



INCIDENT RESPONSE

POLICY

The Information Technology Security Incident Response Policy defines the responsibilities of Sherman College faculty and staff when responding to or reporting security incidents. It delineates roles within the Sherman Information Technology department and outlines which members of College administration should be involved in different types of security incidents.

Roles and Responsibilities

Director of Information Technology — The director of information technology is responsible for assessing the initial scope of a security incident, assembling the Incident Management Team, and appointing the incident manager.

Incident reporting — All members of the College community are required to report actual or suspected security incidents. All suspected technology security incidents should be reported to the Sherman Information Technology department at ext. 288 or help@sherman.edu.

Incident Manager — This role is designated by the director of information technology and will lead the response to the incident. This is a technical role and will coordinate the work of log collection, evidence preservation, and analysis activities.

Incident Management Team

When a breach of Category 1 data has been declared, the following College administration roles will be added to the incident response team:

- Senior administrator for impacted systems
- Director of Information Technology
- Executive Vice President
- Director of Marketing and Communications
- Campus Security and Safety Manager
- Others appointed as needed

The Incident Management Team will work with the director of marketing and communications to determine when and how to inform individuals outside the Incident Management Team regarding the incident.

Members of the Incident Management Team and all Information Technology staff shall receive annual incident response training.



INCIDENT RESPONSE

Incident Severity Levels

The incident response will be addressed based on the severity of the incident. Incident severity takes several factors into account: sensitivity of the data involved, number of end users impacted, and its overall impact on the ability of Sherman College to fulfill its mission. Incident severity also will be used to determine who manages an incident, who is informed about an incident, and the extent and immediacy of the response to the incident.

High

A security incident will be considered “high” if any of the following characteristics are present:

1. Threatens to impact (or does impact) systems critical to Sherman College’s ability to function normally. This includes but is not limited to: email, courseware, human resources, financials, internet connectivity, or portions of the campus network
2. Poses a serious threat of financial risk or legal liability
3. Threatens to expose (or does expose) Category 1 data as defined by Policy 3305 (Data Classification)
4. Threatens to propagate to or attack other networks, or organizations internal or external to Sherman College
5. Terroristic threats or other threats to human life or property when received by the Sherman Information Technology department

Medium

A security incident will be considered “medium” if any of the following characteristics are present:

1. Threatens to impact (or does impact) a significant number of systems or people. Sherman College can still function, but a group, department, unit, or building may be unable to perform its mission
2. Systems impacted contain only Category 2 and/or Category 3 data
3. Impacts a non-critical system or service



INCIDENT RESPONSE

Low

Low severity incidents have no characteristics from the “medium” or “high” categories and may include the following:

1. Only a small number of people or systems are impacted
2. Systems impacted contain only Category 3 data
3. Little to no risk of the incident spreading or impacting other organizations or networks

Incident Response Summary Table

The following table summarizes how Information Technology security incidents will be handled based on severity. It includes response times, who will manage each type of incident, and reporting requirements.

Incident Severity	Response Time	Incident Manager	Who to Notify	Incident Report Required?
High	Immediate	Information Technology Security Officer	Director of Information Technology Department Director Executive Vice President Director of Marketing and Communications Campus Security and Safety Manager Others on a need-to-know basis	Yes



INCIDENT RESPONSE

Incident Severity	Response Time	Incident Manager	Who to Notify	Incident Report Required?
Medium	4 hours	Information Technology Security Officer or Incident Response lead	Director of Information Technology Department Director Others on a need-to-know basis	If requested by Information Technology Security Officer, CIO, or other administrator
Low	Next business day	Incident Response lead	Director of Information Technology Department Director Others on a need-to-know basis	No

Exclusions or Special Circumstances

Exceptions to this Policy shall only be allowed if previously approved by the director of information technology and this approval is documented and verified.

Consequences

Use of College electronic information resources contrary to this policy or applicable federal, state or local law is prohibited and may subject the user to disciplinary action including, but not limited to, suspension of the user's access to the electronic information resources. Users also should be aware of other possible consequences under college policies and federal, state, or local laws, particularly those related to computer crime and copyright violation.