (Distributed Denial of Service) attack originating from within the University network.
- A firewall is accessed by an unauthorized entity.
- A network outage is attributed to the activities of an unauthorized entity.

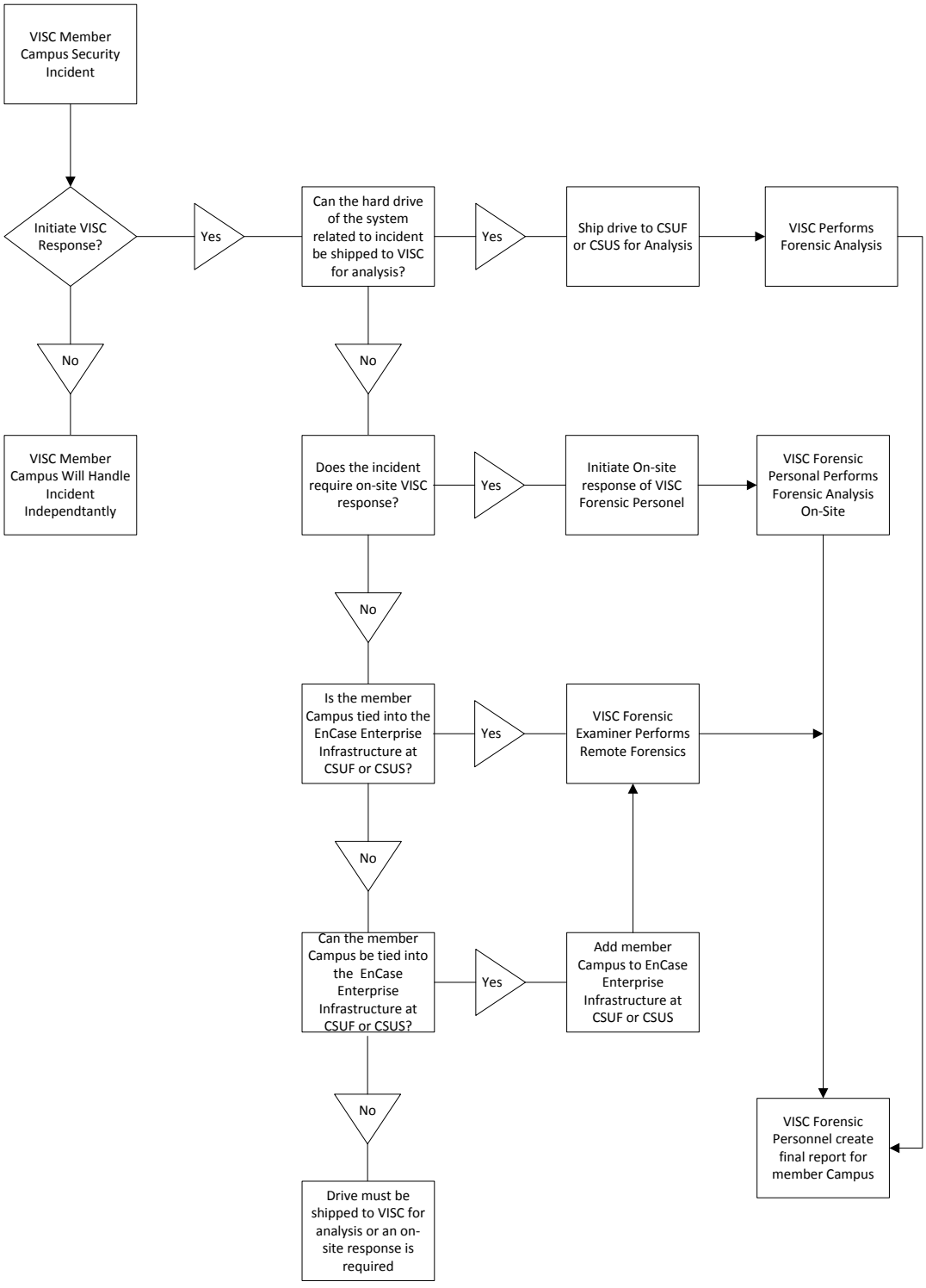
Typically, any Campus security incident that results in the loss or possible loss of Level 1 or Level 2 data should be handled by the VISC. Incidents that deal with Level 3 data can usually be handled by the member Campus but VISC involvement can still be requested. For examples of data for each Level Type, see Appendix A.

