**Information Security Incident UPPS No. 04.01.10**

**Management Issue No. 3**

**Effective Date: 10/11/2023**

**Next Review Date: 09/01/2025 (E2Y)**

**Sr. Reviewer: Chief Information Security Officer**

**POLICY STATEMENT**

*Texas State University is committed to establishing and maintaining an effective security incident response program.*

**01. BACKGROUND INFORMATION**

01.01 The Chief Information Security Officer (CISO) is charged with establishing and maintaining an effective security incident response program to ensure that:

a. security events are thoroughly investigated and documented;

b. immediate damage is minimized, latent risks are identified, and subsequent exposures are mitigated;

c. incident reporting and notification are timely and legally compliant; and

d. remedial actions are taken to prevent recurrence (see [TAC 202.70](http://texreg.sos.state.tx.us/public/readtac%24ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=70), [TAC 202.73](http://texreg.sos.state.tx.us/public/readtac%24ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=73), and [NIST SP 800-53 IR](https://dir.texas.gov/sites/default/files/2023-05/Security%20Control%20Standards%20Catalog%20Version%202.1.pdf)).

**02. DEFINITIONS**

02.01 Event – an observable or suspected deviation from the expected operations of information resources. While all incidents stem from events, not all events are considered incidents. Events may also include observations of actions, procedures, or statuses of information resources that are determined to be an imminent threat to the confidentiality, integrity, or availability of information resources.

02.02 Incident – an event that, as determined by the CISO, or designee, meets or is reasonably expected to meet one or more of the criteria below:

1. violates [UPPS No. 04.01.05](https://policies.txstate.edu/university-policies/04-01-05.html), Network Use Policy; [UPPS No. 04.01.07](https://policies.txstate.edu/university-policies/04-01-07.html), Appropriate Use of Information Resources; other applicable Texas State University policies, procedures, and ethical codes; or [The Texas State University System (TSUS) Rules and Regulations](https://www.tsus.edu/about-tsus/policies.html);
2. directly or indirectly compromises the confidentiality, integrity, or availability of information resources;
3. creates the potential for harm or compromise that arises as a result of security risks from suppliers, their supply chains, and their products or services; or
4. presents an impending or incipient threat to the confidentiality, integrity, or availability of information resources or the reputational standing of the university or other relevant stakeholders.

02.03 Incident Classification – the severity of each incident is classified based on the overall impact it had or is expected to have on the institution.

Throughout the incident investigation and response process, the classification of an incident could be adjusted, depending on the context of the incident and emergence of new information.

Some incidents will not require a formalized assessment or response from the CISO; such events typically involve temporary losses of availability caused by natural disasters, power outages, or interruption of upstream services provided by external third parties.

The institutional impact of an incident may be classified as low, moderate, or high, as defined below:

1. Low-Impact Incidents – common occurrences that happen regularly and are treated as a cost of doing business. The occurrence of low-impact incidents is almost a statistical certainty over a long enough time span. These incidents have standard, operationalized responses, and do not have severe consequences that affect the continuation of operations. Examples of low-impact incidents include phishing and infection or compromise of non-critical systems such as individual workstations.
2. Moderate-Impact Incidents – may affect the confidentiality, integrity, or availability of limited amounts of information resources, including sensitive or confidential information.
This is intentionally a broad category, as most incidents that do not have operationalized responses and do not meet the definition of low-impact incidents are considered moderate-impact incidents. Moderate-impact incidents may also include an anomalous collection or pattern of related, low-impact incidents, such as a targeted spear-phishing campaign or malware that exploits an unpatched vulnerability.
3. High-Impact Incidents – affect the confidentiality, integrity, or availability of a large amount of sensitive or confidential information, or have direct, long-lasting effects to core infrastructure systems, services, or other high-value, business-critical information resources. High-impact incidents are a rare occurrence.

**03. INFORMATION SECURITY INCIDENT RESPONSE PROCEDURES**

03.01 While specific and technical methods and response measures will vary depending on the details and context of any given incident, general response procedures may be defined based on the classification of each incident, as defined in Section 02.03.

03.02 Information Security incident response will be managed by the CISO, or designee, and will involve at a minimum, Information Security staff and the owners and custodians of the compromised information resources.

03.03 Response to Low-Impact Incidents – Low-impact incidents do not necessitate major, individualized responses and are tracked and reported as required. Operationalized responses to low-impact incidents are frequently delegated to authorized information custodians as part of routine operations.

Required parties include: the CISO, or designee, and the custodian of the affected information resource.

Optional or recommended parties include: the owner of the affected information resource, and depending on context, a member of the Information Technology Assistance Center (ITAC).

