CYBERSECURITY FOR EVERYONE

CYTAD

Cybersecurity Checklist for Small businesses

For easy audits and compliance

SANTOSH KAMANE

Cybersecurity Checklist	Response		
	Yes	No	N/A
1. Security Policies and Procedures:			
1.1. Have you reviewed and updated security policies and procedures regularly?			
1.2. Have you developed an incident response plan?			
1.3. Do you have defined roles and responsibilities for security incidents?			
1.4. Is there an active security awareness training program for employees?			
1.5. Have all employees signed security policy acknowledgment forms?			
2. Access Control:			
2.1. Is there a strong password policy in place?			
2.2. Do you enforce multi-factor authentication for sensitive accounts?			
2.3. Are access permissions regularly reviewed and updated?			
2.4. Are inactive accounts disabled or removed?			
2.5. Is administrative access restricted to authorized personnel only?			
2.6. Do you monitor and log user access and activities?			
3. Network Security:			
3.1. Are firewalls installed and configured?			
3.2. Are intrusion detection and prevention systems (IDS/IPS) in place?			
3.3. Is there regular scanning and patching of network vulnerabilities?			
3.4. Is network segmentation used to isolate critical assets?			
3.5. Are network equipment and software regularly updated and patched?			
4. Endpoints and Devices:			
4.1. Is endpoint security (antivirus, anti-malware) deployed?			
4.2. Is device encryption enforced for laptops and mobile devices?			
4.3. Are all endpoints regularly updated and patched?			
4.4. Are there secure data wiping capabilities for lost or stolen devices?			

4.5. Are application whitelisting and blacklisting policies enforced?			
5. Data Protection:			
5.1. Is sensitive data encrypted at rest and in transit?			
5.2. Is data regularly backed up, and data restoration procedures tested?			
5.3. Is access to sensitive data limited to a need-to-know basis?			
5.4. Is data loss prevention (DLP) technology in place?			
5.5. Are proper data disposal procedures implemented?			
6. Email and Communication:			
6.1. Are secure email gateways used?			
6.2. Are employees trained to recognize phishing and social engineering attempts?			
6.3. Is email encryption implemented for sensitive communication?			
6.4. Are email server software and configurations regularly updated?			
6.5. Are email retention policies enforced?			
7. Web Security:			
7.1. Are web application firewalls (WAFs) installed and updated?			
7.2. Are web applications scanned for vulnerabilities?			
7.3. Are secure coding practices followed?			
7.4. Are web server logs regularly monitored and audited?			
7.5. Are SSL/TLS protocols used for secure web connections?			
8. Wireless Security:			
8.1. Are Wi-Fi networks secured with strong encryption?			
8.2. Are default router passwords changed?			
8.3. Are guest and internal Wi-Fi networks segmented?			
8.4. Is scanning conducted for rogue access points?			
8.5. Is physical access to network infrastructure limited?			
9. Vendor and Third-Party Risk:			
9.1. Do you assess the security practices of third-party vendors?			
9.2. Are security requirements established in vendor contracts?			

9.3. Is third-party access regularly reviewed and audited?			
9.4. Is monitoring in place for data breaches or incidents involving vendors?			
9.5. Is there a process for swift vendor termination in case of security concerns?			
10. Physical Security:			
10.1. Is physical access to data centres and server rooms secured?			
10.2. Are surveillance and alarm systems in place?			
10.3. Are laptops and mobile devices secured against theft?			
10.4. Are hardware assets regularly inventoried and tracked?			
10.5. Are access control measures established for physical access?			
11. Cloud Security:			
11.1. Is due diligence conducted before selecting cloud providers?			
11.2. Are cloud security best practices implemented?			
11.3. Is data in cloud storage encrypted?			
11.4. Are cloud access permissions regularly reviewed?			
11.5. Is cloud usage monitored for unusual activity?			
12. Training and Awareness:			
12.1. Are employees provided with regular security training?			
12.2. Are employees tested with simulated phishing attacks?			
12.3. Is there a security-conscious culture promoted?			
12.4. Are resources available for employees to report security concerns?			
12.5. Are training materials updated based on evolving threats?			
13. Incident Response:			
13.1. Is there an incident response plan with defined roles?			
13.2. Are communication protocols established for security incidents?			
13.3. Is the incident response plan tested with simulations?			
13.4. Is there an incident log for post-incident analysis?			

13.5. Is the incident response plan continuously improved?			
14. Compliance and Regulations:			
14.1. Are relevant data protection regulations identified?			
14.2. Is compliance maintained with GDPR, HIPAA, or other applicable laws?			
14.3. Are security practices documented for compliance audits?			
14.4. Is legal and compliance guidance sought for adherence to changing regulations?			
14.5. Are security measures regularly updated to align with changing regulations?			
15. Monitoring and Alerts:			
15.1. Is a Security Information and Event Management (SIEM) system implemented?			
15.2. Are network and system logs monitored for unusual activity?			
15.3. Are automated alerts set up for potential security incidents?			
15.4. Are security logs regularly reviewed and analyzed?			
15.5. Is there a response plan for different types of security alerts?			
16. Secure Development:			
16.1. Are secure coding practices implemented in software development?			
16.2. Are security code reviews and testing conducted?			
16.3. Are software applications regularly updated and patched?			
16.4. Are applications tested for known vulnerabilities?			
16.5. Is there a secure development lifecycle (SDLC) process in place?			
17. Backup and Recovery:			
17.1. Is critical data and systems regularly backed up?			
17.2. Are backups stored offsite or in the cloud?			
17.3. Are data restoration procedures tested?			
17.4. Is there redundancy for critical systems?			
17.5. Is a disaster recovery plan in place?			
18. Mobile Device Security:			
18.1. Are Mobile Device Management (MDM) solutions implemented?			

18.2. Is device encryption enforced on mobile devices?			
18.3. Are employees educated on mobile security best practices?			
18.4. Are mobile device software regularly updated?			
18.5. Are remote wipe capabilities configured for mobile devices?			
19. IoT Device Security:			
19.1. Are IoT devices secured with strong passwords and encryption?			
19.2. Are IoT devices segmented from critical networks?			
19.3. Are IoT device firmware regularly updated?			
19.4. Are unnecessary features on IoT devices disabled?			
19.5. Are IoT device security and behaviour monitored and assessed?			
20. Secure Social Media Usage:			
20.1. Are employees educated on safe social media practices?			
20.2. Are guidelines established for sharing company information on social media?			
20.3. Is social media monitored for mentions of the company?			
20.4. Are privacy settings for social media profiles regularly updated?			
20.5. Is there a response plan for social media incidents?			
21. Cyber Insurance:			
21.1. Have you considered cyber insurance to mitigate financial risks?			
21.2. Have you reviewed and understood the terms and coverage of the insurance policy?			
21.3. Is the policy updated to reflect changes in the organization's security posture?			
21.4. Is the cyber insurance policy communicated to relevant stakeholders?			
21.5. Is there collaboration with the insurer on security and incident response?			

CYber Thinkers Advisors Doers

@CYTAD

CYTAD - WA Channel

Follow CYTAD on Linkedin for cyber-security advisories, data privacy services, checklists mentoring, services, insights and much more

SANTOSH KAMANE