CORPORATE TECHNOLOGIES LLC
gocorptech.com

CYBERSECURITY FOR ACCOUNTING FIRMS CHECKLIST

Executive Tool for Risk Control & Client Trust

Built for accounting firm leaders and IT decision-makers. Use this checklist to assess cybersecurity posture and reduce client data risk.

How to Use

1. Takes 20–30 minutes
2. Check each box that applies
3. Count the total number of checked items
4. Identify security exposure and control gaps

1

Security Program & Policies

- ☐ Document written cybersecurity policies
- ☐ Define password and authentication standards
- ☐ Publish acceptable use policy for users
- ☐ Document remote work security protocols
- ☐ Establish patch and update policies
- ☐ Assign ownership for policy enforcement

2

Access & Identity Controls

- ☐ Require multi-factor authentication for all users
- ☐ Use centralized identity provider (SSO)
- ☐ Enforce role-based access permissions
- ☐ Audit inactive or orphaned accounts regularly
- ☐ Review privileged accounts quarterly
- ☐ Document account lifecycle process

3

Endpoint Security & Protection

- ☐ Ensure all endpoints have up-to-date antivirus
- ☐ Deploy EDR agents
- ☐ Enable device encryption
- ☐ Configure consistent security configurations
- ☐ Track patch deployment progress
- ☐ Document unmanaged devices

4

Network Security Controls

- ☐ Configure next-gen firewall
- ☐ Segment sensitive networks
- ☐ Encrypt traffic with SSL/TLS where possible
- ☐ Monitor firewall logs for anomalies
- ☐ Disable unused network ports/services
- ☐ Validate remote access configurations

5 Monitoring, Detection & Response

- ☐ Deploy real-time security monitoring tools
- ☐ Enable alerting for suspicious activity
- ☐ Log security events for audit purposes
- ☐ Test incident response process periodically
- ☐ Document incident escalation procedures
- ☐ Review alerts and response logs monthly

6 Third-Party Risk Management

- ☐ Document all third-party service providers
- ☐ Confirm cybersecurity controls of vendors
- ☐ Validate vendor data handling contracts
- ☐ Audit third-party access to systems
- ☐ Track vendor security incidents
- ☐ Document mitigation steps for vendor risks

Scoring Model

- Count the total number of checked items
- Total Possible Score: 36
- 0–12 → High Risk
- 13–29 → Moderate Risk
- 30–36 → Controlled / Secure

Immediate Red Flags

- No written cybersecurity policies
- No multi-factor authentication
- Endpoints without up-to-date protection
- No real-time monitoring enabled
- No incident response process documented
- No third-party risk evaluation

Next Step

If your score indicates exposure, schedule a Cybersecurity Readiness Assessment.

Cybersecurity Readiness Assessment