# IT Security Incident Reporting

Effective: July 1, 2004
Updated/Revised: February 2, 2006
Contact: Office of the CIO

## Introduction

Compromises in security can potentially occur at every level of computing from an individual's desktop computer to the largest and best-protected systems on campus. Incidents can be accidental incursions or deliberate attempts to break into systems and can be benign to malicious in purpose or consequence. Regardless, each incident requires careful response at a level commensurate with its potential impact to the security of individuals and the campus as a whole.

For the purposes of this policy an "IT security incident" is any accidental or malicious act with the potential to

- result in misappropriation or misuse of confidential information (social security number, grades, health records, financial transactions, etc.) of an individual or individuals,
- significantly imperil the functionality of the information technology infrastructure of the ISU campus,
- provide for unauthorized access to university resources or information,
- allow ISU information technology resources to be used to launch attacks against the resources and information of other individuals or organizations.

In the case when an IT security incident is determined to be of potentially serious consequence, the responsibility for acting to resolve the incident and to respond to any negative impact rests with the university rather than individuals, colleges, departments, or units. The university has established procedures and identified an IT Security Response Team (ITSRT) as its authority in developing response plans to serious IT security incidents. As described below, reports of IT security incidents will be forwarded to ITSRT. The ITSRT follows protocols in determining what actions should be taken and depending upon the nature of the security incident will determine whether incidents should be handled within the purview of the department, college, or unit or by security specialists within ITSRT. In some cases, the ITSRT may escalate the incident to law enforcement, university counsel, or other university officers.

This document outlines the procedures individuals should follow to report potentially serious IT security incidents. University staff members whose responsibilities include managing computing and communications systems have even greater responsibilities. This document outlines their responsibilities in securing systems, monitoring and reporting IT security incidents, and assisting individuals, administrators, and other IT staff to resolve security problems.

## Policy Statement

### Dealing with Viruses, Worms, Etc.

Individuals and information technology support professionals are not required to report IT security incidents involving viruses, worms, etc. unless the nature of the virus suggests there may be serious impact as described above. Because viruses and worms can reduce the functionality or otherwise affect the campus computing and communication environment, individuals and information technology support professionals are expected to:

- prevent computer equipment under their control from being infected with malicious software by the use of preventive software and monitoring, and
- take immediate action to prevent the spread of any acquired infections from any computers under their control.

Assistance is available from local information technology support professionals and from university-wide Information Technology (see Resources below).

## Reporting and Responding to IT Security Incidents

### Individuals

- Should attempt to stop any IT security incident as it occurs. Powering-down the computer or disconnecting it from the campus network will stop any potentially threatening activity.
- Report IT security incidents to an information technology support professional. IT support staff will help you assess the problem and determine how to proceed.
    1. Individuals should first attempt to contact their local department, college, or designated IT support professional.
    2. If a local or designated IT support staff is unavailable, individuals should complete the IT Security Incident Report form (see Resources below). The form will be reviewed by the ITSRT to determine what action is necessary.
    3. If the incident has potentially serious consequences and requires immediate attention, individuals can report the security incident by calling 515-294-3221.
- Following the report, individuals should comply with directions provided by IT support staff or the IT Security Response Team to repair the system, restore service, and preserve evidence of the incident.
- No retaliatory action should be taken against a system or person believed to have been involved in the IT security incident. All response actions should be guided by the IT Security policy (see Resources below).

### IT Support Professionals

Department, college, or unit information technology support professionals have additional responsibilities for IT security incident handling and reporting for both the systems they manage personally for their units and the systems of users within their units. In the case of an IT security incident, IT support staff should:

1. Respond quickly to reports from individuals.
2. Take immediate action to stop the incident from continuing or recurring.
3. Determine whether the incident should be handled locally or reported to the IT Security Response Team.
    - If the incident does not involve the loss of confidential information or have other serious impacts to individuals or the university, the IT support staff should repair the system, restore service, and preserve evidence of the incident.
    - If the incident involves the loss of confidential information or critical data or has other potentially serious impacts, the IT support staff should
        1. File an IT Security Incident Report form including a description of the incident and documenting any actions taken thus far.
        2. If the security incident needs immediate attention, report the incident by calling 515-294-3221. The ITSRT will investigate the incident in consultation with the IT support staff and develop a response plan.
        3. Notify the appropriate college, department or unit administrator that an incident has occurred and that the IT Security Response Team has been contacted.
        4. Refrain from discussing the incident with others until a response plan has been formulated.
        5. Follow the ITSRT response plan to:
            - Repair the system and restore service.
            - Preserve evidence of the incident.
4. No retaliatory action should be taken against a system or person believed to have been involved in the IT security incident. All response actions should be guided by the IT Security policy.

# Resources

- Information Technology
- IT Security Incident Report Form
- IT Security Policy