Cybersecurity Security Assessment Checklist

Use this checklist to assess your organization's cybersecurity posture and identify areas for improvement.

1. Governance & Policies

- ☐ Have you defined your organization's cybersecurity policies and procedures?
- ☐ Do you have a designated cybersecurity team or individual responsible for managing security?
- ☐ Is your cybersecurity policy regularly updated to reflect new threats and technologies?
- ☐ Are employees trained on your organization's cybersecurity policies and best practices?

2. Network & Infrastructure Security

- ☐ Are all network devices (routers, switches, firewalls, etc.) secured and monitored?
- ☐ Do you use firewalls and intrusion detection systems (IDS) to protect your network?
- ☐ Are your wireless networks encrypted and protected by strong passwords?
- ☐ Is remote access to your network restricted and monitored?
- ☐ Have you segmented sensitive parts of your network (e.g., customer data, financial records)?

3. Endpoint Protection

- ☐ Are all endpoints (computers, mobile devices, IoT devices) regularly updated with the latest patches?
- ☐ Do you have antivirus or anti-malware software installed on all devices?
- ☐ Are devices configured to require strong passwords or biometric authentication?
- ☐ Is data on devices encrypted to protect against theft or loss?
- ☐ Do you have a mobile device management (MDM) system in place to secure employee devices?

4. Data Protection & Encryption

- ☐ Is sensitive data encrypted both at rest and in transit?
- ☐ Are backups of critical data performed regularly, and are they securely stored?
- ☐ Do you have a data retention and disposal policy to ensure that old, unnecessary data is securely destroyed?
- ☐ Are encryption keys and credentials securely managed and periodically rotated?

5. Identity & Access Management

- ☐ Are employees required to use multi-factor authentication (MFA) for accessing sensitive systems?
- ☐ Do you have a process for managing user access and permissions based on roles?
- ☐ Are accounts with elevated privileges regularly reviewed and monitored?
- ☐ Are dormant or unused accounts disabled promptly?

6. Application Security

- ☐ Are security patches for applications and software applied as soon as they are released?
- ☐ Have you conducted a vulnerability scan on your web applications (e.g., SQL injection, cross-site scripting)?
- ☐ Are third-party applications and plugins used on your network properly vetted for security risks?
- ☐ Do you have a secure software development lifecycle (SDLC) for custom applications?

7. Incident Response & Recovery

- ☐ Do you have an incident response plan that outlines how to handle different types of cyber incidents?
- ☐ Are all employees aware of the steps to take in the event of a cyberattack?
- ☐ Do you perform regular drills to ensure that your incident response plan is effective?
- ☐ Are you able to recover critical data quickly from backups in case of an attack or disaster?

8. Cloud Security

- ☐ Do you understand your responsibilities under the shared responsibility model for cloud security?
- ☐ Are your cloud services configured securely (e.g., preventing public access to storage buckets)?
- ☐ Is access to cloud resources controlled and monitored using strong authentication methods?
- ☐ Are sensitive data and applications hosted in the cloud encrypted and regularly tested for vulnerabilities?

9. Employee Awareness & Training

- ☐ Do all employees receive cybersecurity training as part of their onboarding process?
- ☐ Is cybersecurity training updated regularly to cover new threats like phishing and social engineering?
- ☐ Do employees know how to recognize phishing emails and other common cyber threats?
- ☐ Are regular security awareness campaigns or drills conducted to test employees' preparedness?

10. Compliance & Legal Considerations

- ☐ Are you compliant with relevant cybersecurity regulations (e.g., GDPR, HIPAA, PCI-DSS)?
- ☐ Do you have a process for documenting and reporting data breaches, as required by law?
- ☐ Are third-party vendors and partners assessed for cybersecurity risks and compliance?
- ☐ Do you regularly audit your cybersecurity policies to ensure ongoing compliance with legal requirements?

Next Steps:

✅ Review your answers and identify areas that need improvement.

✅ Prioritize critical vulnerabilities and assign resources to address them.

✅ Work with cybersecurity professionals, if needed, to develop or strengthen your security measures.