Level 1 Data: This is information that can cause the most serious harm to individuals and to the campus as a result of unauthorized access. Much of this information is protected by statutes, regulation, other legal obligation or mandate. The CSU has identified specific guidelines regarding the disclosure of much of this information to parties outside of the University and controls needed to protect the unauthorized access, modification, transmission, storage, or other use.

Level 2 Data: This is information that must be guarded due to proprietary, ethical or privacy considerations.

Level 3 Data: This is information that is regarded as publicly available. These data values are either explicitly defined as public information (e.g., state employee salary ranges), intended to be readily available to individuals both on- and off- campus (e.g., an employee's work email addresses), or not specifically classified elsewhere in the protected data classification standard. Publicly available data may still be subject to appropriate campus review or disclosure procedures to mitigate potential risks of inappropriate disclosure.

APPENDIX A: VISC INCIDENT RESPONSE PROCESS MAP



APPENDIX B: INFORMATION CLASSIFICATION

Classification	Description	Examples
Level 1	This is information that can cause the most serious harm to individuals and to the campus as a result of unauthorized access. Much of this information is protected by statutes, regulation, other legal obligation or mandate. The CSU has identified specific guidelines regarding the disclosure of much of this information to parties outside of the University and controls needed to protect the unauthorized access, modification, transmission, storage, or other use.	• Passwords or credentials • PINs (Personal Identification Numbers) • Birth date combined with last four of SSN and name • Credit card numbers with cardholder name • Tax ID with name • Driver's license number, state identification card, and other forms of national or international identification (such as passports, visas, etc.) in combination with name • Social Security number and name • Medical records related to an individual • Psychological Counseling records related to an individual • Bank account or debt card information • Vulnerability/security information related to a campus or system
Level 2	This is information that must be guarded due to proprietary, ethical or privacy considerations.	**Identity Validation Keys** • Birth date (full: mm-dd-yy) • Birth date (partial: mm-dd only) • Mother's maiden name **Student Information** • Educational records (Excludes directory information) – Grades – Courses taken – Schedule – Test Scores – Advising records – Educational services received – Disciplinary actions • Non-directory student information may not be

Classification	Description	Examples
		released except under certain prescribed conditions **Employee Information** • Employee net salary • Employment history • Home address • Personal telephone numbers • Personal email address • Parents and other family members names • Payment History • Employee evaluations • Background investigations • Biometric information • Electronic or digitized signatures • Private key (digital certificate) • Birthplace (City, State, Country) • Ethnicity • Gender • Marital Status • Personal characteristics • Physical description • Photograph **Other** • Linking a person with the specific subject about whom the library user has requested information or materials. • Legal investigations conducted by the University. • Sealed bids • Trade secrets or intellectual property such as research activities • Location of assets

Classification	Description	Examples
Level 3	This is information that is regarded as publicly available. These data values are either explicitly defined as public information (e.g., state employee salary ranges), intended to be readily available to individuals both on- and off-campus (e.g., an employee's work email addresses), or not specifically classified elsewhere in the protected data classification standard. Publicly available data may still be subject to appropriate campus review or disclosure procedures to mitigate potential risks of inappropriate disclosure.	**Campus Identification Keys** • Campus identification number User ID (do not list in a public or a large aggregate list , protection of SPAM, where it is not the same as the student email address) **Student Information** • Educational directory information (FERPA) **Employee Information** • Employee Title • Employee public email address • Employee work location and telephone number • Employing department • Employee classification • Employee gross salary • Name (first, middle, last) (except when associated with protected information) • Financial budget information • Signature (non-electronic)

APPENDIX C: VISC INCIDENT RESPONSE HANDLING

When should a VISC member Campus notify the VISC regarding a security incident on their Campus?

Whenever a VISC member Campus experiences a security incident, no matter how large or small, the VISC should be notified immediately prior to taking any actions on potentially compromised systems.

If a VISC member Campus believes a system may be infected that contains University Level I or Level II Data or it is believed a system may be participating in a Denial of Service (DoS) attack, can that system be unplugged from the Campus network?

Yes, in these cases the VISC recommends that the system be unplugged from their respective Campus network. No further action should be taken on these system(s) prior to contacting the VISC. A system that is believed to be involved in a security incident should never be powered down prior to contacting the VISC.

What if a VISC member Campus takes actions on a system involved in a security incident prior to contacting the VISC?

If a member Campus were to take actions against a system (i.e. attempt to fix the issue, run virus scans, etc.) that is believed to be involved in a security incident, those actions may prevent the VISC from initiating and following through with a proper investigation. These actions may also prevent due legal process if such process is warranted.

