# IT 6823 LM 12. Incident Response and Recovery

# Learning Material

**Note**: The learning material is composed of a list of web links, videos, and other materials screened and/or created by the instructor. The material is organized by student outcomes. Essential information is included in this document and students are recommended to go to the links to learn more about a specific topic.

## Overview

The module gives an overview of incident response and recovery. The learning material is mainly based on NIST publication SP 800-61 Rev. 2 which provided in the D2L course website as a PDF file. The document is referred as “SP 800-61” in the rest of this document. SP 800-61 is available at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

Incident response and recovery is response phase in the NITS security framework.

## Student Learning Outcomes

* **Discuss the need for incident response**
* An event is any observable occurrence in a system or network.
* Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data
* A computer security incident is a violation or imminent threat of violation1 of computer security policies, acceptable use policies, or standard security practices.
* Needs of incident response – 1) supports responding to incidents systematically; 2) the ability to use information gained during incident handling to better prepare for handling future incidents and to provide stronger protection for systems and data; 3) comply with law, regulations, and policy.
* Source: page 6-7 of SP 800-61.
* **Describe the elements of incident response policy**
* Section 2.3 of the SP 800-61. Just focus on the elements of incident response plan and outside parties involved in the communications.
* Elements of the incident response plan:
	+ Mission
	+ Strategies and goals
	+ Senior management approval
	+ Organizational approach to incident response
	+ How the incident response team will communicate with the rest of the organization and with other organizations
	+ Metrics for measuring the incident response capability and its effectiveness
	+ Roadmap for maturing the incident response capability
	+ How the program fits into the overall organization.
* Communication with outside party



* **Discuss the incident response team structure**
* Section 2.4 of SP 800-61. Need to know the team models, team model selection consideration, and incident response team services, and recommendations of incident handling.
* Team models:
	+ Central Incident Response Team. A single incident response team handles incidents throughout the organization. This model is effective for small organizations and for organizations with minimal geographic diversity in terms of computing resources.
	+ Distributed Incident Response Teams. The organization has multiple incident response teams, each responsible for a particular logical or physical segment of the organization.
	+ Coordinating Team - An incident response team provides advice to other teams without having authority over those teams—for example, a departmentwide team may assist individual agencies’ teams
* Team model selection:
	+ The Need for 24/7 Availability
	+ Full-Time Versus Part-Time Team Members
	+ Employee Morale
	+ Cost
	+ Staff Expertise
* Team services
	+ Intrusion Detection
	+ Advisory Distribution
	+ Education and Awareness
	+ Information Sharing
* Recommendation for Incident handling
	+ Establish a formal incident response capability.
	+ Create an incident response policy, plan, and procedure
	+ Establish policies and procedures regarding incident-related information sharing.
	+ Provide pertinent information on incidents to the appropriate organization.
	+ Consider the relevant factors when selecting an incident response team model.
	+ Select people with appropriate skills for the incident response team
	+ Identify other groups within the organization
	+ Determine which services the team should offer
* **Explain the incident response life cycle**
* Section 3 of SP 800-61. Needs to 4 phases of the life cycle and activities involved in each phase.



* **Discuss the coordination and information sharing**
* Section 4 of SP 800-61. Subsection 4.1, 4.1.1, 4.2, and 4.4