UtahStateUniversity

# POLICY MANUAL

## OPERATING POLICIES AND PROCEDURES

**Number 5205**
**Subject: Network Monitoring & Vulnerability Scanning**
**Effective Date: September 24, 2008**

## 5205.1 PURPOSE

Computers that are connected to the Utah State University Network are at risk of compromise resulting in unauthorized access to computing resources (processor power and storage space) and to confidential data (personal and financial) stored on or transmitted through the computer as part of university operations. This Policy defines a means by which vulnerable and/or compromised computers might be identified and isolated from the network pending correction of the problem.

## 5205.2 POLICY

The University's Information Technology (IT) Security Team is authorized and directed to monitor network traffic patterns and to probe ports of connected computers for the purpose of identifying vulnerable and compromised computers on the USU network. All computer and communication devices connected to the Utah State University network are subject to this monitoring, whether or not they are owned or operated by Utah State University. Arrangements with the Security Team for exceptions can be made if probes or other vulnerability testing interfere with research applications and other security assurances can be obtained.

IT is directed to develop procedures for announcement or notification of network-connected devices with vulnerabilities or compromises. Vulnerabilities and other policy violations will be resolved by communication to the user of record, with denial of network access reserved as a last resort. Compromises and other security breaches will be resolved immediately by termination of network access to protect the resources. That termination will be followed by communication with affected users or system administrators to identify and resolve the issue.

IT will implement procedures for subsequent handling of incidents to achieve a good resolution, maintaining or restoring the user's network access while protecting the institutions resources, consistent with the Information Security (5200) and the Appropriate Use of Computing, Networking, and Information Resources (5201).

The Security Team will monitor patterns and attributes of network traffic but not the information content except as needed to identify known attack vectors. Privacy of individual communication will be respected by the Security Team, consistent with the Data Privacy (3016).

Network performance and/or availability may be affected by the network scanning. The IT Security Team is the authorized entity to perform enterprise-wide network scanning of all USU computer systems. System administrators may scan systems and subnets in their area of responsibility. Those scans must be coordinated with the IT Security Team to avoid confusion with unauthorized intrusion attempts.

## 5205.3 DEFINITIONS

**Vulnerability** - lack of a security barrier to unauthorized access or use.

**Compromise** - a vulnerability that has been found and exploited by an unauthorized user.

**Network Traffic Patterns** - information about the source, destination, protocol, port and bandwidth of network packets.

**Network Scanning** - systematic attempts to communicate with a class of network addresses via a particular port or protocol to see which computers respond. A first step to identify and exploit vulnerabilities.