Phone: (877) 807-1332
www.xsolutions.com

Cybersecurity Audit Checklist

Start Date: **End Date:**

1. General Security Measures	Complete?
Acceptable Use Policy (AUP): Is there a clearly defined and enforced AUP for all staff?	☐
Regular Security Training: Do employees receive ongoing cybersecurity training (e.g., phishing awareness, password management)?	☐
Access Control: Are user accounts reviewed periodically to ensure proper access levels and deactivation of inactive accounts?	☐
Multi-Factor Authentication (MFA): Is MFA implemented for all sensitive systems, including email and cloud portals?	☐
Password Policies: Are strong password policies enforced (e.g., complexity, unique passwords)?	☐

2. Network Security	Complete?
Firewall Configuration: Is a next-generation firewall and high-availability (secondary) firewall in place and properly configured to block unauthorized access?	☐
Wi-Fi Security: Is Wi-Fi secured with the latest encryption, and are there separate networks for employee phones and guest access?	☐
VPN for Remote Work: Is a Virtual Private Network (VPN) used for secure remote access?	☐
Network Monitoring: Are tools in place to monitor network traffic and detect anomalies?	☐
Secure Communication: Are email communications encrypted (e.g., TLS, S/MIME)?	☐

3. Device Security	Complete?
Antivirus/Anti-Malware: Are all devices protected with up-to-date antivirus and anti-malware software?	☐
Device Encryption: Are laptops, smartphones, and other devices encrypted to protect data in case of loss or theft?	☐
Patch Management: Are operating systems, software, and firmware regularly updated and patched across all devices?	☐
Managed Detection and Response (MDR): Are advanced MDR solutions in place for real-time threat detection and resolution?	☐

4. Data Security	Complete?
Data Backup: Are regular, automated backups performed for critical files and systems?	☐
Backup Testing: Are backups tested periodically to ensure they can be restored successfully?	☐
Data Classification: Is sensitive data identified, classified, and stored securely?	☐
Client Data Access: Are access permissions for client files limited to only those who need them?	☐
Secure Disposal: Are old devices and files disposed of securely (e.g., shredding, degaussing)?	☐

5. Threat Detection and Response	Complete?
Incident Response Plan: Is there a documented plan for responding to cyber incidents?	☐
Security Information and Event Management (SIEM): Is a SIEM solution in place to detect and alert on potential threats?	☐
Ransomware Protection: Are anti-ransomware measures implemented and tested?	☐
Penetration Testing: Is penetration testing conducted to identify vulnerabilities?	☐
Security Incident Drills: Are employees trained on and tested for incident response protocols?	☐

6. Physical Security	Complete?
Secure Office Access: Is office access restricted through keycards, biometric locks, or similar methods?	☐
Server Room Security: Is the server room locked, climate-controlled, and monitored?	☐
Document Security: Are sensitive physical documents stored in locked cabinets and shredded when no longer needed?	☐

7. Ongoing Maintenance	Complete?
Quarterly Reviews: Are cybersecurity policies and procedures reviewed quarterly?	☐
Annual Risk Assessment: Is an annual risk assessment conducted to address evolving threats?	☐
Cybersecurity Insurance: Is the firm covered by a comprehensive cybersecurity insurance policy?	☐
IT Budget Review: Is there sufficient allocation of funds for IT security improvements?	☐

Next Steps:

After completing this checklist, prioritize addressing any unchecked items. For assistance, schedule a **Free Cybersecurity Assessment** with us to identify and resolve gaps in your security posture.

You can always reach us at (877) 807-1332.