


<p>CAMPUS POLICY</p>  <p>UNIVERSITY OF COLORADO at COLORADO SPRINGS</p>	<p>POLICY NUMBER: 700-005</p>	<p>PAGE NUMBER: 1 of 1</p>
	<p>CHAPTER: Information Technology</p>	
	<p>SUBJECT: UCCS Computer Security Incident Response</p>	
	<p>EFFECTIVE DATE: 10/16/08</p>	
<p>OPR: Information Technology</p> <p>VC: Information Technology</p>	<p>SUPERSESION:</p> <p>APPROVED: by Pamela Shockley-Zalabak, Chancellor on October 16, 2008</p>	

I. POLICY

This policy establishes a requirement for the creation of a UCCS Computer Security Incident Response Plan at the University of Colorado at Colorado Springs.

II. AUTHORITY FOR CAMPUS POLICIES

Authority for the creation of campus administrative policies is found in the *Laws of the Regents*, 1990, Article 3 Section B.8, which states:

The chancellor of the University of Colorado at Colorado Springs shall be the chief academic and administrative officer responsible to the president for the conduct of affairs of the Colorado Springs campus in accordance with the policies of the Board of Regents. The chancellor shall have such other responsibilities as may be required by these *Laws*, the Board, and as may be delegated by the president.

III. PURPOSE

The purpose of a Computer Security Incident Response Plan is to provide the University with a plan that outlines how UCCS will respond in the event of a serious computer security incident. A computer security incident is an event involving university-owned computer resources that threatens confidentiality, integrity or availability of University information assets.

IV. DEFINITIONS

- A. Information Assets: Technology including but not limited to data, computer hardware, computer software, networks owned or operated by the University of Colorado.

V. PROCEDURES

- A. The Information Technology Department shall develop and promulgate a Computer Security Incident Response Plan.

- B. The Information Technology Department shall review and revise the plan annually or as needed due to changes in the industry.
- C. All UCCS staff, faculty, students, contractors, affiliates and community members utilizing University technology resources are responsible for compliance with this policy and the subsequent plan.

VII. HISTORY

VIII. ATTACHMENTS:

Attachment A-UCCS computer Security Incident Response Plan

UCCS Computer Security Incident Response Plan

October 2, 2008

1. Purpose

The purpose of this Computer Security Incident Response Plan (CSIRP) is to provide the University with a plan that outlines how UCCS will respond in the event of a serious computer security incident. A computer security incident is an event involving university-owned computing resources that *threatens confidentiality, integrity or availability* of University information assets. This plan focuses on events with high impact and threat, involving high risk and vulnerability.

This document defines the roles and responsibilities for UCCS employees who may be called upon to help discover, report, investigate or remediate a computer security incident. It also outlines a process flow for incident management, includes a communication hierarchy chart and briefly describes how the incident will be communicated to organizations outside of UCCS.

2. Scope

This CSIRP applies to all information technology devices, systems and networks owned by the University of Colorado at Colorado Springs (UCCS), or used to store University data, or connected to the University's network. The UCCS IT department is mandated to take all actions necessary to assure the protection of UCCS's reputation, information assets and the student's, faculties', and staff's information assets that reside under UCCS's control.

3. Roles and Responsibilities

Computer security incidents may occur that require full participation of University personnel as well as organizational unit leadership to properly manage the outcome. Various roles and responsibilities must be fulfilled to ensure that appropriate leadership and technical resources are involved in successfully resolving an incident and minimizing damage to the University.

Within this section, the roles and responsibilities during a computer security incident are defined for the Chief Technology Officer / Executive Director of IT (CTO), Information Technology Security Principal (ITSP), Computer Incident Response Team (CIRT), the Information Technology department (IT), and other supporting organizations.

3.1. Chief Technology Officer / Executive Director of IT (CTO)

The CTO will either involve or inform as the needs of the incident dictate. Communication of information during an incident will follow this flow to eliminate confusion and misinformation between groups.

