Tax Ready Bookkeeping

IT Security Basics Checklist

Tax Ready Bookkeeping | projectbits.com/taxready

Overview

Financial data requires protection. This checklist covers fundamental IT security measures every business should implement, regardless of size.

Section 1: Authentication

Password Requirements

Requirement	Standard	Your Status
Minimum length	12+ characters	[ ] Met
Complexity	Mixed case, numbers, symbols	[ ] Met
No reuse	Last 10 passwords	[ ] Met
Maximum age	90 days (or use password manager)	[ ] Met
No sharing	Never	[ ] Met

Two-Factor Authentication (2FA)

Required on ALL financial systems:

System	2FA Enabled?	Method
QuickBooks Online	[ ] Yes	App / SMS / Email
Bank accounts (all)	[ ] Yes	App / SMS / Token
Payroll system	[ ] Yes	
Bill pay platform	[ ] Yes	
Credit card portals	[ ] Yes	
Email accounts	[ ] Yes	
Password manager	[ ] Yes	

Authentication Best Practices

- ☐ Unique passwords for each system (use password manager)
- ☐ No passwords written on sticky notes or near computers
- ☐ No passwords shared via email or text
- ☐ Password manager used (e.g., 1Password, LastPass, Bitwarden)
- ☐ Recovery options documented securely

Section 2: Access Control

User Access Management

For each financial system, document:

User	System	Role	Access Level	Last Review
			Admin / User / View	
			Admin / User / View	
			Admin / User / View	

Access Control Checklist

- ☐ Each user has unique login (no shared accounts)
- ☐ Access limited to job requirements (least privilege)
- ☐ Admin access restricted to essential personnel
- ☐ Guest/temporary access time-limited
- ☐ Access reviewed quarterly

Termination Procedure

When an employee leaves: - [ ] All system access disabled within 24 hours - [ ] Passwords changed on any shared accounts (shouldn't have any) - [ ] Company devices returned - [ ] Building/physical access revoked - [ ] Documented and logged

---

Section 3: Device Security

Computer Security

Requirement	Status
Operating system updated	[ ] Yes
Antivirus/anti-malware installed	[ ] Yes
Automatic updates enabled	[ ] Yes
Firewall enabled	[ ] Yes
Screen locks automatically (5 min)	[ ] Yes
Full disk encryption enabled	[ ] Yes
Login password required	[ ] Yes

Mobile Device Security

Requirement	Status
Device passcode/PIN (6+ digits)	[ ] Yes
Biometric lock (fingerprint/face)	[ ] Yes
Remote wipe capability	[ ] Yes
Automatic updates enabled	[ ] Yes
Financial apps use separate PIN	[ ] Yes
No jailbroken/rooted devices	[ ] Yes

Wi-Fi Security

☐ Office Wi-Fi uses WPA3 or WPA2 encryption
☐ Wi-Fi password is strong and not publicly shared
☐ Guest network separate from business network
☐ No financial work on public Wi-Fi without VPN
☐ VPN used when working remotely

Section 4: Email Security

Email Protection

Measure	Implemented?
Spam filtering enabled	[ ] Yes
Malware scanning on attachments	[ ] Yes
DMARC/DKIM/SPF configured	[ ] Yes
Phishing awareness training	[ ] Yes
Suspicious email reporting process	[ ] Yes

Email Security Practices

☐ Don't click links in unexpected emails
☐ Verify unusual requests by phone (not reply email)
☐ Don't open attachments from unknown senders
☐ Report suspected phishing to IT/manager
☐ Never send passwords, SSNs, or account numbers via email

Phishing Red Flags

- Sender address slightly different from normal
- Urgent language ("act now", "account suspended")
- Generic greeting ("Dear Customer")
- Requests for passwords or sensitive info
- Links to unfamiliar websites
- Poor grammar or spelling
- Unexpected attachments

