

# Security Audit – Risk Assessment

Goal: Implement “Reasonable Security” to attempt to prevent or deter breaches, prepare for the inevitable breach, and be prepared to defend the security in-place.

- Security AUP
- Password Access Control
- BYOD
- Etc.

## Policies/Procedures

## Security Policy / Plan

## Training

- Annual
- All, from leadership on down
- Bi-weekly reminders
- Live v. online training
- Effective training

## Standards: Govt. & Commercial

- FIPS
- ISO
- NIST
- PCI
- HIPAA
- Etc.

## Cyber-Security

## Physical-Security

## Technology / IT

## Technology / Integrator

- Firewalls
- Routers
- Anti-virus
- Access control
- IPS / IDS
- Etc.

- Locks
- IP Cameras
- DVR / Video
- Sensors
- Guards
- Monitoring
- Surveillance
- Etc.

- Device Password Security (Changing Defaults)
- Adding Encryption
- Use of Hardening Guides
- Upgrading Firmware
- Manufacturers Warning Reports
- Using Cyber Security Designed Products
- Secure On-Line Support

## Threats

- Botnets
- Malware
- Viruses
- Vulnerabilities
- Zero-day attacks
- User error
- Negligence

- Botnets
- Malware
- Viruses
- Vulnerabilities
- Zero-day attacks
- User error
- Negligence