Security Incident Response

I. INTRODUCTION

This policy sets expectations for responding to security incidents at the University of Denver (the University), including defining the roles and responsibilities of participants, the overall characterization of incident response, relationships to other policies and procedures, and guidelines for reporting requirements.

II. POLICY OVERVIEW

This policy establishes the authority, roles, and responsibilities for managing and handling incidents. Furthermore, it requires a comprehensive plan for a quick and orderly response to computer-related security incidents.

III. POLICY PROCESS

A. Expectations

1. The University will establish and maintain a Security Incident Response Plan (SIRP) to manage information security incidents effectively.
2. The University will establish and maintain a security incident response team (SIRT) responsible for quick and orderly responses to information security incidents.
3. Information on security incidents will be classified as confidential. *See IT 13.10.051 Data Classification Policy.*
4. The incident response plan must be reviewed at least annually.
5. In preparation for security incidents, the SIRT, IT, and other business stakeholders will train and refine their ability to handle computer security incidents at least annually.

B. Roles and Responsibilities

1. All employees are responsible for reporting known or suspected information security events to their supervisor, unit leadership, or the University's Information Security Office.

2. The Chief Information Security Office (CISO) shall have overall authority and responsibility for the security incident response plan and activities, including:
   a. Coordinating efforts to manage an information security incident.
   b. Identifying and constituting a security incident response team.
   c. Ensuring the prompt investigation of a security incident.
   d. Determining what University data may have been exposed.
   e. Securing any compromised systems to prevent further damage.
   f. Authorizing the use of University resources to manage and address security incidents.

3. Executive Response Team
   The Executive Response Team (ERT) consists of University Officials with the authority to make key decisions in managing an incident related to confidential or restricted data. The ERT shall be comprised of the following standing members:
   a. CISO
   b. CIO

c. General Counsel
d. A representative from the Office of the Chancellor
e. University Communications
f. Enterprise Risk Management
g. Dean, Director, or Department Head of the area where the exposure is determined to have occurred

4. Incident Response Coordinator
   Throughout the course of the incident, the Incident Response Coordinator is responsible for:
   a. Directing efforts to gather appropriate information
   b. Providing expertise in the procedural aspect of gathering information and documentation of process
   c. Updating CISO and other leadership as necessary

5. Incident Response Handler
   Throughout the course of the incident, Incident Response Handlers are responsible for:
   a. Gathering data from systems
   b. Providing specific expertise in technology and data
   c. Entering appropriate data for Incident Management, including procedural information

IV. DEFINITIONS

- **Security Event** – An event is an exception to the normal operation of IT infrastructure, systems, or services. Events may be identified through automated systems; reported violations to the ISO, Compliance/Privacy, or other university departments; or during normal system reviews, including system degradation/outage. It is important to note that not all events become incidents
- **Security Incident** – Any real or suspected event that may adversely affect the security of the University's information or the systems that process, store, or transmit that information.