Section 5: Data Backup

Backup Requirements

Data Type	Backup Frequency	Retention	Status
QuickBooks file	Daily	30 days	[ ] Yes
Documents/receipts	Daily	90 days	[ ] Yes
Email	Continuous	1 year	[ ] Yes
Full system	Weekly	4 weeks	[ ] Yes

Backup Best Practices

☐ Backups stored offsite or in cloud
☐ Backups encrypted
☐ Backups tested monthly (can you restore?)
☐ Multiple backup copies (3-2-1 rule)
☐ Backup status monitored

3-2-1 Backup Rule

- 3 copies of data
- 2 different storage types
- 1 copy offsite/cloud

Section 6: Physical Security

Office Security

Measure	Status
Doors locked when unattended	[ ] Yes
Server/network equipment secured	[ ] Yes
Check stock locked	[ ] Yes
Sensitive documents secured	[ ] Yes
Visitor sign-in/escort required	[ ] Yes
Security cameras (if applicable)	[ ] Yes

Clean Desk Policy

☐ No sensitive documents visible on desks
☐ Computer screens locked when away
☐ Sensitive documents shredded (not trashed)
☐ Portable devices secured when not in use

Section 7: Software Security

Software Requirements

Requirement	Status
Only authorized software installed	[ ] Yes
Software from legitimate sources only	[ ] Yes
Automatic updates enabled	[ ] Yes
Unused software removed	[ ] Yes
Browser extensions vetted	[ ] Yes

Software Inventory

List all software with access to financial data:

Software	Purpose	Version	Update Status
			Current / Outdated
			Current / Outdated
			Current / Outdated
			Current / Outdated

Section 8: Incident Response

If You Suspect a Security Incident

Immediate Actions: 1. [ ] Don't panic 2. [ ] Disconnect affected device from network (if active attack) 3. [ ] Document what you observed 4. [ ] Report to manager/IT immediately 5. [ ] Don't try to "fix it yourself"

Incident Contacts

Contact	Name	Phone	Email
IT Support			
Management			
Bank (fraud line)			
Cyber insurance			
Law enforcement	Local police		

Types of Incidents

- Phishing email clicked
- Malware/virus detected
- Suspicious login attempt
- Lost/stolen device
- Data breach suspected

- Ransomware
- Unauthorized access

Section 9: Training

Security Awareness Training

Training Topic	Frequency	Last Completed
Password security	Annual	
Phishing recognition	Quarterly	
Physical security	Annual	
Device security	Annual	
Incident reporting	Annual	

Training Checklist

☐ All employees complete security awareness training
☐ Training documented and tracked
☐ Refresher training provided annually
☐ New hires trained during onboarding
☐ Simulated phishing tests conducted

Section 10: Compliance

Security Documentation

Document	Exists?	Last Updated
Acceptable use policy	[ ] Yes	
Password policy	[ ] Yes	
Data classification policy	[ ] Yes	
Incident response plan	[ ] Yes	
Backup and recovery plan	[ ] Yes	

Regular Reviews

Review	Frequency	Last Completed
Access rights	Quarterly	
Software updates	Monthly	
Backup testing	Monthly	
Security policies	Annually	
Incident response plan	Annually	

Quick Security Checklist

Daily

- ☐ Systems locked when away
- ☐ Suspicious emails reported
- ☐ Backups running

Weekly

- ☐ Software updates installed
- ☐ No unauthorized devices
- ☐ Physical security check

Monthly

- ☐ Test backup restoration
- ☐ Review access logs
- ☐ Security news review

Quarterly

- ☐ Access rights review
- ☐ Phishing test
- ☐ Policy review

Annually

- ☐ Full security assessment
- ☐ Policy updates
- ☐ Training refresh

Assessment Completed By:

Date:

Next Review Date:

For more resources: projectbits.com/taxready/ch8

Tax Ready Bookkeeping by Don Lovett | ProjectBits Consulting

Tax Ready(TM) Bookkeeping