

Computer Incident Response Team – Operational Standards

Office of Information and Educational Technology

1.0 Overview

This document defines the establishment of a computer Incident Response Team. The purpose of the Incident Response Team is to limit the adverse effects of misuse or abuse of UC Davis computer or network resources and/or prevent loss of or damage to electronic information resources.

The Incident Response Team will follow the operational standards in this document. The standards provide a formalized approach to computer/network incident identification, investigation and reporting.

The standards will be periodically updated to reflect the changing technology environment and campus needs. Request for changes to the Incident Response Team standards should be forwarded to the campus designated Information Resource Security Guidelines Coordinator (Security@ucdavis.edu).

If there are conditions under which the applicability of the standards is unclear, it is the responsibility of the campus user to seek interpretive guidance from the Information Resource Security Guidelines Coordinator.

2.0 Establishment of Incident Response Team

2.1 Incident Response Team (IRT)

The Incident Response Team is an ad hoc group of technology and functional specialists established by the Office of Information and Educational Technology for the investigation and reporting of computer/network security incidents. Security incidents are events that could adversely affect UC Davis computer or network resources and/or cause loss of or damage to electronic information resources.

2.2 Incident Response Goals

The overall goal of the IRT is to protect and preserve electronic information and network assets to ensure the availability, integrity and, as required, confidentiality, of campus electronic information and network assets.

Computer Incident Response Team – Operational Standards

Office of Information and Educational Technology

2.2 Incident Response Objectives

There are five primary objectives of the IRT:

- Control and manage the incident
- Timely investigation and assessment of the severity of the incident
- Timely recovery or bypass of the incident to normal operating conditions
- Timely notification of the incident to senior campus administrators
- The prevention of similar incidents in the future.

3.0 Incident Response Organization

Campus response to computer/network security incidents is handled within a framework of the UC Davis Misuse Committee and Incident Response Team (IRT). The UC Davis Misuse Committee provides high-level oversight of the IRT. The Committee also actively participates in any information technology (IT) incident investigation that is classified with the highest severity rating.

The IRT is the operational team of specialists that is responsible for conducting an incident investigation and recommending measures to correct or bypass a problem or condition relating to the incident. The nature of the incident will determine the actual role the IRT will have in respect to implementing a corrective or preventive action. For example, if an incident is traced to a departmental hardware source, it may be the responsibility of the specific department staff to implement a corrective action.

3.1 Misuse Committee

The Misuse Committee is composed of the Vice Chancellor of Resource Planning and Budget, Vice Provost for Academic Affairs, Campus Counsel, Associate Vice Chancellor for Human Resources, Director of Internal Audit Services, UCDCM Compliance Officer and Chief of Police. As determined by the Chairperson of the Misuse Committee, the campus designated Information Resource Security Guidelines Coordinator will participate in the Misuse Committee, as requested, during discussions involving the suspected abuse and/or misuse of computing and/or network resources.

3.1.1 Misuse Committee – Responsibilities

The primary responsibility of the Misuse Committee, in regards to IT incidents, is to provide operational guidance to the IRT. Such guidance may include, but not be limited to, general investigative protocol, data/evidence preservation, information custody issues, quality assurance and report content. In addition, the Misuse Committee may authorize the request of external law enforcement assistance in an incident investigation

Computer Incident Response Team – Operational Standards

Office of Information and Educational Technology

The Misuse Committee will receive IRT notification for all investigations involving incidents classified with a moderate or high severity rating. The Misuse Committee will actively consult with the IRT on all incidents that have been classified at the highest severity rating. The Misuse Committee must approve the escalation of an incident from a lower severity rating to the highest severity rating. The Misuse Committee must also approve the de-escalation of an incident from the highest severity rating to a lower severity rating.

