

10 Basics for Businesses Cyber Security

Protect your business from cyber threats with these 10 essential cybersecurity practices designed to safeguard your data, systems, and operations. By implementing these proactive measures, you can minimize risks, prevent breaches, and ensure your company remains secure in an increasingly digital world.

1

PURCHASE A CYBER INSURANCE POLICY

Secure financial protection against cyber incidents, ensuring your business can recover swiftly from potential breaches.

2

IDENTIFY, BACKUP OFFLINE, AND TEST RESTORES ON ALL MISSION-CRITICAL DATA

Safeguard essential data by creating offline backups and regularly testing restoration processes to ensure data integrity and availability.

3

STRONG MULTIFACTOR AUTHENTICATION ON ALL INTERNET ACCESSIBLE ACCOUNTS

Enhance security by requiring multiple verification methods for accessing sensitive accounts, reducing the risk of unauthorized access.

4

UPDATE OPERATING SYSTEMS, APPLICATIONS, AND FIRMWARE ON ALL DEVICES

Regularly update all systems to patch vulnerabilities and protect against the latest security threats.

5

INSTALL, UPDATE, AND MONITOR ENDPOINT SECURITY SOFTWARE ON ALL DEVICES

Deploy robust security software on all devices to detect, prevent, and respond to potential threats.

6

REMOVE ADMINISTRATIVE PRIVILEGES FROM ALL DAILY USE ACCOUNTS

Limit user permissions to reduce the risk of accidental or intentional system changes that could compromise security.

7

PERFORM REGULAR SECURITY AWARENESS TRAINING FOR ALL END USERS

Educate employees on cybersecurity best practices to prevent human errors that could lead to security breaches.

8

DEVELOP AN INCIDENT RESPONSE PLAN (WITH KEY CONTACTS AND CHANNELS)

Prepare for potential incidents with a detailed response plan, ensuring quick and coordinated action during a breach.

9

IMPLEMENT APPLICATION ALLOW LISTING

Restrict devices to run only pre-approved applications, minimizing the risk of malicious software execution.

10

IMPLEMENT A CYBERSECURITY FRAMEWORK (CIS, NIST, ASD-E8)

Adopt a recognized framework to establish comprehensive security measures and maintain regulatory compliance.