Ntiva

Your Success. Secured.

CHECKLIST

Cybersecurity Best Practices

Protect Your Business

Businesses face an ever-growing number of cyber threats that can compromise their data, disrupt operations, and damage their reputation. Whether you're a small business or a large enterprise, having strong cybersecurity protocols in place is critical for protecting your company from these risks. This checklist provides a practical guide to the essential cybersecurity best practices every organization should follow to stay secure and resilient in the face of evolving threats.

Instructions for Using the Checklist:

1. Print the checklist and go through each best practice to assess your current cybersecurity posture.
2. Check 'Yes' if the practice is already implemented in your organization.
3. Check 'No' if the practice is missing and needs immediate attention.
4. Check 'Need to Improve' if some elements are in place, but there's room for improvement.
5. Use the Comments/Notes section to add specific details or next steps or each practice.

BEST PRACTICE	YES	NO	NEED TO IMPROVE	COMMENTS/NOTES
1. Strong Password Policies				
Are passwords at least 12 characters long with a mix of letters, numbers, and symbols?				
Is multi-factor authentication (MFA) implemented for all critical accounts?				
Are passwords changed regularly, and are employees discouraged from sharing passwords?				

BEST PRACTICE	YES	NO	NEED TO IMPROVE	COMMENTS/NOTES
2. Data Backup Strategy				
Is critical data backed up regularly and stored securely?				
Are backups isolated from the main network to prevent ransomware attacks?				
Are backups tested periodically to ensure data recovery works?				

BEST PRACTICE	YES	NO	NEED TO IMPROVE	COMMENTS/NOTES
3. Software Updates & Patching				
Are all systems and software updated regularly with the latest patches?				
Is patching automated to prevent delays in applying security updates?				

BEST PRACTICE	YES	NO	NEED TO IMPROVE	COMMENTS/NOTES
4. Security Audits				
Are regular security audits performed to identify potential vulnerabilities?				
Are access controls reviewed regularly to ensure only authorized personnel have access to sensitive information?				

BEST PRACTICE	YES	NO	NEED TO IMPROVE	COMMENTS/NOTES
5. Employee Education & Training				
Is cybersecurity training conducted regularly for all employees?				
Are employees trained to recognize phishing attempts, AI-driven social engineering, and suspicious emails?				

BEST PRACTICE	YES	NO	NEED TO IMPROVE	COMMENTS/NOTES
6. Network Security				
Are firewalls installed and configured to monitor network traffic?				
Are VPNs and encryption used for secure remote access and data transmission?				
Is network segmentation implemented to limit access to sensitive areas?				

BEST PRACTICE	YES	NO	NEED TO IMPROVE	COMMENTS/NOTES
7. Endpoint Protection				
Is antivirus and anti-malware software installed on all devices?				
Are endpoint detection and response (EDR) solutions deployed to detect and mitigate threats?				

BEST PRACTICE	YES	NO	NEED TO IMPROVE	COMMENTS/NOTES
8. Monitoring & Logging				
Are logs enabled across systems to monitor for suspicious activity?				
Are alerts set up for unusual behaviors such as unauthorized access attempts?				

BEST PRACTICE	YES	NO	NEED TO IMPROVE	COMMENTS/NOTES
9. Incident Response Plan				
Is there a defined incident response plan in place for handling security breaches?				
Are incident response simulations conducted to ensure readiness?				

BEST PRACTICE	YES	NO	NEED TO IMPROVE	COMMENTS/NOTES
10. AI-Driven Threat Detection				
Are AI-driven threat detection tools being utilized to analyze data and identify emerging threats?				
Is AI being used to detect anomalies and unusual patterns that human eyes may miss?				

BEST PRACTICE	YES	NO	NEED TO IMPROVE	COMMENTS/NOTES
11. Zero Trust Architecture				
Has a Zero Trust security model been implemented to ensure strict identity verification for every user and device?				
Are systems segmented and are users given the minimum access necessary?				

BEST PRACTICE	YES	NO	NEED TO IMPROVE	COMMENTS/NOTES
12. Remote Work & Hybrid Security				
Is there a clear policy and security framework for remote and hybrid workers?				
Are remote workers using secure, monitored networks and devices?				

BEST PRACTICE	YES	NO	NEED TO IMPROVE	COMMENTS/NOTES
13. Cloud Security Measures				
Are proper security configurations in place for cloud services used by the company?				
Are data encryption and secure access management in place for cloud environments?				

BEST PRACTICE	YES	NO	NEED TO IMPROVE	COMMENTS/NOTES
14. AI-Based Phishing Detection Tools				
Are AI-driven phishing detection tools in place to identify and block sophisticated phishing attempts?				

Want to ensure your business is fully protected? Don't wait until it's too late.

Schedule a free cybersecurity consultation with Ntiva today and let us help you build a comprehensive security strategy to safeguard your company from cyber threats.

Request a Free Consultation

Ntiva