Cyber Security Checklist

Please refer to these as guidelines of things to think about.

Most systems will not use every item listed.

- ☐ Assign static IP addresses
- ☐ Set strong admin password
- ☐ Create user-level accounts with least privileges required with strong passwords
- ☐ Update firmware to the latest version
- ☐ Enable SSL encryption
- ☐ Disable guest login/unauthenticated RTSP connections
- ☐ Update system clock/NTP, DST, time zone
- ☐ Enable multicast only if needed
- ☐ Enable DDNS only if needed
- ☐ Enable bonjour only if needed
- ☐ Enable UPnP only if needed
- ☐ Enable link-local address only if needed
- ☐ Enable FTP only if needed
- ☐ Enable e-mail notifications only if needed
- ☐ Enable QoS only if needed
- ☐ Enable 802.1x certificate-based access control
- ☐ Enable SD card recording
- ☐ Enable tamper detection
- ☐ Enable network disconnect detection if using low voltage power
- ☐ Enable SNMP v3 or disable all versions if not needed
- ☐ Check device logs
- ☐ Ensure cameras are on a separate network from corporate/production network/Internet
- ☐ Enable VLANs on network
- ☐ Enable IP Filtering
- ☐ Change default ports from well-known ports to high ports
- ☐ Ensure camera is out of reach, cables are protected
- ☐ Document configuration and create an export/backup
- ☐ Save a snapshot of camera view
- ☐ Place a recognizable setting to indicate tampering/defaulting
- ☐ Utilize VPN for remote access
- ☐ Configure port forwarding for the least number of devices/ports needed
- ☐ Use proprietary video file format for SD recording and exporting video
- ☐ Ensure all network switches, NVRs/VMS, & PoE midspans/injectors are protected by a UPS