Procedure III.3010.A.c, Cybersecurity Incident Response

Associated Policy
Policy III.3010.A, Information Resources

1. Purpose

The Incident Response Procedure (IRP) serves as the foundation for the College's response to cybersecurity incidents. Specifically, this Procedure grants the College's Chief Information Security Officer (CISO) the authority to appoint a Cyber Incident Response Team (CIRT) in response to actual or suspected information privacy or security event/incidents. The CIRT then has authority to investigate, respond, mitigate, and report such incidents as required by Federal and State Laws.

2. Applicability

This Procedure applies to all College Information Resources and the Users of such Information Resources, in any form, and is intended to be broad enough to include all Users.

3. Laws, Regulations, and Standards

The College is required to comply with Federal and State Laws and Regulations. Specifically, the College's Incident Response Procedure is required by Texas Government Code 2054.518, Texas Government Code 2054.603, TAC 202.76, and Texas DIR Security Controls Standard Catalog.

4. Associated Program Controls

The following Program Controls associated with this Procedure are:

IR Incident Response Control Family
- IR-1 Incident Response | Policy and Procedures
- IR-2 Incident Response Training
- IR-3 Incident Response Testing
- IR-4 Incident Handling
- IR-5 Incident Monitoring
- IR-6 Incident Reporting
- IR-7 Incident Response Assistance
- IR-8 Incident Response Plan
- IR-9 Information Spillage Response

5. Roles and Responsibilities

The roles and responsibilities as defined by the Information Security Program are described in Procedure III.3010.A.a, Information Security Program. Described below are additional roles and responsibilities that pertain to this Procedure.

a. **Cyber Incident Response Team (CIRT).** This is a temporary cross-functional team appointed and led by the CISO. The creation of this team is required by Texas State Law and is described in Texas DIR Incident Response Team Redbook. The CIRT is responsible for responding to security breaches, viruses, and other discovered or suspected security incidents at the College.

b. **College User(s)** is an individual, automated application, or process that is authorized by the College to access an Information Resource. Includes, but is not limited to, all College students, faculty, staff, contractors, guests, departments, and any individual, application, or process that accesses and or uses the College's Information Resources.

6. College Incident Response Team Redbook

The College's Incident Response Team Redbook describes:

- The membership, roles, and responsibilities of the CIRT, and the activities required when responding to actual or suspected information privacy or security event/incidents.
- The trigger events and process for activating a CIRT to respond to an actual or suspected event/incident. Once activated, the CIRT has the authority to request cooperation/establish event response priorities which may supersede daily business responsibilities or require attention outside normal business hours.

Resolution of a security event/incident is determined upon review by the CISO to ensure all appropriate steps were accomplished. Practices and playbooks will be created as needed within each step of the incident response process.

7. Reporting

The following mandatory reports are required as defined in the Texas DIR Security Controls Standard Catalog (DIR CC):

a. **Urgent Incident Report.** Each State institution of higher education shall assess the significance of a security incident based on the business impact on the affected resources and the potential technical effect of the incident. Confirmed or suspected security incidents shall be reported to the DIR not later than 48 hours of discovery as required by Texas SB 271. No later than 10 business days after incident eradication, closure, and recovery the state agency shall report to DIR, including the state agency CISO, the details and root cause of the incident as required by Texas SB 271. The College's Office of Cybersecurity (OCS) also has the authority to require that incident reporting requirements be included in any contract where such reporting may be necessary.

b. **Additional Reporting.** Further reporting actions may be required by Texas Government Code.

8. Definitions

The terms referenced in this Procedure are outlined in **Procedure III.3010.A.a, Information Security Program,** Section 14. Definitions**.**

Note: See **Procedure III.3010.A.b, Cybersecurity Risk Management** for additional information on cybersecurity.

Date of SLT Approval	February 15, 2024
Effective Date	February 15, 2024
Associated Policy	Policy III.3010.A, Information Resources
Primary Owner of Policy Associated with the Procedure	Chief Technology Innovations Officer
Secondary Owner of Policy Associated with the Procedure	Chief Information Security Officer