UCCS CAMPUS POLICY

Policy Title: Computer Security Incident Response

Policy Number: 700-005
Policy Functional Area: INFORMATION TECHNOLOGY

Effective: August 5, 2016
Approved by: Pam Shockley-Zalabak, Chancellor
Responsible Vice Chancellor: Chancellor
Office of Primary Responsibility: Chief of Information Technology (CIO)
Policy Primary Contact: CIO, 719-255-3419
Supersedes: October 16, 2008
Last Reviewed/Updated: May 20, 2016
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 Plan and identifies formal IT security management and governance procedures for UCCS.

II. POLICY STATEMENT

A. 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.

B. 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.
C. PROCEDURES

1. The Information Technology Department shall maintain an Information Security Program Computer Security Incident Response for the protection of information at UCCS. The Information Security Program includes:
   
a. Periodic assessments of the risk and magnitude of the harm that could result from a security incident.
   
b. A Process for providing adequate Information Security for the communication of information resources.
   
c. Information Security awareness training.
   
d. Periodic testing and evaluation of the effectiveness of Information Security.
   
e. A process for detecting, reporting and responding to security incidents.
   
f. Plans and procedures to ensure the continuity of IT operations in the event of a security incident.

2. The Information Technology Department shall review and revise the plan annually or as needed due to changes in the industry.

3. 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.

III. DEFINITIONS

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

IV. RELATED POLICIES, PROCEDURES, FORMS, GUIDELINES, AND OTHER RESOURCES

A. Administrative Policy Statements (APS) and Other Policies

B. Procedures

C. Forms

D. Guidelines

Other Resources: Detailed documentation of the Information Security Program files will be maintained online at the UCCS Information Technology, Information Security website: https://www.uccs.edu/it/security.html.

E. Frequently Asked Questions (FAQs)
V. HISTORY

Initial policy approved October 16, 2008