3.1.2 Misuse Committee – Consultation with Vice Provost, Information and Educational Technology

The Misuse Committee will notify the Vice Provost, Information and Educational Technology, of any high-severity incident or incident containment action that, in the judgment of the Committee, will disrupt the broad availability of UC Davis electronic resources, without the consent of resource users. Such incident containment action would only be taken when required by and consistent with law, when there is substantiated reason to believe that violations of law or University policies may have taken place, when there are compelling circumstances, or under time-dependent, critical operational circumstances.¹

The Misuse Committee will also notify the Vice Provost, Information and Educational Technology, of any incident that requires campus-wide coordination, or initiation of investigation communication with collateral organizations and/or external law enforcement agencies. Collateral agencies include, but are not limited to organizations such as the Carnegie Mellon University CERT Coordination Center, and the Forum of Incident Response and Security Teams (FIRST).

In the absence or unavailability of the Vice Provost, Information and Educational Technology, the Misuse Committee will notify the Chief Operations Officer, Information and Educational Technology.

3.2 Incident Response Team (IRT)

The IRT is an ad hoc group of technical and functional specialists. The actual team consists of a core team of technical specialists who are assisted by functional specialists, depending on the nature of a particular incident under investigation.

¹ Policy Section III.E, Access Restriction, Electronic Communications Policy, University of California, Office of the President, November 17, 2000.

Computer Incident Response Team – Operational Standards

Office of Information and Educational Technology

3.2.1 IRT – Core Team Members

The IRT is composed of a minimum of six members. Two members each participate from Information Resources and Communication Resources and the Deans and Vice Chancellors will appoint the remaining two members. These core team members are journey-level specialists with operating system and/or telecommunication and network knowledge and skills. The Directors of the Communications Resources and Information Resources, respectively, appoint the two staff members to serve indefinite assignments on the IRT. The Chief Operations Officer, Information and Educational Technology, will confirm the IET appointments. The Deans and Vice Chancellors will annually appoint two members to the IRT.

The organizational unit participants are further distinguished as either a primary or alternate IRT member. This distinction assists incident communication between the IRT members and coverage scheduling.

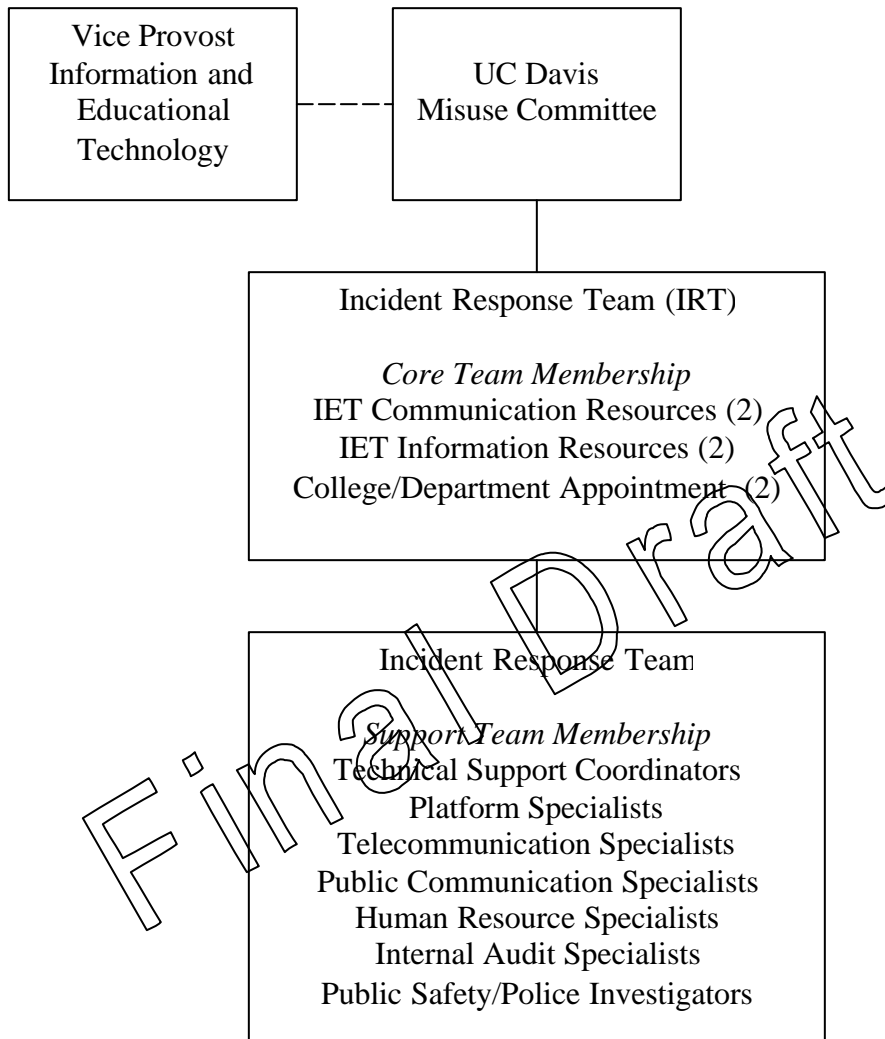
Any security incident investigation, which focuses on an IET administered system, will be performed by a minimum of two IRT members.

