Information Security Incident Response and Reporting

Original Implementation: July 24, 2018
Last Revision: None

This policy governs the actions required for reporting or responding to information security incidents involving Stephen F. Austin State University (SFA) information and/or information technology resources to ensure effective and consistent reporting and handling of such events.

Scope
This policy applies to all who are granted access to SFA information resources, including, but not limited to, faculty, staff, students, alumni, vendors, contractors and visitors.

Definitions
Chief Information Security Officer (CISO) **-** Staff member responsible for providing and administering the overall information security program for the university.

Data Custodian – An SFA employee who is responsible for day-to-day maintenance of SFA Information Resources. In some instances this may be assigned to a third-party vendor.

Data Owner – The manager or agent responsible for the business function supported by the information resource or the individual upon whom the responsibility rests for carrying out the program using the information resource.

Incident Response Team (IRT) – The group of individuals who determine if a security incident is reportable to state authorities. The members include the chief information officer (CIO), chief information security officer (CISO), general counsel, and the chief audit executive. Other individual(s) may be included as the IRT deems necessary. A team member may assign a designee to serve on the IRT.

Information Resources - The procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information. This may include, but not limited to, any and all computer printouts, online display devices, mass storage media, and all computer-related activities involving any device capable of receiving email, browsing websites, or otherwise capable of receiving, storing, managing, or transmitting data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, mobile devices, pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (e.g., embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and hosted services.

Information Security Administrator (ISA) - A staff member who, in close cooperation with the information security office, provides assistance with the implementation and administration of information security initiatives and data owner security needs.

Information Security Incident – An event which results in unauthorized access, loss, disclosure, modification, disruption or destruction of information resources, whether accidental or deliberate.

Response Planning Team (RPT) - The group that plans and implements notification of affected individuals when an information security incident occurs. Members include the CIO, CISO, chief audit executive, general counsel, and other individual(s) the RPT deems necessary. A team member may assign a designee to serve on the RPT.

Responsibilities

Data Owner

- Participates in the IRT

Chief Audit Executive

- Participates in the IRT
- Participates in the RPT

Executive Director, University Marketing and Communications

- Participates in the RPT

Chief Information Officer

- Participates in the IRT
- Participates in the RPT

Chief Information Security Officer

- Participates in the IRT
- Participates in the RPT

General Counsel

- Participates in the IRT
- Participates in the RPT

Incident Response Team

- Determines when a reportable incident has occurred, and determines individuals involved and who should be notified.
- Determines course of action in response to an information security incident.
- A designee of the IRT will notify the appropriate division head of the information security incident.

Response Planning Team

- Plans and implements notifications when an incident has occurred, including what information is provided and how the incident will be communicated.
- Drafts pertinent communications to affected individuals.

Procedures

Information Security Incident Monitoring

The CISO will aggregate information security incident data and share it on a regular basis with SFA's executive oversight compliance committee and CIO. If criminal activity is suspected, the CISO will notify the University Police Department. This data may include number and type(s) of security incidents and other information.

Reporting Security Incidents

Any member of the SFA community who suspects the occurrence of a security incident must report incidents through the following channels:

1. All suspected information security events must be reported directly to the CISO or information security office as quickly as possible by phone, e-mail, or in person. If the CISO or a representative of the information security office cannot be reached, the CIO must be contacted.
2. For suspected security incidents occurring in areas with departmental IT support, suspected incidents must also be reported to the departmental IT support staff or ISA.
3. Any attempt to interfere with, prevent, obstruct, retaliate for or dissuade the reporting of an information security incident, critical security concern, policy violation, or information resource vulnerability is strictly prohibited and may be cause for disciplinary action.

Information Security Incident Investigation and Identification

1. Upon notification of a potential information security incident, the CISO shall promptly assess and gather information to determine the impacted data, systems and business processes. When applicable, the data owner will be required to complete and submit a statement describing the stored or processed data and submit it to the CISO. The CISO may also require copies of files.
2. The IRT will determine whether an actual information security incident has occurred and provide input on whether the incident warrants notification to affected individuals**.**
3. If a security incident is confirmed, the following individuals shall be notified: unit or department head, and dean (if in an academic area).

Information Security Incident Containment

1. In some cases, action will be necessary to limit the magnitude and scope of the information security incident.
2. Should any action be necessary which has a likelihood of having a substantial impact on business processes, the unit or department head or data owner, CIO and data custodians will be notified in advance.
3. Reasonable efforts will be made by Information Technology Services to minimize the impact.
4. In rare cases it may be necessary to take action without receiving input from individuals who manage the affected information resources.

Information Security Incident Responsive Actions

1. The affected unit is responsible for taking action to identify and either eliminate or mitigate the vulnerabilities resulting in the security incident.
2. The CISO will provide recommendations to the affected unit and coordinate any remaining efforts needed to eliminate or mitigate the vulnerabilities.

Information Security Incident Notification

1. The CISO will notify state and federal entities as required by law.
2. If a decision has been made to notify individuals affected by the information security incident, the RPT will develop and implement a data breach notification process.
3. Individuals will be notified as expediently as possible without unreasonable delay. Note that the creation and dissemination of the communications may be assigned outside of the RPT.
4. Any media inquiries regarding the information security incident are to be directed to the executive director, University Marketing and Communications.

Information Security Incident Follow-up

1. The CISO will develop a security incident report summarizing the information security incident and outlining recommended actions.
2. The security incident report will be amended to include the responsible unit head's action plan and action plan progress and will be shared with the RPT.

Compliance

All users of SFA information technology resources are required to comply with this policy. SFA reserves the right to deny, limit, restrict, or extend privileges and access to its information technology accounts and systems.

Cross Reference: 1 Tex. Admin. Code Ch. 202; Information Security Management (14.1)

Responsible for Implementation: Chief Information Officer

Contact for Revision: Chief Information Security Officer

Forms: None

Board Committee Assignment: Academic and Student Affairs Committee