

IT Security

Information Technology Systems and Services

UND Information Technology (IT) Incident Response Policy

Table of contents

- I. Reason for the Policy
- II. Applicability of the Policy
- III. Policy Statement
- IV. Procedures
- V. Definitions
- VI. Related Documents / Policies
- VII. Effective Dates
- VIII. Contacts

I. Reason for the Policy

The university network, information systems, and data are critical resources for accomplishing the mission of the University of North Dakota. All university users have an interest in the security of these resources, and share in the responsibility for protecting them. Prompt and consistent reporting of and response to *IT incidents* protects and preserves the integrity, availability, and privacy of data and *IT resources* and helps the university to comply with applicable law.

II. Applicability of the Policy

This policy applies to all members of the University of North Dakota community.

III. Policy Statement

Users and/or local support providers of *IT resources* must report all *IT incidents* promptly and to the appropriate party or office. If necessary, *local support providers* are responsible for containing, eradicating, and restoring the compromised system.

IV. Procedures

a. Reporting and Classification

An end user of an *IT resource* should report all suspected incidents to their *local support provider*, the UND IT Security Officer (ITSO), or the Information Technology Systems and Services (ITSS) helpdesk.

Upon receiving a notification, or detecting an *IT incident*, the *local support provider* must determine if the incident is a *major incident* (see section V. Definitions).

If the incident is not a *major incident*, the *local support provider* should submit a ticket to the ITSS helpdesk or verify a ticket has been submitted regarding the incident. The *local support provider* (with assistance, if necessary, from the ITSO, helpdesk, *SIRT* or local IT support) should then contain, eradicate, and restore the system as outlined in these procedures. If the incident involves the loss of a device, then containing, eradicating, and restoring are unnecessary.

If the incident is a *major incident*, the *local support provider* must report the incident to the UND ITSO and the *Data Steward* and/or Unit Head/Dean. The ITSO will maintain a log of all reported *major incidents* recording the relevant information, including, but not limited to, the date of the incident, the College or Department affected, the type of *private* or *confidential* information involved (if any), a summary of the incident, any measures taken to

respond to the incident, and lessons learned. The *local support provider* (with assistance, if necessary, from the ITSO, helpdesk, *SIRT* or local IT support) should then contain, eradicate, and restore the system and perform follow-up as outlined in these procedures. If the major incident involves the loss of a device, then containing, eradicating, and restoring are unnecessary.

If necessary, the ITSO will work with the *local support provider* and the *UND Security Incident Response Team (SIRT)* to determine whether or not *private* or *confidential* data is involved in the incident, and to what level. Based on the results of this determination, the ITSO and CIO will decide whether or not to convene the *Information Security Incident Response Team (ISIRT)*.

b. Containment

Ideally, the affected system(s) should be removed from the network, either by physically removing the network cable or working with the *SIRT* to disable network access. If the *local support provider* determines the system is critical to university business, then he or she should work with the *SIRT* to isolate the system in such a way that university business can be performed while still protecting other areas of campus and the data held on the system.

c. Eradication

If the incident is a *major incident*, the system should not be altered until the *local support provider* reports the incident, receives guidance from the ITSO, and creates a *forensic image* to assist in any necessary investigation. The *local support provider* should then determine the cause of the incident and, if appropriate, remove the cause of the incident. If the eradication is unsuccessful or the compromise/infection reoccurs within two days, the *local support provider* should notify the ITSO and await further instructions.

d. Restoration

If the eradication is successful, the *local support provider* should clean and restore the data and availability of the affected system and return the system to normal operations. If necessary, the system should be restored from backup and appropriate patches should be applied and server hardening should be performed to prevent future incidents. Once the system is returned to normal operations, the *local support provider* should perform a backup of the system and then monitor the system for a reoccurrence of the incident.

e. Follow-Up

If a *major incident*, the *local support provider* should notify the ITSO of the resolution to the incident. The ITSO will work with the *local support provider* to collect lessons learned and develop best practices to publish and share with appropriate individuals.