Final Draft

Computer Incident Response Team – Operational Standards

Office of Information and Educational Technology

Diagram of Incident Response Team Organization



Computer Incident Response Team – Operational Standards

Office of Information and Educational Technology

3.2.2 IRT – Core Team Responsibilities

The primary responsibilities of the IRT are investigation and reporting. In order to carryout these responsibilities, the following support activities will be performed be the IRT:

- Maintain availability for 24x7 communication access and incident response
- Develop and maintain incident classification scheme
- Monitor UC Davis abuse listserv and other campus reporting mechanisms for reports of incident reports
- Notify and consult with campus Technical Security Coordinators
- Assess scope of incident damage
- Classify incidents by severity
- Determine if incident can be investigated
- Control and contain incident
- Collect, document and preserve incident evidence
- Maintain chain of custody of all incident evidence
- Interview individuals involved in incident
- Conduct investigation to identify incident root cause of source, extent of damage, and recommended counter action
- Coordinate release of information with public communications staff
- Consult with law enforcement agencies, as authorized
- Follow all policies, laws and regulations relating to privacy
- Prepare reports describing incident investigations
- Prepare recommendations to prevent future similar incidents
- Prepare recommendations to disrupt incident and/or reduce impact of incident
- Prepare recommendations to bypass or correct conditions leading to incident
- Monitor recovery
- Identify IRT operational improvements
- Assist recovery from incident, where applicable

3.2.3 IRT – Support Team Members

Support members are not permanent IRT members. The support team members have expertise in particular subject matter that could be relevant to an IRT investigation. The IRT leader will determine when such expertise is required during an investigation. The support member will be added to the incident team at that time.

Any security incident investigation, which includes a departmental computing system, will be conducted by a minimum of three IRT members. One of the three members will represent the department computing system under review.

Computer Incident Response Team – Operational Standards

Office of Information and Educational Technology

Support Team members will typically be drawn from the following areas:

- Technical Support Coordinator
When the target of the security incident is a departmental computing/network system, not administered by IET staff, the IRT will include a Technical Support Coordinator from the impacted department. This IRT member will typically be a technical or administrative specialist who is responsible for supporting the system that is being misused or experiencing some other type of unauthorized activity. For example, if an incident involves a department email server, the IRT leader will request the subject department to designate a technical or administrative IRT participant. This participant would be expected to possess the requisite experience and knowledge to assist in the investigation.
- Platform Specialists (e.g., Operating Systems, Applications, Hardware)
- Telecommunication Specialists (e.g., Network Infrastructure, Microwave, Wireless, Telephones)
- Public Communication Specialists
- Human Resource Specialists
- Internal Auditors
- Public Safety/Police Investigators

