CAMERON UNIVERSITY
Information Security Incident Response Policy

Policy Statement

This policy describes the procedures to be followed when an information security incident is discovered to have occurred involving an Academic or Administrative Computing System operated by Cameron University and its faculty, students and employees. This policy outlines the procedures for decision-making regarding emergency actions taken for the protection of Cameron University's information resources from accidental or intentional unauthorized access, disclosure or damage.

Contents

Who Should Know This Policy

President
Vice Presidents
Deans
Department Chairs
Directors
Faculty
Other Accounting/Finance Personnel
Students
Other Groups
All Employees

Responsibilities

Responsible for Policy
University Officer Responsible — Vice President for Academic Affairs

Procedure

STATEMENT OF PURPOSE: In support of the above policy statement, the following procedures and information are provided:

1.0 Notification

1.1 Information Security Incident—an information security incident is defined as any real or suspected adverse event in relation to the security of computer systems or computer networks. Examples of incidents include activities such as:

- Attempts (either failed or successful) to gain unauthorized access to a system or its data
- Unwanted disruption or denial of service
- The unauthorized use of a system for the processing or storage of data
- Unauthorized changes to system hardware, software, data, or networks

1.2 Administrative Computing System—any application or information system that directly or indirectly deals with or supports financial, administrative, or other information that is an integral part of running the business of the university.

1.3 Academic Computing System—any application or information system that directly or indirectly deals with or supports the University's primary mission of teaching, learning and research.

2.0 General Guidelines

2.1 The purpose of information security incident response is to mitigate the effects caused by such an incident and to protect the information resources of the University from future unauthorized access, use or damage. Such procedures include:

a. Ensuring that the appropriate level of the University's management becomes involved in the determination of actions to be taken in response to an information technology security incident

2.1 A standard, University-wide approach to information security events is important because of the following factors:

a. The need to promptly and effectively address any improper access of University information systems or the data contained therein
b. Legal and regulatory requirements regarding the safeguarding of University information assets
c. The University's implementation and reliance on University-wide information systems
d. Intellectual capital that Cameron University both produces and owns needs to be protected against premature disclosure or unauthorized tampering
e. Damage to Cameron University's reputation can have both direct and indirect negative effects
f. A general worldwide increase in the number and severity of computer security incidents
g. The need to protect the privacy of persons whose information is stored on University information systems

3.0 Notification

A member of the University community who becomes aware of an information security incident involving an Academic or Administrative Computing System should immediately contact the University's Information Security Officer at (580) 581-6735.

The University's Information Security Officer may convene a preliminary fact-finding working group comprised of appropriate Cameron University Business Office and technical personnel and, when appropriate the Office of Legal Counsel (such as instances where legal requirements are implicated, e.g., where private data of individuals is compromised). In all cases, an incident summary will be provided to the Vice President for Academic Affairs.

4.0 Information Security Incident Response Team

When warranted by information obtained during preliminary fact-finding, the University's Information Security Officer will promptly appoint and convene a meeting of an Information Security Incident Response Team (ISIRT). The membership of the ISIRT will be selected by the Information Security Officer in order to have appropriate breadth and depth of expertise.

5.0 Escalation of Decision-Making

The ISIRT will plan and coordinate the activities of all the areas involved, keeping other concerned areas advised as appropriate. In carrying out this responsibility, the ISIRT will ensure that important operational decisions are elevated to the appropriate levels to protect the fundamental interests of the University and others impacted by the incident. Such decisions include, but are not limited to:

- Restricting information system access or operations to protect against unauthorized information disclosures
- Reporting and/or publicizing unauthorized information disclosures, as required by law
- Involving law enforcement agencies in cases where applicable statutes appear to have been violated
- Reporting this incident to the Oklahoma Computer Crimes Alliance (OCCA), following the procedures provided in the current state policy—see Appendix E: Revision 1. Computer (Cyber) Incident Reporting Procedures on page 70 in the Appendix of the statewide Information Security Policy, Procedures, and Guidelines document which can be found at: https://oklahoma.gov/content/dam/ok/en/omes/documents/InfoSecPPG.pdf.
- The Information Security Officer will also be responsible for documenting the deliberations and decisions of the ISIRT as well as all actions taken pursuant to ISIRT deliberations.

6.0 Report Preparation

The Information Security Officer, jointly with the Internal Audit Department, will be responsible for writing and submitting a final report to the appropriate University office(s). The report will summarize findings regarding the information security incident and, if appropriate, include recommendations for improvement of related information security practices and controls.

7.0 Sources of More Information

Section 298 - [HB 2357] - An Act relating to technology; requiring governmental agencies to notify persons of a breach of computer systems which results in unauthorized release of personal information: https://www.oscn.net/applications/oscn/DeliverDocument.asp?CiteID=446247.

State of Oklahoma Information Security Policy outlining the prudent IT procedures and practices: https://oklahoma.gov/content/dam/ok/en/omes/documents/InfoSecPPG.pdf.

Contacts

Policy Questions: Information Security Officer, (580) 581-6735

Forms

In support of this policy, the following forms are included:

None

Policy History

Policy

Issue Date:	April 25, 2012
Reviewed, no revision:	February 2016
Reviewed, no revision:	June 6, 2023