CodeBlue technology

CYBER SECURITY CHECKLIST

For Business Owners

Network Security □

- Implement a firewall with intrusion detection and prevention systems (IDPS).
- Regularly update firewall firmware and security configurations.
- Segment networks to minimize the impact of breaches.
- Enable logging and monitoring of network traffic.

Endpoint Protection □

- Deploy endpoint protection software (antivirus/antimalware) on all devices.
- Ensure endpoint software is regularly updated and centrally managed.
- Implement endpoint detection and response (EDR) solutions for advanced threat detection.

Patch Management □

- Establish a patch management process for operating systems and applications.
- Automate patch deployment where possible to reduce vulnerabilities.

Multi-Factor Authentication (MFA) / Two-Factor Authentication (2FA) □

- Enable MFA/2FA for all critical systems and applications.
- Educate employees on the importance of MFA/2FA and how to use it securely.

Data Backup and Recovery □

- Implement regular automated backups of critical business data.
- Store backups securely (encrypted and offsite) to protect against ransomware and data loss.
- Test backup restoration procedures periodically.

Cyber Liability Insurance □

- Evaluate the need for cyber liability insurance based on business operations and data sensitivity.
- Review coverage options to ensure they align with potential cyber risks and financial exposure.

Email Security □

- Implement email filtering to block phishing attempts and malware attachments.
- Educate employees on recognizing phishing attacks and suspicious emails.
- Consider using DMARC, SPF, and DKIM protocols to authenticate outgoing emails.

Secure Wi-Fi and VPN □

- Secure Wi-Fi networks with strong encryption (e.g., WPA3) and unique passwords.
- Use VPNs (Virtual Private Networks) for remote access to internal networks and sensitive data.

Web Security □

- Use web filtering to block access to malicious websites and content.
- Regularly update web server software and apply security patches.

Employee Training and Awareness □

- Conduct regular cybersecurity awareness training for employees.
- Educate employees on recognizing social engineering tactics and cybersecurity best practices.

Incident Response Plan □

- Develop an incident response plan outlining steps to take in case of a cybersecurity breach.
- Conduct tabletop exercises to test the incident response plan and train staff on their roles.

Access Control □

- Implement the principle of least privilege for access to systems and data.
- Use strong, unique passwords for all accounts and enforce password policies (e.g., length, complexity).

Encryption □

- Encrypt sensitive data both at rest and in transit using strong encryption algorithms.
- Ensure encryption keys are managed securely and rotated periodically.

Vendor Security □

- Assess the cybersecurity posture of third-party vendors and service providers.
- Include cybersecurity requirements in vendor contracts and agreements.

Compliance and Regulations □

- Stay compliant with relevant data protection regulations (e.g., GDPR, CCPA).
- Conduct regular audits to ensure compliance and address any gaps.

Mobile Device Security □

- Implement mobile device management (MDM) solutions for company-owned devices.
- Enforce security policies for BYOD (Bring Your Own Device) scenarios.

Cloud Security □

- Secure cloud services and applications with strong authentication and access controls.
- Encrypt data stored in the cloud and monitor for unauthorized access.

Disaster Recovery Planning □

- Develop and maintain a disaster recovery plan for IT systems and data.
- Test disaster recovery procedures regularly to ensure readiness.

Physical Security □

- Secure physical access to IT infrastructure, data centers, and server rooms.
- Implement CCTV/IP Cameras, access control systems, and visitor logs for restricted areas.

Continuous Change Monitoring and Improvement □

- Implement continuous security monitoring for networks, systems, and applications.
- Regularly review and update cybersecurity policies, procedures, and controls.

CodeBlue Technology supports businesses in all industries, sizes and locations around the United States. Our mission is to delivery positively memorable technical service while improving your businesses health in the data landscape.

Our team of solutions engineers, networking technicians and business professionals are here to guide, coach and implement a strategy that best suits your needs. If you or any member of your team would like a free consultation, please consider CodeBlue Technology for all of your IT needs.

You can visit us around the web @CodeBlueTech
Or (804) 521-7660

Contact Sales today at Sales@codebluetechnology.com