TECHVFY

IT AUDIT CHECKLIST

System Security

Physical Security

□ Have locks on all company properties.
□ Have all security cameras in place.
□ Lock all mobile hardware with check-in/out system.
□ Have remote wipe software on all mobile devices.

Accounts

□ Remove all dormant accounts.
□ Encrypt transmitted account information.
□ Selectively grant Admin privileges.

Anti-virus

□ Active on all devices.
□ Regular updates.

Hardware

□ All devices are password-protected.
□ All hardware devices meet minimum security requirements.
□ Devices are inventoried and tracked.

Alerts

□ Unauthorized access alerts.
□ System modification alerts.
□ Monitor alerts 24/7.

Passwords

□ Encrypted passwords.
□ Make sure passwords has many requirements.
□ Regular password changes.
□ Account lock after invalid attempts.

Network Firewall

□ Active and regularly updated.
□ Intrusion detection.

IT AUDIT CHECKLIST

Standards and procedures

Backups

- □ Daily critical data backups.
- □ Regular backup validation.

Employee Requirements

- □ Background checks.
- □ Security policy acknowledgment.
- □ Annual security training.

Document Disposal

- □ Shred all sensitive documents.
- □ Store all shredded documents and disposed professionally.
- □ Factory reset all devices before changing user or being thrown.

Disaster Recovery

- □ Documented emergency plan.
- □ Annual emergency response training.
- □ Defined emergency chain of command.

Performance & System Management

Documentation & Reporting

- □ Secured IT logs.
- □ Weekly log reviews.
- □ Incident reports with detailed records.

Cost & Network Performance

- □ Monitor IT expenses.
- □ Track network speeds and outages.

System Development

- □ Comprehensive testing.
- □ Documented implementation process.
- □ Documented post-implementation review.

Storage & Utilization

- □ Monitor RAM, hard drive, and cloud storage utilization.