

Information & Technology Services Internet-Accessible Server Security Standard

Scope

This standard applies to all Internet-accessible servers that are connected to the Minnesota State University, Mankato network and accessed via the University firewall.

Standard

- **Contact:** Information & Technology Services will maintain a record of the responsible party for each server and which services have been opened for that server. The responsible party must notify ITS of changes in the server's requirements and changes in contact information. ITS will contact the responsible party annually to confirm that the requirements have not changed.
- **Network Identity:** All servers must have fixed IP addresses, assigned by DHCP, and must have DNS entries. Static IP addresses may be set on machines that do not support DHCP.
- **Software Maintenance:** All servers must be maintained with operating system and application patches in accordance with MnSCU System Guidelines [1].
- **Passwords:** All servers must be configured with password requirements adhering to the ITS Secure Password Standard [2].
- **Vulnerability Assessment:** All servers must be free of vulnerabilities ranked medium or greater as detected by the latest version of Nessus, Nikto, or other vulnerability management software. ITS will regularly perform vulnerability scans of servers that are open to the Internet.
- **Non-public Data:** Servers that facilitate credit card transactions or store non-public personal data (as defined by FERPA [3], HIPAA [4], MGDPA [5], and the PCI DSS [6]) in a location accessible to multiple simultaneous Internet users must adhere to the following requirements:
 - Access to the server must be protected by user authentication and session encryption.
 - A root/administrator level account must be provided to Information & Technology Services for credentialed vulnerability management testing.
 - The server's network configuration must ensure that all inbound and outbound traffic will be inspected for malware, protocol violations, and intrusion attempts by a separate device that has the ability to block these threats proactively such as the ITS application-layer firewall.
- **Establishment of Firewall Rules:** Information & Technology Services will open firewall connections for servers based on the service that is requested if the server is compliant with every applicable item in this standard.

- Where practical, inbound firewall connections must be configured to accept connections from a white list of known good IP addresses.
- ICMP echo, TCP port 22 (SSH), TCP port 80 (HTTP), and TCP port 443 (HTTPS) will be opened as requested.
- TCP port 25 (SMTP) will be opened only if the server is not configured as an open SMTP relay and is approved by the ITS email administrator.
- TCP and UDP port 53 (DNS) will be opened only if the server is not configured to perform recursive lookups and is approved by the ITS networking group.
- Remote Desktop ports, such as those required for VNC, RDP, or PcAnywhere, will be opened only if:
 - Configured to allow remote log on for specific accounts rather than all accounts on the server.
 - Configured to encrypt the authentication and session data.
- TCP port 21 (FTP), and TCP port 23 (Telnet) will be opened in the rarest of circumstances and will require an exception to this standard.
- Other ports not listed above will be opened if doing so is judged to be safe by the Information Security Manager, or a member of the networking group.
- For connectivity testing, all inbound ports to a server may be allowed for short-period tests lasting no longer than one week.
- **Removal of Firewall Rules:** Information & Technology Services will close firewall openings for the following reasons:
 - If no response is received from the responsible party within three weeks of sending notification of an annual audit.
 - If the server does not comply with this standard or where an obvious security flaw exists. In most cases, ITS will attempt to notify the responsible party prior to removing firewall openings.
 - If the server is exposing non-public data or is being used for illegal activities.

Authority

Information & Technology Services System Hardening Policy
<URL to be added when the final location is settled>

References

[1] MnSCU ITS Standard 5.23.C, Security Patch Management.
<http://its.mnscu.edu/security/standardsguidelines/patchstandard523C.pdf>

[2] Information & Technology Services Secure Password Standard
<http://www.mnsu.edu/its/security/Secure%20Password.pdf>

[3] Family Educational Rights and Privacy Act
<http://www.law.cornell.edu/uscode/20/1232g.html>

[4] Health Insurance Portability and Accountability Act

<http://www.cms.hhs.gov/HIPAAgenInfo/Downloads/HIPAALaw.pdf>

[5] Minnesota Government Data Practices Act

<https://www.revisor.leg.state.mn.us/statutes/?id=13>

[6] Payment Card Industry Data Security Standard

<https://www.pcisecuritystandards.org/>