

Information Technology
Information and Systems Security/Compliance



NORTHWESTERN
UNIVERSITY

Information Security Incident Response Protocol

Version 1.0 - Abridged

Refer all questions or recommendations regarding this document to:

Dave Kovarik, Director
Information and Systems Security/Compliance
Office: (847) 467-5930
E-mail: david-kovarik@northwestern.edu

Information Security Incident Response Protocol

Revision data

Date	Version	Modified by	Comments
Mar 24, 2006	1.0	D. Kovarik david-kovarik@northwestern.edu	Published

Information Security Incident Response Protocol

I. The Information Security Incident Response Protocol

The purpose of the Information Security Incident Response Protocol is to establish procedures in accordance with applicable legal and regulatory requirements and University policy to address instances of unauthorized access to or disclosure of University Information, to be known as an Incident. Depending on the circumstances, the University may decide to modify or not to follow one or more of the procedures outlined in this protocol in response to a particular security incident with the understanding that the University will take reasonable steps to investigate and resolve any security incidents.

In addition to all the defenses that have been mounted in protection of the infrastructure and the information processed within, conventional wisdom recommends a high level of preparedness for a security incident. This protocol describes the response to such events, the conditions whereby this process is invoked, the resources required, and the course of recommended action. Central to this process is the Incident Response Team (IRT), assembled with the purpose of addressing that particular circumstance where there is credible evidence of an incident.

The primary emphasis of activities described within this protocol is the return to a normalized (secure) state as quickly as possible, while minimizing the adverse impact to the University. The capture and preservation of incident relevant data (e.g., network flows, data on drives, access logs, etc.) is performed primarily for the purpose of problem determination and resolution, and methods currently employed are suitable for that purpose. It is understood and accepted that strict forensic measures are not used in the data capture and retention.

This document may reference other documentation, policies and procedures that support this protocol but are not contained within the document, e.g., policy that defines sensitive data, scripts to be followed by the NUIT Help Desk (HelpDesk) and NUIT Network Operations Center (NNOC) personnel, or documented CIRT (Computer Incident Response Team) procedures. Where this occurs, instructions to obtain these materials will be specified.

Circumstances may dictate the activation of other operational teams and execution of other protocols. The IRT must monitor and coordinate all activities occurring under other operational teams and protocols, and communicate to all interested parties in a timely manner to ensure accurate assessments and avoid efforts that may be duplicated or at cross-purposes.

Information Security Incident Response Protocol

II. Definitions

A. Information Security Incident

An Information Security Incident is generally defined as any known or highly suspected circumstance that results in an actual or possible unauthorized release of information deemed sensitive by the University or subject to regulation or legislation, beyond the University's sphere of control.

Examples of an Information Security Incident may include but are not limited to:

- the theft or physical loss of computer equipment known to hold files containing SSNs
- an unencrypted list of alumni contributors emailed to an unauthorized recipient
- a server known to hold sensitive data is accessed or otherwise compromised by an unauthorized party
- printed copies of student loan applications are discovered in a publicly accessible dumpster
- an outside entity is subjected to a DDoS (Distributed Denial of Service) attack originating from within the University network
- a firewall is accessed by an unauthorized entity
- a network outage is attributed to the activities of an unauthorized entity

Categories

For the purposes of this protocol, incidents are categorized as "Unauthorized Access" or "Unauthorized Acquisition", and can be recognized by associated characteristics.

Unauthorized Access

The unauthorized access to or disclosure of University information through network and/or computing related infrastructure, or misuse of such infrastructure, to include access to related components (e.g., network, server, workstation, router, firewall, system, application, data, etc.)

Characteristics of security incidents where unauthorized access might have occurred may include but are not limited to:

- Evidence (e-mail, system log) of disclosure of sensitive data
- Anomalous traffic to or from the suspected target
- System alerts (NUSA)
- Unexpected changes in resource usage
- Increased response time
- System slowdown or failure
- Changes in default or user-defined settings
- Unexplained or unexpected use of system resources
- Unusual activities appearing in system or audit logs
- Changes to or appearance of new system files
- New folders, files, programs or executables
- UserID lock out
- Appliance or equipment failure

Information Security Incident Response Protocol

- Unexpected enabling or activation of services or ports
- Protective mechanisms disabled (firewall, anti-virus)

Unauthorized Acquisition

The unauthorized physical access to, disclosure or acquisition of assets containing or providing access to University information (e.g., removable drives or media, hardcopy, wiring closets, file or document storage, appliance hardware, etc.)

Characteristics of security incidents where unauthorized acquisition might have occurred may include but are not limited to:

- Theft of computer equipment where sensitive data is stored
- Loss of storage media (removable drive, CD-Rom, DVD, flash drive, magnetic tape)
- Printed materials containing University sensitive data mishandled or left unsecured
- Illegal entry (burglary)
- Office equipment in disarray or out of place
- Suspicious or foreign hardware is connected to the network
- Normally-secured storage areas found unsecured
- Broken or non-functioning locking mechanisms
- Presence of unauthorized personnel in secured areas
- Disabled security cameras or devices

Severity

Incidents are further delineated by the actual and potential impact on the business of the University. The primary focus of this protocol is the handling of Severity 1 Incidents.

B. Information Security Incident Response Team

The Information Security Incident Response Team (IRT) is comprised of individuals with decision-making authority from within the University and charged by the Administration with the responsibility of assisting in the process described within this document.