3.2.4 Support Team Responsibilities

The primary responsibilities of the IRT Support Team members are to assist IRT Core Team investigation and reporting. The Support Team members provide professional and technical expertise to the IRT core team in special subject knowledge areas. Type responsibilities Support Team members include:

- Assess scope of incident damage
- Assist classification of incidents by severity
- Assist determination whether incident can be investigated
- Assist control and containment of incident
- Collect, document and preserve incident evidence
- Maintain chain of custody of all incident evidence
- Interview individuals involved in incident
- Assist investigation to identify incident root cause or source, extent of damage, and recommended counter action
- Provide public communications guidance
- Provide guidance regarding law enforcement role
- Follow all policies, laws and regulations relating to privacy
- Assist preparation of reports describing incident investigations
- Assist preparation of recommendations to prevent future similar incidents
- Assist preparation of recommendations to disrupt incident and/or reduce impact of incident

Computer Incident Response Team – Operational Standards

Office of Information and Educational Technology

- Assist preparation of recommendations to bypass or correct conditions leading to incident
- Assist monitor recovery
- Identify IRT operational improvements
- Assist recovery from incident, where applicable

3.2.5 IRT - Leader

The IRT leader designation will be periodically rotated among core IRT members. The team leader is responsible for the initiation of an IRT investigation and IRT activities performed in support of the investigation. These responsibilities include:

- Convene IRT
- Notify Misuse Committee regarding new incidents and investigation status
- Conduct IRT meetings
- Coordinate IRT investigation
- Ensure incidents are classified according to severity class
- Determine investigation objectives
- Define/obtain resource requirements
- Communicate with external agencies, as authorized by Misuse Committee
- Coordinate IRT training and exercises
- Prepare post-investigation “Lessons Learned” analysis
- Request support team resources
- Prepare IRT management reports
- Consult with Information Resource Security Guidelines Coordinator on incidents classified with a moderate or high severity rating.
- Communicate with senior department managers regarding incident investigation status
- Advise Misuse Committee on incident investigations
- Arrange for responsibility coverage during temporary absences

Computer Incident Response Team – Operational Standards

Office of Information and Educational Technology

4.0 IRT Operational Resources

In order to conduct incident response investigations, the IRT needs to acquire and maintain selected investigation tools. In addition, the IRT needs to have a physically secure location to store investigation tools, conduct investigation analysis and store material collected and/or prepared during the incident investigation. The following operational resources will be used by the IRT:

- Hardware
 - Portable data storage devices
 - Workstations (Win/Apple/Unix)
- Software
 - Forensic analysis
 - Forensic imaging
 - Password recovery
 - Encryption Software
 - Cryptographic Hash Utilities
- Miscellaneous Supplies
 - Photographic Imaging Equipment
 - Portable evidence storage containers
 - Spare backup media
 - Locking file cabinets
- Secured physical room with restricted entry

Final Draft

Computer Incident Response Team – Operational Standards

Office of Information and Educational Technology

5.0 IRT Training

IRT team members are required to obtain training and periodic updates in the following knowledge and skill areas:

- State and Federal Laws
- UCOP and UC Davis policies
- Investigative processes
- Evidence handling and protection
- Technical IRT hardware and software tools
- Testimony skills

6.0 IRT Exercises

The IRT will conduct an annual exercise that simulates a computer security incident. The purpose of the exercise will be to maintain the skills and knowledge of IRT members. The exercises will involve all IET core team members. Support team members will be selected to participate as required by the nature of the exercise. At the termination of the drill, the IRT leader will prepare a brief report to the Misuse Committee evaluating the exercise. Any skill and/or knowledge area that needs to be improved as well as procedural enhancements will be identified in the report.

