



SPACE INSTITUTE

UT Space Institute IT Procedure: Incident Response Management	
Version: 1	Effective Date: 10/01/2025

Purpose

To develop and maintain a thorough written incident response plan that includes a written process for users to report incidents and guidance for security issues.

Scope

This procedure applies to University owned or managed Assets, Systems, and Resources only. It does not apply to Assets, Systems, and Resources not owned by the University unless specifically stated in the policy.

Procedure

1. The CIO has overall responsibility of the Security Incident Reporting & Response (IR) program at UTSI and ensures:
 - a. The program is developed, documented, and disseminated to appropriate UTSI entities in accordance with University policy.
 - b. The program is reviewed and updated annually.
 - c. Consults with system owners to ensure effective procedures are implemented.
 - d. Ensures compliance to federal, state and university policy and regulations.
 - e. Develops, documents and maintains a campus-wide Cyber Incident Response Plan.
 - f. Monitors, tracks and reports, on a periodic basis, all Security Incidents to the UTSA CISO.
 - g. Ensures departments and users have assistance during recovery from Security Incidents.
 - h. Ensures potential forensic evidence is protected from corruption.
2. System owners/administrators are responsible for adhering to this program for their respective system(s).
3. All users are to report suspicious activity, compromised systems or accounts, or any potential security incidents to the IT Help Desk at (931) 393-7363 or helpdesk@utsi.edu.

Exceptions

Campus or institute CIOs/DTLs are authorized to grant exceptions to campus or institute processes and procedures.



SPACE INSTITUTE

UT Space Institute IT Procedure: Incident Response Management	
Version: 1	Effective Date: 10/01/2025

Related Policies

- [IT0001 – General Statement on Information Technology Policy](#)
- [IT0003 – Information Technology Security Program Strategy](#)
- [IT0004 – Information Technology Risk Management](#)
- [IT0005 – Data Categorization](#)
- [IT0002 – Acceptable Use of Information Technology Resources](#)
- [HR0580 – Code of Conduct](#)
- [IT0017 – Information Technology Incident Response Management](#)
- [IT0102 – Information Technology Asset Management](#)
- [IT0311 – Information Technology Data Access, Management, and Recovery](#)
- [IT0506 – Information Technology Account and Credential Management](#)
- [IT1318 – Information Technology Network Monitoring and Defense and Penetration Testing](#)
- [IT1516 – Information Technology Service Provider Management and Application Software Security Management](#)
- [IT4912 – Information Technology Secure Configuration Management](#)
- [IT7810 – Information Technology Vulnerability Management, Audit Log Management, and Malware Defense Policy](#)