Will the VISC always handle security incidents at member Campuses?

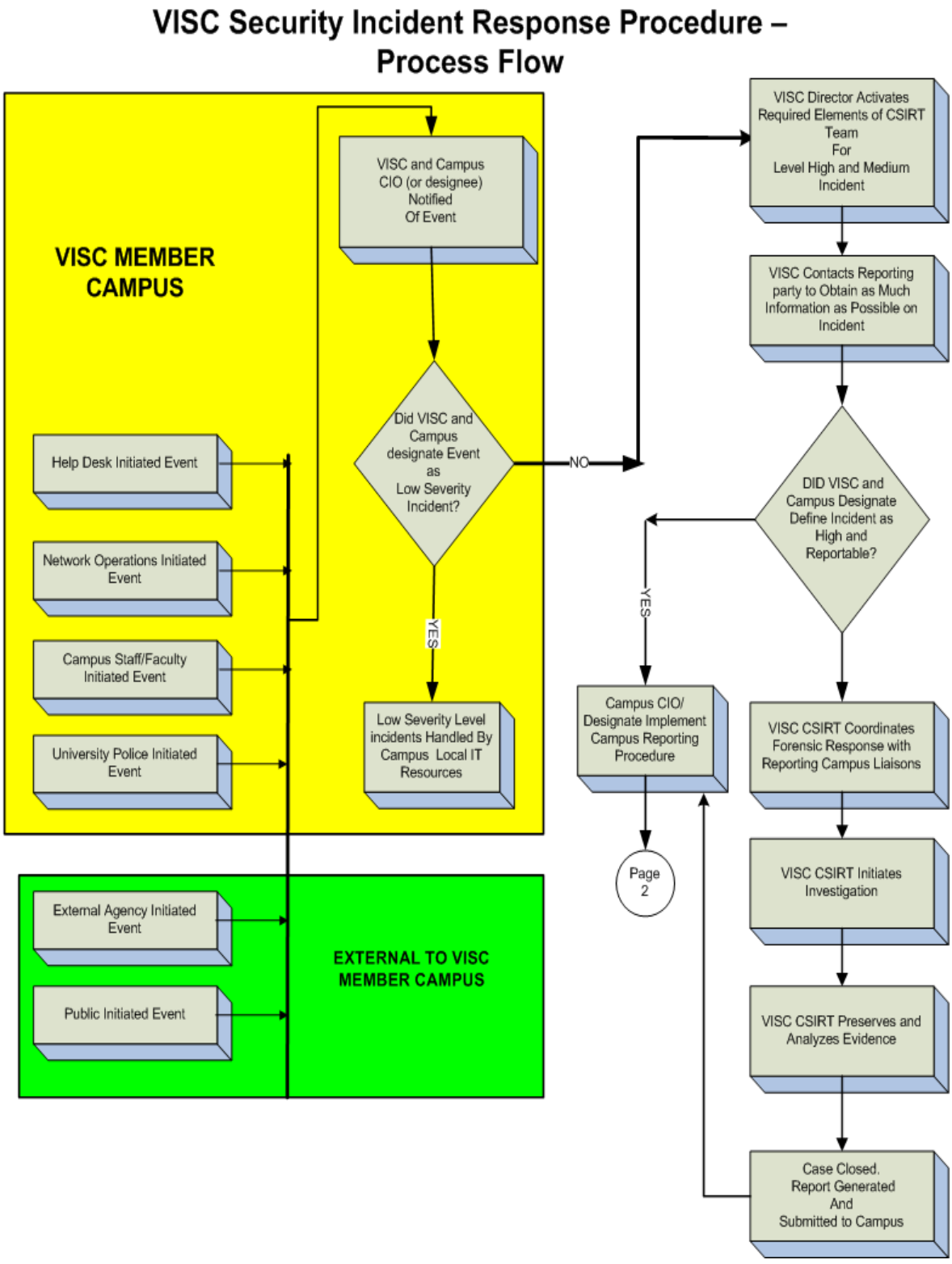
Some incidents may be handled by the member Campus themselves depending upon their nature and/or scope. Security incidents should first be reported to the VISC where it will be determined if a VISC response is warranted or required.

