Cyber Security Checklist

From Small Biz Tipster

1. Asset Management

Inventory of Assets: Maintain an up-to-date inventory of all hardware, software, and data.
Asset Classification: Classify assets based on their sensitivity and importance to the business.

2. Access Control

User Access Review: Regularly review and audit access rights to ensure least privilege access.
Strong Authentication: Implement Multi-Factor Authentication (MFA) for all critical systems.
Password Policies: Enforce complex, unique passwords with expiration policies.
Account Management: Disable or remove accounts and access for terminated employees immediately.

3. Network Security

Network Segmentation: Isolate critical systems from general user networks.
Firewall Configuration: Ensure firewalls are properly configured, and rules are regularly reviewed.
Intrusion Detection and Prevention Systems (IDPS): Deploy and maintain IDPS to monitor network

4. Endpoint Security

Antivirus/Anti-malware: Ensure all endpoints have up-to-date antivirus software.
Endpoint Detection/Response (EDR): Implement EDR solutions for advanced threat detection.
Patch Management: Regularly update operating systems, applications, andfirmware

5. Data Protection

Encryption: Encrypt data at rest and in transit, especially sensitive information.
Data Backup: Implement and test regular backups in secure, off-site locations.
Data Loss Prevention (DLP): Use DLP tools to prevent data exfiltration.

6. Incident Response

Incident Response Plan: Develop, document, and regularly update an incident response plan.
Response Team: Establish an incident response team with defined roles and responsibilities.
Regular Drills: Conduct tabletop exercises to test and improve the incident response process.

7. Security Awareness and Training

Employee Training: Conduct regular cybersecurity training focusing on phishing, password management, and social engineering.
Phishing Simulations: Run phishing simulation exercises to assess employee awareness.

8. Physical Security

Secure Physical Access: Control physical access to server rooms, data centers, and any areas housing sensitive equipment.
Visitor Management: Implement a visitor policy to prevent unauthorized access.

9. Application Security

Secure Coding Practices: Implement and enforce secure coding practices in software development.
Code Audits: Regularly audit code for vulnerabilities, especially before deployment.

10. Compliance and Policies

Policy Development: Have clear policies for acceptable use, data protection, remote access, etc.
Compliance Checks: Ensure compliance with relevant standards like GDPR, HIPAA, regulations.
Third-Party Risk Management: Assess and manage the cybersecurity risks posed by third-party vendors.

11. Monitoring and Logging

Log Management: Collect, monitor, and analyze logs from all systems and applications for anomalies.
Security Information and Event Management (SIEM): Use SIEM tools for real-time analysis of security alerts generated by network hardware and applications.

12. Continual Improvement

Security Assessments: Perform regular security assessments, penetration testing, and vulnerability
Risk Assessments: Conduct periodic risk assessments to identify new threats and vulnerabilities.

13. Recovery

Disaster Recovery Plan: Develop and test a disaster recovery plan to ensure business continuity.
Business Continuity Planning: Ensure plans are in place for the continuation of essential functions in the face of cyber disruptions.