THE UNIVERSITY OF ARIZONA.

Standard Title: Minimum Security for Networked Devices
Standard Number: IS-S602
Responsible Office: Office of Information Security

The use of *networked devices* with access to *university resources* has become a part of everyday life within the university, and sharing of *confidential university data* is commonplace. Securing these *devices* is necessary to ensure the *confidentiality*, *integrity*, and *availability* of *university resources*. As users of these *devices*, it is important for everyone to understand and contribute to the overall security of the *university network*.

The following standards will assist *university employees*, *affiliates*, *associates* and *volunteers* in managing, maintaining and securing *University-networked devices*. *Units* and individuals are encouraged to maintain stricter limits where practical or required. These standards should not be used to reduce the level of security that may already exist.

These security standards apply to all *devices* connected to the *university network* used to access, store, transmit or interface with a *university resource.*

1. **Operating system and software patch updates**
   All *networked devices* must have all available *patches* that address security *vulnerabilities* installed. Vulnerable systems face disconnection from the *university network*. Delaying installation until a convenient time, such as semester breaks, is unacceptable. Exceptions, as stated in the Information Security Policy, may be made for *patches* that *compromise* the usability of critical applications, provided additional security measures are taken. Images should be vetted and kept up to date with both critical operating system and application *patches*.

   For more information, please see the *University's* Software Patching Guideline (IS-G602B).

2. ***Antivirus software***
   All computers connected to the *university network* must be running current *antivirus software*, and must check for updates at least daily, preferably hourly. The minimum standard for *antivirus software* is to meet or exceed the effectiveness of the software products *site-licensed* by the *University*. Non-compliant or infected systems are subject to removal from the *network*.

   For more information, please see the *University's Antivirus Software* Guideline (IS-G602C).

3. **Anti-spyware software**
   All computers connected to the *university network* should have anti-spyware software installed (if available) and periodic *scans* performed to detect and remove spyware.

   For more information, please see the University's Spyware and Adware Prevention Guideline (IS-G602D).

4. ***Host-based firewall software***
   Host-based *firewalls* may be used to provide an additional level of security to individual computer systems. *Device* users are encouraged to seek out and follow the advice of their *network manager, system administrator or other technical support person* regarding the use of *host-based firewall*

software. The *University site-licensed* host-based *firewall*, a *firewall appliance*, or equivalent measures must be used to protect any computer that cannot receive the latest software security *patches*.

For more information, see the *University's Firewall* Software Guideline (IS-G602E).

5. Passwords

All *devices* and/or accounts with access to *university resources* shall require adequate passwords or an alternate secure *authentication* system (e.g., biometrics or Smart Cards). This standard applies to *university employees*, *affiliates*, *associates* and *volunteers*, as well as contractors and vendors, with access to those resources. Students are strongly encouraged to implement passwords on personal systems. *University* computer account owners have a responsibility to construct, secure, and maintain their passwords in accordance with the requirements specified in the Password Construction and Maintenance Guideline (IS-G703).

6. Account Management

All *networked devices* with access to *university resources* shall implement the following account management practices where possible:

6.1.1. Accounts shall be configured to lock after repeated login failures.

6.1.2. Accounts shall be deactivated after termination of a user's employment or separation of a user's affiliation.

6.1.3. Accounts shall be assigned to a single individual. The use of group accounts is highly discouraged. If you use a group account it must be affiliated with a responsible individual.

6.1.4. Account holders are responsible for any activity initiated from their account.

6.1.5. Accounts shall be created with the minimum amount of access necessary to meet the needs of the account holder. Access requirements should be reviewed for changes regularly.

More information on account management can be found in Management Responsibilities for Information Security Standard (IS-S400).

7. Encrypted Authentication

All *networked devices* should use only *encrypted authentication* mechanisms. In particular, historically insecure services such as Telnet, FTP, SNMP, POP, and IMAP should be replaced by their *encrypted* equivalents.

More information on encrypted authentication can be found in item #7 of the Minimum Security for Networked Devices Implementation Guideline (IS-G602A) and the Encryption Standard (IS-S303).

8. Email Relays and Proxy Servers

When possible, system administrators should migrate to user-authenticated SMTP services. University *devices* must not provide an active SMTP service that allows unauthorized third parties to relay e-mail messages.

Software program default settings in which web or email proxies are automatically enabled must be identified and reconfigured to prevent unauthorized use.

More information on email relays and proxy servers can be found in item #8 of the Minimum Security for Networked Devices Implementation Guideline (IS-G602A).

9. Session Controls

Devices must be configured to "lock" or logoff and require a user to re-authenticate if user leaves device unattended. The following time limits are recommended maximums:

Category	Time	Action
Private Office Workstation	20 minutes	Lock
Cubicle/Shared-Office Workstation	15 minutes	Lock
Multiple-User Workstation	10 minutes	Lock / Logoff*
Monitored Computer Lab	10 minutes	Lock / Logoff*
Public Use Computer Lab	5 minutes	Logoff
Research Lab Workstation	15 minutes	Lock
Data Collection Devices	5 minutes	Lock
Physically Secured Servers	10 minutes	Lock
Physically Accessible Servers	5 minutes	Lock

* At *units'* discretion

More information on session controls can be found in item #9 of the Minimum Security for Networked Devices Implementation Guideline (IS-G602A).

10. Physical Security

Mission-critical *devices* and/or *devices* containing *confidential university data* must be located in a locked location accessible only to authorized personnel

For additional requirements applicable to *units*, see the FRS Departmental Manual Policy 15.40, Security and Control of Theft Loss.

11. Services and Protocols

Services or protocols that are unnecessary for the operation of a device should be disabled or removed. Assistance identifying services running on a device may be obtained by contacting the Network Technology Services – Security Operations Group (NTS-SecOps).

More information on services and protocols can be found in item #11 of the Minimum Security for Networked Devices Implementation Guideline (IS-G602A).

Related Guidance

Information Security Policy (IS-100)
Information Security Terms Guideline (IS-G100)
Exceptions Procedure (IS-P100)
Encryption Standard (IS-S303)
Minimum Security for Networked Devices Implementation Guideline (IS-G602A)
Software Patching Guideline (IS-G602B)
Antivirus Software Guideline (IS-G602C)
Spyware and Adware Prevention Guideline (IS-G602D)
Firewall Software Guideline (IS-G602E)
Server Security Standard (IS-S603)

Information System Activity Review Procedure (IS-G603)
Access Control Standard (IS-S702)
UA NetID Password Standard (IS-S703U)
Password Construction and Maintenance Guideline (IS-G703)

All *italicized terms* used in this standard are defined in the Information Security Terms Guideline (IS-G100).

Revision History

Initial Draft:	08/09/07
Effective Date:	05/27/08
Revision (only new numbering):	08/22/12
Effective Date:	11/26/12