V. Definitions

Confidential Information Confidential Information is information that is not to be publicly disclosed. The disclosure, use, or destruction of Confidential Information can have adverse affects on the UND and possibly carry significant civil, fiscal, or criminal liability. This designation is used for highly sensitive information such as open legal investigations, sealed bids, research activity, social security numbers, etc., whose access is restricted to selected, authorized employees.

Data Steward The individual who has ultimate responsibility and ownership for a particular set of data (e.g. a department head, dean, or V.P.)

Forensic Image The process of making a duplicate of the computer system hard drive(s) using some form of hardware write protection, such as a hardware write blocker, to ensure no writes are made to the original drive. There are two goals when making an image:

1. Completeness (imaging all of the information)

2. Accuracy (copying it all correctly)

Information Security Incident Response Team (ISIRT)

The role of the UND ISIRT is to coordinate the University response to breaches of security involving *confidential* or *private* information. The responsibilities of the ISIRT include, but are not limited to:

- Notifying affected constituents of the incident
- Coordinating responses to public inquiries
- Making the decision to involve outside entities, including law enforcement agencies and computer forensic experts
- Discussing, reviewing, and documenting any lessons learned from the security breach

The ISIRT reports to the Provost, and is comprised of members from the following areas:

- Chief Information Officer (CIO)
- Office of General Counsel
- University Relations
- Finance & Operations
- Campus Safety and Security/Risk Management
- University Police
- IT Security Officer
- Data Steward (incident specific)
- Unit Head/Dean (incident specific)
- Local Support Provider (incident specific)

IT Incident

An activity or event that results in damage to, misuse of, or loss of, an *IT resource*. Incidents include but are not limited to:

- Loss of a computing device (misplaced, stolen, vandalized)
- Detection of a malicious program, such as a virus, worm, Trojan horse, keystroke logger, rootkit, remote control bot, etc.
- Detection of unauthorized users, or users with unauthorized escalated privileges.
- Detection of a critical or widespread vulnerability or misconfiguration that might lead to a compromise affecting the confidentiality, integrity, or availability of university systems or data.

IT Resource

A computing asset provided by the University to further its mission. Examples include, but are not limited to, network bandwidth, networking equipment, workstations, computer systems, data, databases, servers, and printers.

Local Support Provider

An individual or group with principal responsibility for the installation, configuration, security, and maintenance of an *IT resource*. When there is no formally identified local support provider (e.g., a personally owned computer used from home to connect to the UND network), the user is the local support provider.

Major Incident

An IT incident which:

- Involves a device or system containing *private* (see definition) or

confidential (see definition) data

- Threatens the business continuity of the college, department, or university
- Affects multiple systems or servers
- Involves the violation of North Dakota state or U.S. federal law

Private Information

Private Information includes information that UND is under legal or contractual obligation to protect such as FERPA, HIPAA or GLBA data. Examples would include Employee ID numbers, birth dates, location of assets, donors, gender, etc.

Security Incident Response Team (SIRT)

The UND SIRT consists of individuals from various departments within ITSS including Network Services, Server Administration, and IT Security. The SIRT reports to the Director of ITSS who assigns the team to respond to an incident:

- Which requires coordination across multiple departments
- When a single department lacks the resources to respond
- When the *local support provider* requests assistance
- When the *ISIRT* determines involvement is necessary

VI. Related Documents/Policies

- [UND Student Acceptable Use Policy](#)
- [NDUS Procedure 1901.2 Computer and Network Usage](#)
- [NDUS Data Classification and Information Technology Security Standards](#)
- ConnectND Procedure for Data Protection and Incident Response in Higher Education

VII. Effective Dates

Last Edited: Mar 8, 2007

Approved: Sept 24, 2007

Next Review Date: Sept 24, 2009

VIII. Contacts

Contact	Phone
UND IT Security Officer (ITSO)	777-3587
UND ITSS Helpdesk	777-2222
UND Chief Information Officer (CIO)	777-4328