

## Information Security Incident Reporting and Response

### INTRODUCTION

Information security is a growing problem. Effective response and collective action are required to counteract information security violations and activities that lead to security breaches.

UNMC management, must know the extent of information security problems in order to make proper decisions pertaining to policies, programs and allocation of resources. Responding to information security alerts will help to prevent incidents from occurring. 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 Computer Use and Electronic Information Security policy, and misuse or vandalism of University resources. Serious attacks on University resources will not be tolerated. This policy provides a method for pursuing the resolution and follow-up of incidents.

#### Definition:

##### *Information Security Incident:*

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

1. Evidence of tampering with data;
2. Denial of service attack on the network (system is overloaded to the point it is not responsive);
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 adversely affect servers or multiple workstations;
7. Email which includes threats or material that could be considered sexual harassment
8. Discovery of unauthorized hardware or software in your area
9. Other incidents that could undermine raise concern about the stability or reliability of the UNMC information technology systems.

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

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

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

## **Policy**

All members of the workforce must report events 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 an email has had a virus removed.

The ultimate goal of information security incident response and centralized reporting is to protect data and prevent obstruction of UNMC operations.

This policy:

1. Provides guidance in determining the proper response to a misuse of Information Technology resources from within or outside the University.
2. Documents the process UNMC will follow to resolve the situation
3. Applies to all UNMC information technology resources.

ITS and the system administrator will jointly work 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 who in turn will notify the IT 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 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
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 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 Emergency Response Team (CERT) as required.  
***NOTE: The CERT will be composed of the following organizational units: ITS, Human Resources, Legal, Public Relations, Campus Security, Organizational Management.***
6. Ensure that incident is reviewed retrospectively to determine methods of improving information security.