The CTO is responsible for executing or delegating the following:

- i. Setting priorities
- ii. Notifying the University Chancellor and the Office of Information Security that an incident has occurred
- iii. Participating with the ITSP in forensic investigation decisions
- iv. Designating an alternate to cover the responsibilities of the CTO role
- v. Managing incident resources
- vi. Notifying University Relations as appropriate for internal and external communication
- vii. Notifying Human Resources as appropriate
- viii. Notifying Legal Counsel as appropriate
- ix. Notifying Campus Public Safety as appropriate
- x. Defining and issuing 'gag' orders within IT for particularly sensitive issues; the default guideline for communicating about a computer security incident is on a need-to-know basis

3.2. Information Technology Security Principal (ITSP)

This position will update the CTO on a regular basis during a critical incident. The ITSP will obtain technical expertise based on the incident declared.

The ITSP is responsible for the following:

- i. Receiving and recording the incident report
- ii. Declaring the security incident and its severity if appropriate
- iii. Coordinating the incident response and task assignments
- iv. Activating the CIRT and notifying the team of meeting locations
- v. Maintaining communications between CIRT and the CTO
- vi. Reminding staff that communication is on a need to know basis, or if the CTO has defined a 'gag order' informing team members of the 'gag'
- vii. Beginning a case file for the incident and ensuring information and evidence are properly collected and documented
- viii. Working with the CIRT to determine the root cause of the incident
- ix. Working closely with the CTO and Legal during forensic investigations
- x. Raising dependency issues as they arise
- xi. Identifying external personnel/resources as needed
- xii. Certifying that all systems are returned to operational quality
- xiii. Assuring secure destruction/retention of all materials at incident's close.
- xiv. Escalating the incident's severity if warranted
- xv. Ensuring that proper follow-up debriefing and reporting occur
- xvi. Adjusting procedures so that responses to future incidents are improved

3.3. Computer Incident Response Team (CIRT)

The CIRT is UCCS's response team designed to assist the UCCS IT Security Principal in handling security incidents. The CIRT must be capable of quickly coordinating internal and external organizations to collect evidence and act on it. Its members must determine whether to pursue the attackers for prosecution (possibly allowing the attack to continue to catch them in the act and capture evidence) or protect the system (contain, eradicate and recover immediately). The team must also disseminate incident information to IT staff, the user community and to various CU and governmental organizations.

3.3.1 Members of the CIRT

The IT Security Principal will be the coordinator of the CIRT. Additionally, for each individual security incident, the CIRT may be composed of different individuals, including but not limited to:

- The CTO / Executive Director of IT
- Senior technical members of the IT staff
- Appropriate IT staff based on the type of platform (Windows, Mac, Linux, etc.) that was affected
- The Web Services Manager when fitting
- The IT User Services Manager when fitting
- The appropriate System Administrator for the system or server that was affected.

3.3.2 Reasons for Convening the Computer Incident Response Team

The CIRT will be convened if the security incident:

- Is likely to become public knowledge
- Places individuals at risk of identity theft, financial loss, or other negative consequences
- Significantly impacts the institution's services, resources, or external relationships
- Represents a significant threat to other organizations, local communities, or the nation
- Disrupts core IT services, leading to a notable cessation of business or academic services

3.4. Chancellor

The CTO will be in direct contact with the Chancellor to determine if/when the CU President and Board of Regents need to be informed about an incident. The Chancellor may also need to assign and approve resources.

3.5. All Organizational Unit Heads

Organizational Unit (OU) Heads are responsible for:

- Having a written computer incident response plan (IRP) for their unit
- Designating an alternate to cover the OU Head role
- Ensuring their employees read and understand the IRP and know how to recognize and report a computer security incident to their supervisor who will report to the OU Head
- **Leaving the computer on/running and untouched after discovery of a suspected incident**
- Removing the computer from the network
- Reporting the incident to the UCCS IT Security Principal (ITSP)
- Assisting the CIRT in investigating and resolving the incident
- Making any business process or technology changes necessary to prevent further incidents.

