Network Security Checklist

By Alex Strickland

- ☐ General
  - ☐ Develop a Security Policy detailing rights and responsibilities of staff, patrons, and contract users
  - ☐ Develop a Acceptable Use Policy (AUP) developed for patrons and staff
  - ☐ Train staff not to reveal system passwords to anyone other than specified individuals
  - ☐ Train staff not to allow anyone access to systems and network equipment without authorization
  - ☐ Require companies performing maintenance/configuration to sign a disclosure agreement
- ☐ Physical & Data Security
  - ☐ Lock servers and network equipment.
  - ☐ Rotate one backup set offsite regularly and store in a secure location
  - ☐ Secure Keys used for securing equipment or media
  - ☐ Keep computers visible
  - ☐ Use locks on computer cases
  - ☐ Perform regular inspections.
- ☐ Password Security
  - ☐ Develop written password security policy
  - ☐ Develop written instructions in creating strong passwords
  - ☐ Store password documentation in secure location
- ☐ Workstation Security
  - ☐ Require logon at each workstation
  - ☐ Configure workstations with private IP addresses to be either static or dynamic
  - ☐ Remove unnecessary/unused files and programs
  - ☐ Install anti-virus software on all workstations
  - ☐ Schedule anti-virus software Updates 2 times per week
  - ☐ Schedule software updates 1 time per week
  - ☐ Schedule Operating System updates 1 time per week.
  - ☐ Install Pop up blockers
- ☐ LAN/Domain Server Security

- ☐ Remove unnecessary services
- ☐ Remove unnecessary files/programs
- ☐ Configure file system with proper file/folder access permissions
- ☐ Disable anonymous user logon information
- ☐ Configure account policy to restrict unauthorized logon attempts
- ☐ Block account after too many failed logon attempts
- ☐ Create administrators to perform different functions
- ☐ Limit remote administrator rights
- ☐ Disable administrator rights on remote server
- ☐ Configure Remote Access Service security
- ☐ Rename Administrator Account
- ☐ Configure auditing of Administrator account logon attempts
- ☐ Set a strong password for current administrator/root account
- ☐ Use different passwords for domain/server accounts than for local workstation accounts
- ☐ Restrict access permissions for the Everyone group
- ☐ Disable Guest account if enabled
- ☐ Create appropriate user and group accounts
- ☐ Set appropriate group access permissions
- ☐ Configure audit logs to track unauthorized access to files/folders/accounts
- ☐ Schedule periodic download and installation of operating system patches

☐ Network Equipment Security

- ☐ Record and secure any password settings created by staff or contractor
- ☐ Configure audit logs properly, if available
- ☐ Schedule periodic installation of firmware updates

☐ Router/Firewall Security

- ☐ Use firewall; public services (web/ftp/e-mail) are provided on separate network segment, the DMZ
- ☐ Implement network address translation (NAT), if possible
- ☐ Configure router to deny inbound access to unused ports
- ☐ Configure firewall so no packets with source addresses outside the LAN are allowed into the LAN, but only to DMZ

- ☐ Firewall uses stateful packet inspection, providing protection against denial-of-service attacks and IP spoofing
- ☐ Schedule periodic installation of firmware updates