COMPLIANCE CHECKLIST FOR SMALL BUSINESSES

This checklist is designed to give you a clear picture of where your business stands with compliance and data protection. You don't need to check every box — most small businesses won't, and that's completely normal. The goal is simply to help you spot gaps early, understand your biggest risks, and know where to focus your efforts.

If you're not sure about an item, leave it blank and we can walk through it together. If something truly doesn't apply to your business, just draw a line through it.

1. Access Control & User Management

☐ All staff have individual logins (no shared accounts)
☐ Strong passwords or passphrases are required
☐ MFA (multi-factor authentication) is enabled for critical systems
☐ Accounts are disabled immediately when someone leaves
☐ Access is based on job roles ("least privilege")
☐ Administrative access is limited and reviewed regularly

2. Device & Network Security

☐ All computers and devices have updated antivirus/EDR
☐ Firewalls are properly configured and monitored
☐ Wi-Fi networks are secured and separated (guest vs. internal)
☐ Devices automatically lock after inactivity
☐ Operating systems and software are regularly updated
☐ Remote access is secured through VPN or approved tools

3. Data Protection & Encryption

☐ Sensitive data is encrypted at rest and in transit
☐ Backups run automatically and are tested regularly
☐ File sharing uses approved tools (not personal email or texting)
☐ Data retention rules are documented and followed
☐ Confidential data is stored only on approved systems
☐ Old devices and documents are securely disposed of

4. Policies & Documentation

☐ Written Information Security Program (WISP) is created and maintained
☐ Password policy is documented and enforced
☐ Acceptable Use Policy (AUP) is provided to all employees
☐ Remote work and device policies exist
☐ Incident Response Plan is documented and accessible
☐ Vendor management or third-party risk process exists
☐ Policies are reviewed annually and updated as needed

5. Employee Training & Awareness

☐ Staff receive regular cybersecurity training
☐ New hires complete security onboarding within first week
☐ Phishing awareness training is ongoing
☐ Employees know how to report suspicious activity
☐ Annual refresher training is documented
☐ Leadership reinforces secure behavior

6. Compliance Requirements (If Applicable)

☐ HIPAA safeguards are documented and followed
☐ FERPA protections are in place for student information
☐ PCI DSS requirements are met for credit card processing
☐ Business Associate Agreements (BAAs) are current (healthcare)
☐ Compliance documentation is stored securely and updated
☐ Annual or quarterly risk assessments are completed

7. Cyber Insurance Requirements

☐ MFA is enabled everywhere required by your carrier
☐ Backups meet insurer specifications
☐ Required policies exist (WISP, Incident Response, etc.)
☐ Logging and monitoring tools are enabled
☐ Annual risk assessment supports renewal questionnaires
☐ Security controls are reviewed before submitting an application

8. Incident Preparedness

☐ Staff know whom to contact in an incident
☐ Your Incident Response Plan is tested annually
☐ Communication steps are documented
☐ Backups can be restored quickly
☐ Critical systems have redundancy
☐ Roles and responsibilities are clearly defined

Assessment Scoring Instructions

If you'd like to get a quick sense of your overall compliance posture, you can score your checklist results. This isn't a formal audit — it's simply a way to understand your risk level at a glance.

1. **Count the number of items you checked.**
   Each checkmark represents a safeguard your business already has in place.
2. **Skip any items you drew a line through.**
   Those do not count for or against your score.
3. **Leave blank anything you're unsure about.**
   Unanswered items usually highlight areas worth reviewing.
4. **Use the chart below to understand where you stand**
   - **0–20 items checked:** High risk — major gaps likely
   - **21–35 items checked:** Moderate risk — good foundation, needs improvement
   - **36–45 items checked:** Low risk — strong compliance posture

Your score isn't a grade — it's simply a starting point. If you'd like help interpreting it or filling in the blanks, we're happy to walk through it with you.