

1. Overview

The University of Arizona network is under continual attack. Attempts to exploit network resources have become commonplace. Computer users must be prepared to respond properly when a security incident occurs. Incident handling isn't a reactionary exercise – it's a logical progression down a predetermined path. Developing a plan of attack for different types of security incidents is crucial to the restoration of normal operations.

2. Purpose

The purpose of this document is to provide system administrators with guidelines for incident handling at the University of Arizona.

3. Scope

These minimum standards apply to all University of Arizona departments and affiliates, including contractors and vendors handling University systems or data.

4. Guidelines

The following guidelines are necessarily general. For more detailed information, see the Related Documents. If you need assistance with any of the evaluation procedures, go directly to Incident Reporting.

4.1. Incident Evaluation

- Change system password(s)
- Check the system for new or modified accounts
- Review log files for abnormal entries or missing timespans
- Look for modifications made to system software and configuration files
- Scan system for new binaries (including user directories)
- Check other local systems and related remote systems

4.2. Incident Reporting

- Fill out an Incident Report Form (<http://security.arizona.edu/files/irf.pdf>)
- Contact SIRT at 626-0100 or sirt@arizona.edu to discuss the nature of the incident.
- If it is determined that a forensic investigation is required, work with SIRT and the appropriate authorities for remediation; otherwise clean or reformat system as appropriate.

5. Related Documents and Resources

CERT's Steps for Recovering from a UNIX or NT System Compromise:

http://www.cert.org/tech_tips/win-UNIX-system_compromise.html

Intrusion Detection Cheat Sheets for Linux:

http://www.sans.org/score/checklists/ID_Linux.pdf

Intrusion Detection Cheat Sheets for Windows:

http://www.sans.org/score/checklists/ID_Windows.pdf

6. Related Guidance

Information Security Policy (IS-100)

Information Security Terms Guideline (IS-G100)

Exceptions Procedure (IS-P100)

All *italicized* terms used in this standard are defined in the Information Security Terms Guideline.

Revision History

Initial Draft	5/25/06
Effective Date	5/27/08