7.0 Incident Definition

For the purposes of this document, an incident is defined as an event that has actual or potential adverse effects on computer or network resources resulting in misuse or abuse; compromise of information; or loss or damage of property or information. Any such events that originate from, are directed towards, or transit University controlled computer or network resources will fall under the purview of the Incident Response Team. This definition is purposely made inclusive, however it is foreseen that many events classified with a “limited” severity rating may be handled by semi-automated means and not require any further escalation.

Incident types include, but are not limited to, denial of service, port scans, system break-ins, email abuse, copyright infringement, and non-acceptable use. Incidents that involve known or suspected misuse of University resources typically fall under the purview of the UC Davis Misuse Committee.² If the misuse investigation involves computer systems, the IRT is not a participant in the investigation unless the Misuse Committee requests the assistance of the IRT through the Information Resource Security Guidelines Coordinator.

² Misuse of University Resources, UC Davis Policy and Procedure Manual 330-95

Computer Incident Response Team – Operational Standards

Office of Information and Educational Technology

8.0 Reporting New Incidents & User Notification

An incident can be reported through existing central reporting mechanisms. A campus community member or anyone affected by a campus network incident should report a suspected incident by email (abuse@ucdavis.edu). In addition, the IRT will coordinate with the IT Express, Data Center Operations and Network Operations Center to ensure that the IRT is notified of any reported problem that may reflect a security incident.

The individual reporting the incident will be asked to provide date, time, timezone, user contact information, brief description of the incident, and, if available, source and target network information.

Acknowledgement of a reported incident by the IRT shall occur via an auto-generated response to email or web notifications. A telephone-reported incident will be acknowledged with a telephone call or email message from the IRT. All user reports will be analyzed, classified by severity rating, and an appropriate response will be generated. The scope of the IRT response will be determined by the incident severity rating, or as directed by senior campus administrators.

If the nature of the incident cannot be reported via non-confidential methods, the incident may directly reported to the Information Resources Security Guidelines Coordinator, Information and Educational Technology or Vice Provost, Information and Educational Technology.

Final Draft

Computer Incident Response Team – Operational Standards

Office of Information and Educational Technology

9.0 Incident Classification and Prioritization

Incidents will be analyzed and the severity of the incident classified according to several factors. As a guide, the overall severity classification of an incident will be higher based on the critical nature of the targeted system for the campus and broad negative organization and user impact of the incident. The overall severity classification of an incident will be reduced when there are readily available alternatives to remedy or bypass the problem situation. Severity ratings will be labeled as limited, moderate or high.

The IRT will use the following table as a guideline in establishing incident severity.

Incident Factors	Severity Characteristics		
	Limited	Moderate	High
Criticality – Application	Non Tier 1 or 2 App	Tier 2 Application	Tier 1 Application
Criticality – Infrastructure	No	Limited scope	Campus-wide impact
Impact – User/system	Affects a few people or a few systems	Department-wide impact	Campus-wide impact
Impact – Public	None	Potential impact	Likely impact
Countermeasures	Solutions are readily available	Weak countermeasures	No countermeasures
Resolution procedures	Available and well-defined	Resolution procedure not well-defined	No resolution procedures available

Incidents receiving a “high” severity classification will receive the highest priority of IRT resources. In the case of multiple incidents, the higher severity rating incidents will receive higher priority IRT work assignment.

The incident severity classification will also determine the degree of involvement of campus senior managers in respect to the incident investigation. The following table describes the typical participation levels for the Misuse Committee and Vice Provost, Information and Educational Technology.

