# IT Audit Checklist

## System security

### Anti-virus software
- Installed and active on all devices
- Updated regularly
- Patches installed and configured properly immediately after incident

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

### 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

### 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

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

## 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 devices have remote wipe software installed in case of theft
- Remote employees' home networks meet minimum security requirements

## Alerts
- Unauthorized system access alert
- Unplanned system modifications alerts
- System or physical security intrusion alerts
- Alerts monitored 24/7
IT Audit Checklist

Standards and procedures

**Employee requirements**
- Background checks required for system access
- Employees must acknowledge and sign security policy agreement before receiving access to secure systems
- Employees must participate in annual security awareness and training

**Disaster recovery and incident response**
- Business emergency plan is documented, updated regularly, and disseminated with all employees, third-party vendors, and partners
- Employees undergo emergency response training annually
- Emergency chain of command is clear and emergency roles are well-defined

**Document disposal**
- All sensitive physical documents are shredded when no longer needed
- Shredded documents are stored in a locked container and disposed of professionally
- All devices are factory reset before changing users or being thrown out/sold/donated

**Backups**
- Critical data backed up daily
- Backups checked and validated regularly
- Files are backed up in 2+ separate places

**Documentation and reporting**

**Security protocols**
- Documented formally
- Updated regularly and after system modifications and security events
- Disseminated to all employees, third-party vendors, and partners

**IT logs**
- Secured in a way that prohibits tampering
- Reviewed at least once per week
- Retained for at least 6 months

**Incident reports**
- Incident descriptions, times, and dates recorded
- Causes and solutions recorded and procedures updated if necessary
- Business impact assessed for each incident
# IT Audit Checklist

## Performance monitoring

### Outages
- Outage frequency (planned and unplanned)
- Mean time to resolve
- Mean time between failures
- Total infrastructure downtime
- Total system downtime
- Downtime by service

### Storage and utilization
- RAM utilization
- Hard drive storage utilization
- Cloud storage utilization

### Network performance
- Upload speeds
- Download speeds
- Network latency

### Cost
- Total IT expenses
- IT expenses per employee
- Cost per user
- Cost per unit asset (e.g. data storage)

## Systems development

### Design and development
- Review process for determining system development needs
- System design and development procedures are adequate, well-documented, and followed
- Approvals are required at appropriate stages in the development process
- Data entry documents are accurate and comprehensive

### Testing
- Tests are comprehensive and sufficiently rigorous
- System and program testing is implemented correctly

### Implementation
- Review procedures for program implementation
- Implementation process is documented and standards are followed
- Changes are properly approved
- Appropriate controls are in place to maintain security during and after implementation
- Post-implementation review process is documented and standards are followed