

## **ITS Security Procedure: Information Security Incident Reporting and Response**

### **UNMC Information Technology Services**

#### **INTRODUCTION**

Information system security is a growing problem. Effective response and collective action are required to counteract security violations and activities that lead to security breaches. UNMC management must know the extent of security problems in order to make proper decisions pertaining to policies, programs and allocation of resources. Responding to security alerts will help to prevent incidents from reoccurring. Quick reporting of incidents, such as new viruses, is essential to stopping them from spreading and impacting other systems.

#### **BASIS FOR POLICY**

Attacks on University [information technology resources](#) are serious infractions of the [UNMC Policy No. 6051, Computer Use and Electronic Information Security](#), and misuse or vandalism of University resources. This policy provides a method for pursuing the resolution and follow-up of [information security incidents](#).

This policy, which applies to all UNMC [information technology resources](#), also provides guidance in determining the proper response to a misuse of [information technology resources](#) from within or outside the University and documents the process UNMC will follow to resolve the situation. The ultimate goal of [security incident](#) response and centralized reporting is to protect data and prevent obstruction of UNMC operations.

#### **Policy**

Attacks on University resources will not be tolerated. All members of the [workforce](#) must report information security incidents that have a real impact on the UNMC organization (such as when damage is done, access is achieved by the intruder, loss occurs, web pages are defaced, malicious code is implanted) or when you detect something noteworthy or unusual (new traffic pattern, new type of malicious code, specific IP as source of persistent attacks). Do not report routine probes, port scans, or other common events such as detection and removal of a virus from an email.

An information security incident includes, but is not limited to the following events, regardless of platform or computer environment:

1. Evidence of tampering with data;
2. System is overloaded to the point it is not responsive ([denial](#) of service attack on

- the network );
3. Web site defacement;
  4. Unauthorized access or repeated attempts at unauthorized access (from either internal or external sources);
  5. [Social engineering](#) incidents;
  6. Virus attacks which cause workstations or servers to be inoperable;
  7. Email which includes threats or material that could be considered harassment;
  8. Discovery of unauthorized or missing hardware or software in your area; and
  9. Other incidents that could undermine or raise concern about the stability or reliability of the UNMC information technology systems

[Information Systems Technology](#) (ITS) and the system administrator will work jointly to resolve the incident. The system administrator responsible for support of the system or network under attack is in all cases expected to:

1. Report the attack to the ITS Help Desk at 559-7700 who in turn will notify the ITS Security Officer or designee;
2. Fully cooperate with the ITS Information Security Officer in resolution of the issue;  
NOTE: ITS Information Security Officer, in consultation with Executive Director of Information Technology Services, unit management, system administrator, Executive Director of Human Resources and the Office of the Vice President and General Counsel will determine if evidence should be preserved or if system should be repaired as soon as possible;
3. Block or prevent escalation of the attack, if possible;  
NOTE: ITS may temporarily block access to or from a certain device until the problem is resolved.
4. Repair the resulting damage and fix the root cause;
5. Restore service to its former level, if possible;
6. Preserve evidence, where appropriate; and
7. Notify the ITS Information Security Officer or designee of resolution of the incident.

In cooperation with the system administrator and unit management, the ITS Information Security Officer or designee will:

1. If applicable, coordinate notification of the Internet service provider;
2. Notify and keep informed the UNMC Executive Director ITS;
3. Notify and keep informed Operating Unit Management;
4. Notify and keep informed the Executive Director of Human Resources and the Office of the Vice President and General Counsel as appropriate. Decision to involve law enforcement will be made by the Executive Director of Human Resources and the Office of the Vice President and General Counsel;
5. Assemble the Computer Incident Response Team (CIRT) as required; and  
NOTE: Computer Incident Response Team (CIRT) is composed of:  
UNMC Executive Director ITS

ITS Security Officer  
Human Resources  
Legal  
Public Relations  
Campus Security  
Unit management

6. Ensure that incident is reviewed retrospectively to determine methods of improving security.

**Definitions:**

*Information technology resources* include but are not limited to voice, video, data and network facilities and services.

*Denial of service* is an event in which a user or organization is deprived of resource services that they would normally expect to have.

*Social engineering* describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures.

*Workforce* refers to faculty, staff, volunteers, trainees, students, independent contractors and other persons whose conduct, in the performance of work for UNMC, is under the direct control of UNMC, whether or not they are paid by UNMC.

For more information, contact the ITS Helpdesk or the ITS Information Security Officer.

Policy Home Page / Intranet Home Page / [Top of this Page](#)

This is a new policy.  
This page updated on , by .