Computer Incident Response Team – Operational Standards
Office of Information and Educational Technology

Incident Response Advisory Group	Severity Characteristics		
	Limited	Moderate	High
UC Davis Misuse Committee involvement	<ul style="list-style-type: none"> • None 	<ul style="list-style-type: none"> • UC Davis Misuse Committee advises IRT • UC Davis Misuse Committee approves incident severity escalation to highest category 	<ul style="list-style-type: none"> • UC Davis Misuse Committee advises IRT • UC Davis Misuse Committee approves incident closure • UC Davis Misuse Committee approves de-escalation of high-severity incident • UC Davis Misuse Committee approves external law enforcement involvement
VPIET involvement	<ul style="list-style-type: none"> • None 	<ul style="list-style-type: none"> • UC Davis Misuse Committee may consult with VPIET 	<ul style="list-style-type: none"> • UC Davis Misuse Committee consults with VPIET

Computer Incident Response Team – Operational Standards

Office of Information and Educational Technology

10.0 Incident Classification Escalation/De-escalation

All new incidents will be assigned a severity rating by the IRT leader. Such incident ratings may change over the course of an incident as more information about the incident becomes available and is reviewed by the IRT. The IRT leader, in consultation with the IRT members, will determine if an incident rating should be escalated or de-escalated. The same criteria used to initially rate a newly reported incident will be used to escalate or deescalate an incident severity rating.

10.1 Incident Severity Escalation

If an incident is escalated to a “moderate” rating, the IRT leader shall inform the UC Davis Misuse Committee via email about the incident and the reason for the escalation. This escalation shall be communicated to all IRT members involved in the incident investigation.

If an incident is escalated from a “limited” or “moderate” severity rating to a “high” severity rating, the IRT leader will review the incident with the UC Davis Misuse Committee via telephone or an ad hoc meeting. The UC Davis Misuse Committee must approve the incident escalation. The UC Davis Misuse Committee, through the Information Resource Security Guidelines Coordinator, will notify the Vice Provost, Information and Educational Technology in regards to any “high” severity rated incident and its possible campus impact.

10.2 Incident Severity De-escalation

The IRT leader may determine an incident rating should be de-escalated to a “moderate” or “limited” category. If a “high” severity incident is downgraded to a “moderate” or “limited” severity rating, the IRT leader must receive approval of the UC Davis Misuse Committee. In such cases, the reason for the de-escalation shall be documented within the incident investigation. The Vice Provost, Information and Educational Technology shall be informed by the IRT of the de-escalation and the reason for the action.

If the incident was previously rated as “moderate” and is downgraded to “limited”, the UC Davis Misuse Committee shall be informed about this action and the justification of the change. The other IRT members involved in the investigation will be notified of the change.

Computer Incident Response Team – Operational Standards

Office of Information and Educational Technology

11.0 Incident Investigation Process

The incident definition, defined in section 7.0, is purposely made inclusive, however it is foreseen that many events classified as limited may be handled by semi-automated means and not require any further escalation. Those events classified with a limited severity rating will follow standard procedures, customized to the units that perform those responsibilities. The incident investigation process defined in this section is geared toward incidents with a moderate or severe rating.

The incident investigation process follows the general objectives of investigation methodology, including:

- Conduct objective, thorough and timely incident investigations
- Preserve individual privacy rights
- Collect, preserve and protect incident/investigation data
- Maintain confidentiality as required
- Maintain thorough documentation of entire investigation process.
- Safeguard investigation material/documentation
- Maintain chain of custody of investigation material/documentation
- Develop conclusions fully supported by facts in evidence
- Conduct a post-incident review of investigation and document policy or procedural issues that enhanced or hindered the incident detection, monitoring, investigation and subsequent development and implementation of corrective or problem bypass measures.

Phase One Identification and Assessment Steps

- Identify and verify problem (incident types and descriptions)
- Characterize the damage and extent of the problem, rate the incident severity
- Determine what investigation actions are to be taken
- Determine IRT resources are required to conduct the investigation, request/secure hardware, software, personnel resources
- Communicate with parties that need to be aware of the investigation

Phase Two Containment and Eradication

- Collect and protect of information associated with an incident investigation
- Contain the incident and determine further recovery or bypass actions to taken
- Eliminate intruder's means of access and any related vulnerabilities

Phase Three Recovery and Follow-up

- Return the systems to normal operations
- Close out the problem and follow up with a periodic post mortem review of the investigation. See “Incident Closure” section for details.

