intelliarts

Technical Audit Checklist

Alerts

- □ Unauthorized system access alert
- □ Unplanned system modifications alerts
- □ System or physical security instruction alerts
- □ Alerts monitored 24/7

Accounts

- □ Dormant accounts removed after deactivation
- □ Account information transmitted via encrypted format only
- □ Admin privileges granted on an as-needed basis

Hardware

- □ All devices have password-protected screen locks
- □ All devices meet minimum hardware requirements for security programs to run properly
- □ Owned devices are inventoried and tracked

Network firewall

- □ Installed and active
- □ Updated regularly
- □ Includes intrusion detection and prevention systems (IDS/IPS)

Anti-virus software

- □ Installed and active on all devices
- □ Updated regularly
- □ Patches installed and configured properly immediately after incident

Passwords

- □ Passwords are encrypted
- □ Passwords require alphabetic, numeric, and symbolic characters
- □ Passwords must be changed every 3 months
- □ Accounts lock after set number of invalid login attempts
- □ Group passwords are not permitted

Physical security

- □ All company properties have locks on all windows and doors
- □ All company properties have full security camera coverage at office
- □ Mobile hardware is locked and checked in and out for use
- □ Mobile hardware have remote wipe software installed in case of theft
- □ Remote employees' home networks meet minimum security requirements

Image source: purshology.com