Information Security Incident Response Protocol

Introduction

Pursuant to the University at Albany Information Security Policy, and SUNY Procedure 6608: Information Security Guidelines, Part 1, this protocol is established as part of the Incident Response Security Domain.

Security Domain

The Incident Response Security Domain establishes procedures and assigns responsibilities for detecting, reporting, and responding to suspected and known information security incidents that result in unauthorized access or alteration of University business records, or attempts to deny or impede legitimate access to those records.

What is an Information Security Incident?

An information security incident is considered to be any adverse event that threatens the confidentiality, integrity or availability of University or affiliate information resources. These events include, but are not limited to, the following activities:

- Suspected criminal use of systems or services, including:
  - Identity theft
  - Disclosure, destruction, or alteration of University or affiliate - managed systems or data
- Loss or theft of devices that contain or enable access to University records
- Compromise of a web page
- Compromised credentials
- Attempts (either failed or successful) to gain unauthorized access to a system or its data
- Unwanted disruption or denial of service (DoS)
- Unauthorized use of a system for the transmission, processing or storage of data
- Changes to system hardware, firmware or software characteristics without the University’s or affiliate’s knowledge, instruction or consent
  - Execution of malicious code, often referred to as malware, such as viruses, Trojans, worms or botnets
  - Unauthorized changes to system configurations
- Attempts (either failed or successful) to cause failures in critical infrastructure services, loss of critical supervisory control and data acquisition (SCADA) systems

Objectives

This protocol defines specific roles and responsibilities to assure that information security incidents are properly reported and personnel respond effectively to these reports. The effectiveness of the University response is measured by the following:

- The ability to identify an incident, i.e., the operation of a robust and up-to-date intrusion detection infrastructure
- The speed and accuracy with which an incident is detected
- How quickly the incident is contained
- Remediation of the underlying vulnerability that was exploited
- Mean time to restoration of the affected system or service
- Documentation and review for the purpose of measurement and prevention
- The establishment and preservation of a chain of custody to assure the admissibility of evidence related to an investigation

Scope

This is a University-wide protocol that applies to all University personnel and the employees of those entities and affiliates that rely on the University’s IT infrastructure, data, or applications for their operations.

Roles and Responsibilities

Chief Information Security Officer- The Chief Information Security Officer (CISO) has primary responsibility for defining the standards and procedures of the University’s Information Security Incident Response plan. The plan will be developed in consultation with the University’s Office of Legal Counsel, the Office of Human Resources Management, Facilities Management, the University Police Department, and IT technical staff.

University Personnel and Employees of University Affiliates -- All staff are required to comply with the standards and procedures of the University’s Information Security Incident Response plan.

Compliance

1. What Types of Incidents Must Be Reported

A. Unauthorized Access

  - Report successful, unauthorized access to systems (e.g., web site defacements, unauthorized root or administrator access).
• Report unsuccessful attempts only if they are considered to be persistent (e.g., someone from the same source keeps locking out accounts trying to brute force passwords, an automated script keeps probing a web server causing response problems).
• Report suspected unauthorized access if you have evidence that suggests anomalies in routine access activity (e.g., access by authorized users outside of normal business hours, or from non-US locations).

B. Malicious Code
• Report instances of viruses, Trojans, worms, botnets or other forms of malicious code that have infected University or affiliate-owned systems.
• Report sources of persistent attempts to install or inject malware on University or affiliate-owned machines or processes, regardless of whether or not they are successful (e.g., large spam runs with malicious attachments or links).

C. Denial of Service (DoS)
• Report all denial of service attacks that adversely affect or degrade access to critical services.
• Report all other attempted denial of service attacks only if they are persistent or significant (e.g., attempted DoS attacks aimed specifically at DNS servers or routers would be significant.)

D. Reconnaissance Scans and Probes
• Scans and probes that precede or are related to the incidents listed above should be reported as part of that incident.
• Any other scans and probes should be reported only if they are persistent or significant.

Review
This protocol and all related published documents will be reviewed no less than once every three years.

Related Documents
SUNY Procedure #6608: Information Security Guidelines, Part 1: Campus Programs & Preserving Confidentiality
NYS Information Security Breach & Notification Law
NYS Governmental Accountability, Audit & Internal Control Act
NYS Cyber Security Policy P03-002: Information Security Policy
NYS Cyber Security Policy P03-001: Cyber Incident Reporting Policy
SUNY Policies of the Board of Trustees

Updated: September 2011

Need more help? Contact the ITS Service Desk.