3.6. University Relations

University Relations (UR) will be the only organization allowed to speak to the media! They will need to be in direct contact with the CTO, with the Chancellor and with Legal Counsel to be aware of the details as they change throughout the incident response process. UR will also create any notices that go to the public or to any individuals whose data was compromised.

4. Reporting Incidents

Computer Security Incidents are highly volatile topics and need to be communicated very carefully to avoid spreading false or misleading information. The facts must be known, and proper approvals must be given before any information about a security incident is released to anyone other than **on a need-to-know basis**. The proper lines of communication are briefly described here, and can be seen in the Computer Security Incident Communications Chart below.

4.1 Reporting To the Information Technology Security Principal (ITSP)

All suspected computer security incidents are to be reported immediately to the UCCS IT Security Principal at 719-262-3211, on campus x3211. Please see the UCCS document “Incident Reporting Guidelines” for more details.

4.2 Reporting To CU Office of Information Security (OIS)

The CU Office of Information Security handles the official communications to the rest of CU. They (usually the Information Security Officer – ISO) communicate directly with the UCCS ITSP at regular intervals and are the ones who report the incident to the CU Chief Privacy Officer, and to the State of Colorado.

For full details on reporting to the OIS, see the “CU Incident Reporting Guidelines.”

4.3 Reporting To CU President and Board of Regents

Only upon the Chancellor’s approval, after we are almost completely certain that a breach has occurred, will the CU President and CU Board of Regents be notified. **The Office of Information Security is the only organization allowed to initially notify the President or Board of Regents** about a security incident.

4.4 Reporting To Compromised Individuals

By law, certain computer security incidents must be reported to the individuals whose private data was compromised. Legal Counsel determines when this needs to be done, the Chancellor gives the approval, and University Relations crafts the notice.

4.5 Reporting To Other Supporting Organizations

Public Safety, External IT Service Providers, CU Treasury Office, the Federal Trade Commission (FTC), etc. may need to be called depending on the circumstances of the incident. The contact information for these organizations can be found in the IT Emergency Plan, in the “UCCS Computer Security Incidence Response Procedure,” and in departmental incident response plans.

4.6 Reporting Credit Card Data Incidents

If credit card data may possibly have been comprised in an incident, **the CU Treasurer’s Office** must be contacted immediately at: **303-837-2183** or **303-837-2182**

5. Six-Phase Incident Response Process *(adapted from FCC, NIS and SANS processes)*

Once a suspected computer security incident is discovered, the incident response process will follow six stages of response when anticipating and servicing a computer security incident. The flowchart below illustrates the incident response process flow.

5.1. Report

See “Section 4: Reporting of Incidents” in this document.

5.2. Identify and Declare

The Computer Incident Response Team will identify the suspected incident’s symptoms, and determine its type, severity, mechanism, impact and what data was affected. If it truly is a computer security incident, the IT Security Principal will declare it as an official incident.

5.3. Contain

The CIRT will decide if they need to pursue the perpetrator of the attack or protect the system(s) immediately. This will determine whether the system(s) will be isolated from the network to keep other systems from being affected, or if it will be allowed to operate in order to collect evidence against the attacker. Containment may mean shutting down other systems temporarily.

5.4. Eradicate

Eradication of the system usually involves cleaning and rebuilding affected systems, and possibly restoring from backups.

5.5. Recover and Return to Normal Operations

The Computer Security Incident Response Team will work with the OU Head and/or the OU System Administrator to bring affected systems back on-line and functioning normally as soon as possible. Potential issues involved in determining when operation can return to normal are:

- Number and type of systems affected
- Legal issues
- Confiscation of systems
- Forensic investigations
- Amount of time systems were down
- Cleaning of systems
- Cost
- Personnel issues

5.6. Follow-up

This involves documenting the incident for the Office of Information Security and the CCHE and possibly other governmental organization, debriefing with organizations involved, filing any work orders to correct any processes or technology to prevent similar attacks in the future.

UCCS Computer Incident Response Process