C. University Information

University Information is any information maintained by or on behalf of the University that is used in the conduct of University business regardless of the manner in which such information is maintained or transmitted. University Information formats include, but are not limited to oral or written words, screen display, electronic transmission, stored media, printed material, facsimile or any other medium.

D. Sensitive Data

Sensitive Data is:

- any University Information declared to be Highly Confidential, Confidential, or Restricted by University policy, and
- any personally identifiable information as determined or governed by law or regulation or University policy requiring protection from disclosure.

Examples include but are not limited to:

- NetID and Password

Information Security Incident Response Protocol

- Name in combination with SSN
- Credit or Debit Card Number and Access Code (e.g., PIN or Password)
- Personal medical records
- Unpublished results of research or financial investment strategies
- Proprietary data (e.g., protected formulas or patents)
- “Anonymous Donor” records

E. University Client (Client)

A University Client (Client) is:

- any faculty, student, staff or alumni affiliated with the University, or
- any department or school of the University, or
- any employee (permanent, temporary and contract personnel)

F. 3rd Party

A 3rd party is:

- any entity having a relationship with the University not described as a Client (e.g., business partner, research subject, vendor), or
- any external entity initiating contact with the University (e.g., RIAA, target of DDoS attack, student applicant, member of the general public).

III. Information Security Incident Response Team (IRT)

A. Incident Response Team Composition

The IRT consists of a Primary Team and Secondary Team, if deemed necessary. Each member of the Primary Team will designate an Alternate member to participate if the Primary Member is unavailable. The Primary Team will consist of representatives from the following areas:

A1. Primary Team (Required)

1. IT - Information and System Security/Compliance (ISS/C) - Team Lead
2. IT – Computing Services (CS)
3. IT - Technology Support Services (TSS)
4. IT – Telecommunications and Network Services (TNS)
5. IT - Management Systems
6. Auditing Department
7. Office of General Counsel
8. University Police
9. University Relations
10. Disaster Recovery/Business Continuity Planning

A2. Secondary Team (as needed)

The circumstances surrounding each incident may differ and require personnel with expertise or skills beyond that of the Primary Team. Members of the Primary Team will determine what, if any, additional resources are required and a Secondary Team may be established with:

Information Security Incident Response Protocol

- Individuals with decision-making authority identified to have a vested interest in the resolution of the incident.
- Individuals identified as subject matter experts or having skills required for resolution of the incident.

Information Security Coordinators representing an affected Client or 3rd Party, or known to have an established relationship with an affected Client or 3rd Party, may be requested to serve on the Secondary Team.

B. Team Objectives

Led by the University's Information and Systems Security/Compliance office, the IRT's objective is to:

1. Coordinate and oversee the response to Incidents in accordance with the requirements of state and federal laws and University policy;
2. Minimize the potential negative impact to the University, Client and 3rd Party as a result of such Incidents;
3. Where appropriate, inform the affected Client and 3rd Party of action that is recommended or required on their behalf;
4. Restore services to a normalized and secure state of operation.
5. Provide clear and timely communication to all interested parties.

C. Responsibilities

To ensure an appropriate and timely execution of this protocol, the IRT Lead (or designated IRT Member) is required to:

1. Confirm the occurrence of an Incident requiring the execution of this protocol.
Confirmation activities include but are not limited to:
 - direct conversation with Client, 3rd Party, HelpDesk, NNOC personnel, "on call" engineer, IRT members or others having information about the event
 - review of system logs or audit records
 - examination or analysis of anomalies or untoward events
 - collection of any evidence supportive of the event
2. Supervise and direct the consistent, timely, and appropriate response to an Incident.
3. Provide appropriate communication to parties having a vested interest in the incident.
4. Offer support to the Client or 3rd Party as appropriate until the Incident is resolved.
5. Conduct a post-Incident review.
6. Maintain the procedures contained in this document.

D. Accountability

Individual IRT members are accountable to the Team and University Administration for the timely and effective execution of this protocol and associated activities.

E. Reporting a Security Incident

Anyone with knowledge or a reasonable suspicion of an incident is instructed to make an immediate report to any of the following:

- The NUIT Network Operations Center (NNOC), 847-467-NNOC (6662)
- The NUIT Help Desk, (847) 491-HELP (4357)

Information Security Incident Response Protocol

- The e-mail addresses of **security@northwestern.edu** or **noc@northwestern.edu**.
Note: These e-mail addresses may be used but are less effective than the direct notification of the Help Desk or NNOC via voice communication or voicemail.

HelpDesk and NNOC personnel use scripts (e.g., lists of predetermined questions) to assist in problem determination and resolution. These scripts assist support personnel to identify those events that may be classified as an Information Security Incident.

Anyone receiving notification of an Incident must contact the NNOC immediately. NNOC personnel will contact the Telecommunications and Network Services “on call engineer” in the likelihood of an incident. The engineer will follow the TNS-defined escalation procedures and immediately contact the IRT Lead when an Incident has or appears to have occurred.

F. Activation of Team

Once the IRT Lead has determined an Incident has occurred, the IRT Lead will activate this protocol within 24 hours after Incident determination. Notification of the Primary Team member or Alternate should occur via a direct communication by telephone or face-to-face contact. Voice-mail and e-mail are not considered direct notification. Respective Primary and Alternate Team members should exchange information frequently to ensure their knowledge of the incident is current.