Computer Incident Response Team – Operational Standards

Office of Information and Educational Technology

- Prepare and publish report, as required. If an incident has a rating of severe, a brief formal report to UC Davis Misuse Committee shall be submitted upon closure of the incident. The report shall describe the incident, investigation methods, general conclusion, recommendations to avoid future related incidents and, if appropriate, lessons learned from the investigation.

12.0 Incident Tracking

The Incident Response Team will log, track and document the investigation and resolution of all security incidents. Where possible, software will be used to perform these functions. The IRT supporting software will generate a trouble ticket within the "security schema," a set of forms containing customized fields and actions.

The trouble ticket data for a particular incident investigation will only be available to the IRT members participating in the investigation and UC Davis Misuse Committee. The trouble ticket data will not include any personally identifiable confidential information. Reports and summaries based on this data shall be generated as provided in Section 13, Incident Reporting.

13.0 Incident Reporting

The reports identified in this section will be generated from the incident tracking system. Where possible, these reports will be generated and distributed automatically:

Daily aging report: A daily report shall be sent via email to the IRT leader and to the Information Resources Security Coordinator on the status of the open tickets.

Monthly statistics report: A monthly report summarizing the incidents over the previous month shall be sent to IET Publications; Information Resource Security Guidelines Coordinator; UC Davis Misuse Committee; Chief Operations Officer, Information and Educational Technology; and Vice Provost, Information and Educational Technology.

Quarterly statistics report: A quarterly report shall be forwarded to the UC Davis Misuse Committee, IRT core members, Technology Share Participants, IET Publications, Technology Infrastructure Forum, Administrative Coordinating Computing Council, and Academic Coordinating Computing Council containing a summary of incidents investigated during the previous quarter. The quarterly report will also include an evaluation of incident trends, including popular entry methods, prevention tips, and new tools.

Computer Incident Response Team – Operational Standards

Office of Information and Educational Technology

Real-time Alerts: As determined appropriate by the Information Resource Security Guidelines Coordinator, alerts describing recent computer/network threats identified by IRT investigations and vulnerability prevention methods will be distributed on a timely basis. Such alerts may be distributed by web publications and/or other means, such as listservs.

Final Draft

Computer Incident Response Team – Operational Standards

Office of Information and Educational Technology

14.0 Incident Closure

Once the systems have been returned to normal operations, the IRT will verify that all corrective and/or preventive tasks are complete and that local services have been restored. In cases where an organizational unit external to Information and Educational Technology is responsible for incident resolution, the IRT Leader will monitor and document incident resolution.

If an incident is rated as a limited severity, the IRT Leader or an individual designated by the IRT Leader may close it. If an incident is rated with a moderate severity, the IRT must approve closure of the incident. If an incident has received a high severity rating, the UC Davis Misuse Committee must approve closure of the incident.

At any time, the UC Davis Misuse Committee; Vice Provost, Information and Educational Technology; Provost, or Chancellor may terminate an incident investigation, regardless of incident severity rating. If an incident is turned over to a law enforcement agency, the IRT incident investigation will, in most cases, be terminated.

15.0 IRT Relationship to Other Campus Organizations

The following campus organizations may be involved with an incident:

- Business Contracts Office (DMCA, copyright law)
- Human Resource & Risk Management, Employee & Labor Relations (staff issues)
- Information and Educational Technology (IET) - Information Resources (account management, email abuse, help desk, core IRT)
- IET - Communication Resources - Network Operations Center (network-related issues, core IRT)
- IET -Office of Information and Educational Technology (communication)
- Office of the Provost (faculty issues)
- Student Housing (RESNET and student issues)
- Student Judicial Affairs (student issues)
- UCD Medical Center (UCDMC) University of California Davis Health System (UCDHS) (Med Center incidents)
- Electronic Security Advisory Council
- Technology Infrastructure Forum
- Administrative Computing Coordinating Council
- Academic Computing Coordinating Council
- Technology Support Program