03.04 Response to Moderate-Impact Incidents – Each moderate-impact incident requires assessment by the CISO, or designee, which may then result in a response of commensurate scope and scale.

 Required parties include: the CISO, or designee, and the custodian and the owner of the affected information resource.

Optional or recommended parties include: the vice president for Information Technology (IT), who also serves as the information resource manager (IRM), or designee, leadership within the affected department, unit, or division, or individuals from the Division of IT who may share in technical custodianship of the affected information resource.

03.05 Response to High-Impact Incidents – High-impact incidents result in a response commensurate to the scope, scale, and context of the incident.

Required parties include: the CISO, or designee, and the custodian and owner of the affected information resources

Optional or recommended parties include: the IRM, or designee, leadership within the affected department, unit, or division, individuals from the Division of IT who may share in technical custodianship of the affected information resource, the TSUS associate general counsel, and the director of Media Relations.

03.06 Involvement of Law Enforcement Officials – If at any time the CISO, or designee, has reasonable suspicion that reportable criminal activity has occurred, appropriate law enforcement officials shall be notified in a timely fashion. As outlined in their official duties, the CISO, or designee, shall act as a liaison between the university and external law enforcement agencies.

**04. NOTIFICATION AND REPORTING REQUIREMENTS**

04.01 Owners, custodians, and users must immediately report suspected information resources security incidents or data breaches to ITAC at 512.245.4822, itac@txstate.edu; or Information Security at 512.245.4225, infosecurity@txstate.edu. Once the report is submitted, IT staff shall follow the Incident Management and Reporting Procedures found on the [Information Security website](http://infosecurity.txstate.edu/).

04.02 The CISO, or designee, shall fully document each moderate- and high-impact incident, the investigation itself, and the results of the investigation. A draft incident report will be prepared and shared internally with the appropriate university stakeholders, selected at the discretion of the CISO or IRM. In addition to the individuals listed in Section 03., such stakeholders may also include some or all of the following: the IRM, the university president, the owners and custodians of the compromised resources, their respective vice presidents, the TSUS associate general counsel, and the director of Audits and Analysis.

The draft report’s completeness and accuracy will be reviewed in a meeting of the report recipients and modifications noted in that meeting.

A final report will be released to necessary recipients following the review meeting. If required, the results will be included in the CISO’s, or designee’s, reports to the Department of Information Resources (DIR).

04.03 The CISO, or designee, shall report certain urgent incidents, as defined in [TAC 202.73](http://texreg.sos.state.tx.us/public/readtac%24ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=73), to the DIR within 48 hours (and to other entities as may be appropriate to the incident) if the initial incident investigation reveals a critical threat that might propagate beyond the confines of the campus network and threaten other networks. The CISO, or designee, shall track and regularly report low-impact incidents to the DIR as required (see [TAC 202.73](http://texreg.sos.state.tx.us/public/readtac%24ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=73)).

 If an information security incident is required to be reported to the DIR under [Texas Government Code Sec. 2054.1125](https://statutes.capitol.texas.gov/SOTWDocs/GV/htm/GV.2054.htm) or the “Urgent Incident Report” rules per [Texas Administrative Code 202.73(b)](https://texreg.sos.state.tx.us/public/readtac%24ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=73), the established event reporting and escalation procedures shall also require notification to TSUS administration via the vice chancellor for Finance and the director of Audits and Analysis in a similar reporting manner and timeline.

04.04 If criminal activity is suspected, the CISO, or designee, shall immediately contact the appropriate law enforcement and investigative authorities (see [TAC 202.73](http://texreg.sos.state.tx.us/public/readtac%24ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=73)).

04.05 In cases where additional reporting or notification is required by law, such as the cases described in [Texas Business and Commerce Code, Chapter 521](https://statutes.capitol.texas.gov/Docs/BC/htm/BC.521.htm), the IRM, CISO, or designees, shall engage appropriate university staff to ensure compliance with such requirements. Such engagement should be conducted under advisement of the TSUS Office of General Counsel.

**05. REVIEWERS OF THIS UPPS**

05.01 Reviewers of this UPPS include the following:

 Position Date

Chief Information Security Officer Sept 1 E2Y

Associate Vice President for Sept 1 E2Y

Technology Resources

Vice President for Information Sept 1 E2Y

Technology

**06. CERTIFICATION STATEMENT**

This UPPS has been approved by the following individuals in their official capacities and represents Texas State policy and procedure from the date of this document until superseded.

Chief Information Security Officer; senior reviewer of this UPPS

Vice President for Information Technology

President