University of Colorado
Colorado Springs

UCCS CAMPUS POLICY

Policy Title: Information Security Incident Response

Policy Number: 700-005 **Policy Functional Area: Information Technology**

Effective:	May 6, 2024
Approved by:	Jennifer Sobanet, Chancellor
Responsible Vice Chancellor:	Vice Chancellor of Administration and Finance (VCAF)
Office of Primary Responsibility:	Chief of Information Technology (CIO)
Policy Primary Contact:	CIO, security@uccs.edu
Supersedes:	October 16, 2008; August 5, 2016
Last Reviewed/Updated:	May 6, 2024
Applies to:	Administration, Faculty, Staff, Students and Vendors

Reason for Policy: This policy establishes an Information Security Plan and identifies formal IT security management and governance procedures for UCCS.

I. INTRODUCTION

This policy establishes an Information Security Incident Response Plan and Procedures and identifies formal Information Systems security management and governance procedures for the UCCS campus.

II. POLICY STATEMENT

The Information Security Incident Response Policy defines the methods for reporting an Information Security Incident and is also used as the OIT Security Incident Response Plan.

A. Purpose

The purpose of an Information Security Incident Response Plan is to provide the University with a plan that outlines how UCCS will respond in the event of an information security incident. An information security incident is a compromising event that disrupts the confidentiality, integrity, or availability of university-owned information systems, regardless of ownership or location, used to store, process, transmit, or access UCCS Data as well as all personnel including employees, students, temporary workers, contractors, those employed by contracted entities, and others authorized to access UCCS enterprise assets and information resources.

B. Roles and Responsibilities

1. The Office of Information Technology (OIT) shall maintain an Information Security Incident Response Plan for the protection of data at UCCS.

2. The Information Security Office shall review and revise the plan annually or as needed due to changes in the industry. These reviews shall be fully documented. Risk assessments will also be conducted annually or as needed to identify any potential risk and harm that could result from a security incident.

3. All UCCS staff, faculty, students, contractors, affiliates, and community members utilizing University IT resources are responsible for reporting any suspected incidents to the Information Security Officer at security@uccs.edu.

4. The Information Security Incident Response Team (ISIRT)

   a. Incident Response Officer – The campus Information Security Officer or designated alternate.
   b. Incident Response Analyst(s) – The Information Security Analyst or designated alternate.
   c. System Administrator(s) – Designated SysAdmin member(s) selected to assist in the incident response.
   d. Forensic Analyst (if applicable) – Designated Forensic Analyst to assist in artifact gathering.
   e. Ad-hoc members of the campus community such as HIPAA privacy officers, FERPA officials, etc. as needed.

5. Responsibilities of the ISIRT

   a. The ISIRT investigates security events to determine whether an incident has occurred, and then the extent, cause, and damage of the reported incident(s).
   b. The ISIRT directs the recovery, containment and remediation of security incidents and may authorize and expedite changes to information systems necessary to do so. The ISIRT coordinates response with external parties when existing agreements place responsibility for incident investigations on the external party. An after-action report will be created by the Information Security Officer (ISO) and disseminated to the appropriate leadership across campus and the CU System if deemed appropriate.
   c. During the conduct of security investigations, the ISIRT is authorized to monitor relevant UCCS IT resources and retrieve communications and other relevant records of specific users of UCCS, including login session data and the content of individual communications without notice or further approval and in compliance with APS 6005.
   d. Any external disclosure of information regarding information security incidents must be reviewed and approved by the ISO or CIO in consultation with the Compliance Office, Office of University Counsel, University Communications, and other university stakeholders as appropriate.
   e. The ISIRT coordinates with law enforcement, government agencies, peer ISIRTs and relevant Information Sharing and Analysis Centers (ISACs) in the identification and investigation of security incidents. The ISIRT is authorized to share external threat and incident information with these organizations that do not identify any member of UCCS or otherwise reveal any proprietary or protected university information.

III. DEFINITIONS

IT Resources: Technology including but not limited to data, computer hardware, computer software, networks owned or operated by the University of Colorado.

Incident: A compromising event that disrupts the confidentiality, integrity, or availability of university-owned information systems, regardless of ownership or location, used to store, process, transmit, or access UCCS Data as well as all personnel including employees, students, temporary workers, contractors, those employed by contracted entities, and others authorized to access UCCS enterprise assets and information resources.

Information System: A major application or general support system for storing, processing, or transmitting University Information. An Information System may contain multiple subsystems. Subsystems typically fall under the same management authority as the parent Information System. Additionally, an Information System and its constituent subsystems generally have the same function or mission objective, essentially the same operating characteristics, the same security needs, and reside in the same general operating environment.

Information Security Officer: The University's Information Security Office, responsible for coordinating the development and dissemination of information security policies, standards, and guidelines for the University.

IV. RELATED POLICIES AND OTHER RESOURCES

A. Administrative Policy Statements (APS) and Other Policies
   1. APS 6005, updated October 1, 2023
   2. UCCS Policy 700-003, Information Technology Security

B. Other Resources
   1. Detailed documentation of the Information Security Program files will be maintained online at the UCCS Information Technology, Information Security website.

V. HISTORY

Initial policy approved:	October 16, 2008
Revised:	August 5, 2016
Revised:	May 6, 2024