Computer Incident Response Team – Operational Standards

Office of Information and Educational Technology

Appendix Definitions

Administrative Computing Coordinating Council (AdC3) reviews proposals and plans that seek to promote the use of information technology for administrative purposes and make appropriate recommendations to the Provost and Executive Vice Chancellor. The Council may also recommend its own proposals and plans. The Council's broad representation will assist the campus administration in assuring that campus resources are deployed to their most strategic advantage. The Council shall recommend administrative computing-related policy to the Information Technology Policy Board. Policy interpretation and financial decision impasses shall also be referred to the Policy Board. The Council may choose to perform its work through smaller subcommittees.

Academic Computing Coordinating Council (AC4) reviews proposals and plans that seek to promote the use of information technology in instruction, research, and public service at UC Davis and makes appropriate recommendations to the Provost and Executive Vice Chancellor. The Council may also recommend its own proposals and plans. The Council's broad representation assists the campus administration in assuring that campus resources are deployed to their most strategic advantage. The Council recommends academic computing-related policy to the Information Technologies Policy Board. Policy interpretation and financial decision impasses are also referred to the Policy Board.

Collateral organizations These organizations have a direct interest in information security issues but are not directly affiliated with UC Davis.

External law enforcement agencies A federal or local government body of civil officers charged with maintaining public order and safety and enforcing the law, including preventing and detecting crime.

Information Resource Security Guidelines Coordinator Individual appointed by the Chancellor to coordinate campus-wide implementation of security controls for disaster recovery, authorization, authentication, system administration, change management, communications security, malicious code, and physical/environment of critical and essential campus applications and systems. The role and responsibilities of the Information Resource Security Guidelines Coordinator are identified and defined within the University of California, Business and Finance Bulletin IS-3.

Misuse Committee This group is charged with implementing the Misuse of University Resources (PPM Section 330-95). Organizational participants include the Office of Resource Management and Planning, Office of the Vice Provost - Academic Personnel, Internal Audits Services, Human Resources, Campus Counsel, and Police Department.

Personally Identifiable Confidential Information Information contained in a student record that would not generally be considered harmful or an invasion of privacy if disclosed. UC Davis has designated several categories of student information as public.

Computer Incident Response Team – Operational Standards

Office of Information and Educational Technology

Public information categories that could be contained in a trouble ticket include the student's name, addresses (local or permanent, including e-mail addresses), and telephone numbers.

Security schema The security schema defines the tables and the fields in the trouble ticket database and the relationships between fields and tables.

Technical Security Coordinators The Technology Support Program (TSP) at UC Davis is a program coordinated by Information and Educational Technology. The program is designed to form close alliances between the central information technology organization and individual departments on campus. The goal is to help departmental support staff provide effective front-line information technology support on an individual and small group basis, particularly for departments that require more specialized attention. Departments wishing to participate are asked to select a department staff member to act as this front-line information technology support person - referred to as a Technology Support Coordinator (TSC)

Technology Infrastructure Forum The Technology Infrastructure Forum is a campus-wide committee comprised of technology specialists from all UC Davis schools, colleges, and administrative units. The Forum provides a mechanism for identifying, evaluating, and resolving critical information technology infrastructure issues for the campus. The Forum focuses primarily on "middleware" issues such as security, authentication, digital certificates, and directories.

Tier 1 and 2 Applications Critical and essential applications used in support of UC Davis teaching, research or public service programs (UC Davis PPM 200-45).

UC Davis Abuse Listserv An e-mail-based mailing list used by campus community and external users for the reporting of misuse or abuse of UC Davis computer or network resources.

Vice Provost, Information and Educational Technology The Vice Provost provides leadership in all aspects of campus-wide information technology policy and planning to ensure effective and strategic deployment of information and educational technologies for the UC Davis campus.