Incident Response Policy and Procedures

Policy

Users and/or administrators of *IT resources* must report all *IT incidents* promptly and to the appropriate party or office as required by the North Dakota University System (NDUS) policy NDUS 1202.2 Incident Response Policy.

Purpose of Policy

The Minot State University (MSU) network, information systems, and data are critical resources for accomplishing the mission of the University. All MSU 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 MSU to comply with applicable law.

Scope of Policy

This policy applies to all MSU employees and individuals that gain access to data or systems on this campus.

Definitions

Restricted Data — This is data that requires the highest level of protection. It is data protected by federal or state laws, regulations, contracts, or policy. The unauthorized disclosure of restricted data would typically require the university system to report the disclosure and/or provide notice to the individual whose data was inappropriately accessed. See the Data Classification and Information Security Standard.

Private Data — This is data that should not be available to the public. It is data that may be protected by federal or state laws, regulations, contracts, or policy.

Public Data — This is data that is not considered to be “Restricted” or “Private”. It is data that can generally be released to the public.

Data Steward — The individual who has ultimate responsibility and ownership for a particular set of data.

Information Security Incident Response Team (ISIRT)

The role of the MSU ISIRT is to coordinate the response to breaches of security involving *restricted* information. The responsibilities of the ISIRT include, but are not limited to:

- Notifying NDUS ISIRT of the incident
- 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 IT Security Officer, and is comprised of representatives from the following areas of the campus:

- Campus President
- IT Director, Desktop Support Services
- VP, Administration & Finance
- VP, Academic Affairs
- Communications and Public Relations
- Director, Security & Safety
- NDUS Information Security Department
- Data Steward (incident specific)
- Department Head (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.

Information Technology (IT) Resource

All institution owned, operated, leased, or contracted systems and services including, but not limited to, computers, databases, storage, servers, networks, input/output connecting devices, telecommunications infrastructure and equipment, software, and applications.

Major Incident

An IT incident which:

- Involves a device or system containing *restricted* (see definition) data
- Threatens the business continuity of MSU
- Affects multiple systems or servers
- Involves the violation of North Dakota state or U.S. federal law

Security Incident Response Team (SIRT)

The SIRT consists of individuals from various departments within MSU including Network Services, Administration, and Campus Security. The SIRT reports to the Information Security Officer who assigns the team to respond to an incident.

Contacts

Contact	Email
MSU Information Technology Department	701-858-4444 helpdesk@minotstateu.edu
Darren Olson – IT Director, Network Service / IT Security Officer	darren.olson@minotstateu.edu
Lisa Haman – IT Director, Desktop Services	lisa.haman@minotstateu.edu

Procedures

a. Reporting and Classification

The end user or administrator of an *IT resource* should report all suspected incidents to the MSU Information Technology Department, or their Department head.

Upon receiving a notification, or detecting an *IT incident*, the end user or administrator must determine if the incident is a *major incident* (see DEFINITIONS section).

If the incident is not a *major incident*, the end user or administrator should submit a ticket to the Minot State University help desk or verify a ticket has been submitted regarding the incident. The end user or administrator with assistance, if necessary, from the MSU IT Department, *Security Incident Response Team (SIRT)* 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 end user or administrator must report the incident to the MSU IT Department and the *Data Steward* and/or Department head. The MSU IT Department will maintain a log of all reported *major incidents* recording the relevant information, including, but not limited to, the date of the incident, the Department or system affected, the type of *restricted* information involved (if any), a summary of the incident, any measures taken to respond to the incident, and lessons learned. The end user or administrator (with assistance, if necessary, from the MSU IT Department) 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 MSU Information Technology Department will work with the end user or administrator and the *SIRT* to determine whether or not *restricted* data is involved in the incident, and to what level. Based on the results of this determination, the MSU IT Department 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 end user or administrator determines the system is critical to MSU business, then he or she should work with the *SIRT* to isolate the system in such a way that MSU 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 or reconnected to the network until remediated by the MSU IT Department.

d. Restoration

Once the system is secured and returned to normal operations by the MSU IT Department, the end user or administrator should perform a backup of the system and then monitor the system for a reoccurrence of the incident.

e. Follow-Up

The MSU IT Department will work with the end user or administrator to collect lessons learned and develop best practices to share with appropriate individuals.