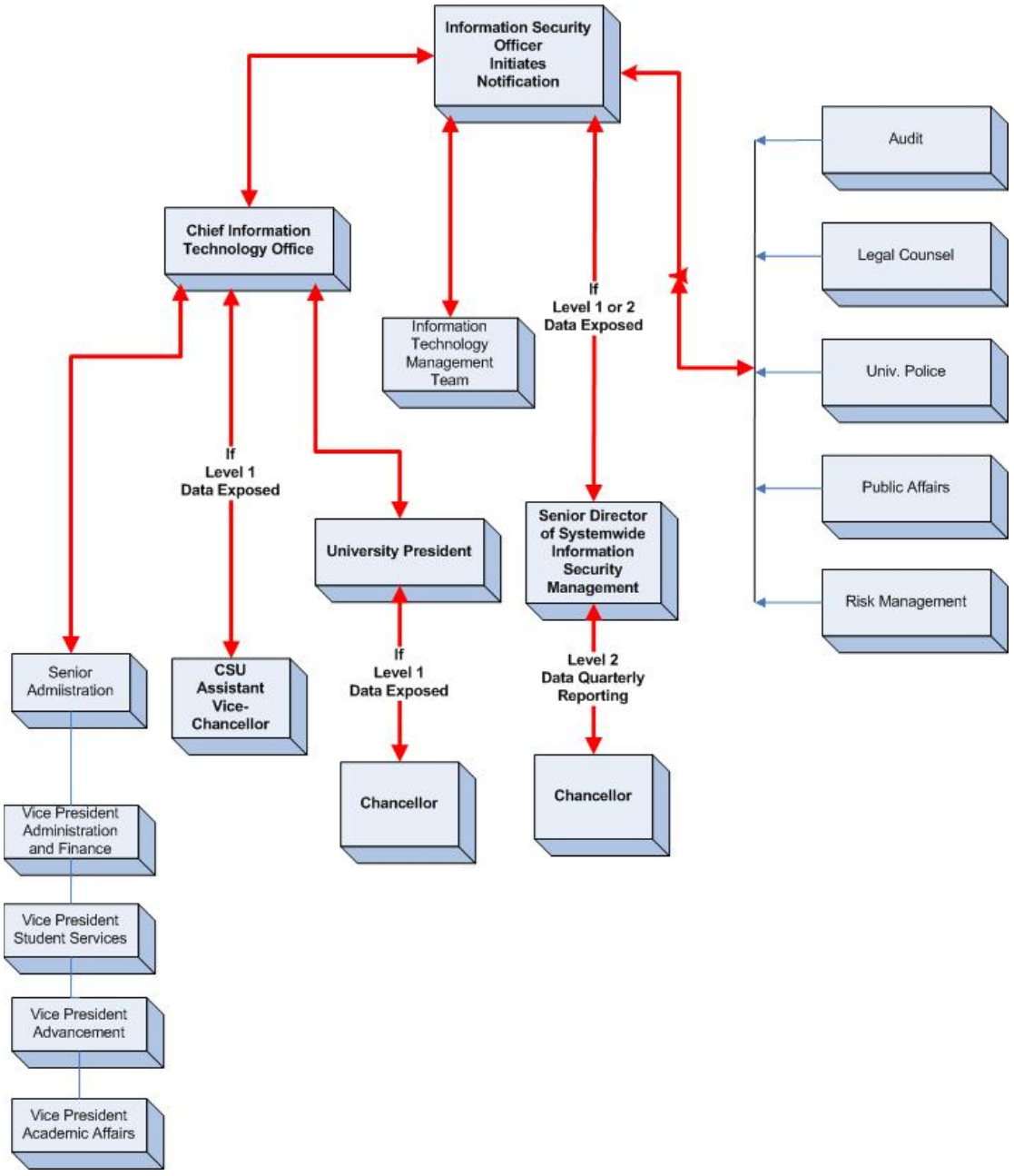
To reach a VISC Incident Response Handler:

Call: (657) 278-3765

Email: visc@calstate.edu

APPENDIX D: PROCESS FLOW CHARTS




Information Security Officer Initiates Notification
Audit
Legal Counsel
Univ. Police
Public Affairs
Risk Management
Chief Information Technology Office
Information Technology Management Team
If Level 1 or 2 Data Exposed
If Level 1 Data Exposed
University President
Senior Director of Systemwide Information Security Management
Senior Admiistration
CSU Assistant Vice-Chancellor
If Level 1 Data Exposed
Level 2 Data Quarterly Reporting
Chancellor
Chancellor
Vice President Administration and Finance
Vice President Student Services
Vice President Advancement
Vice President Academic Affairs