SMB Security Workplan

Addressing the items below will provide a strong security foundation for your business or organization.

This checklist will help you understand what policies and procedures should be implemented to keep your organization safe and secure. For more information, see the summaries below, or contact a team member at contact@axxys.com.

Privacy Program

- ☐  **01** Internal Privacy Policy
- ☐  **02** Train Employees On Your Policy
- ☐  **03** Data Retention Policy

Security Program

- ☐  **04** Security Awareness Training Of Employees And Contractors
- ☐  **05** Phishing Awareness Training
- ☐  **06** Clean Desk Policy
- ☐  **07** Visitor Program
- ☐  **08** Identify Digital Assets
- ☐  **09** Multi-factor Authentication (MFA)

Tools

- ☐  **10** Secure Remote Access
- ☐  **11** Secure Wi-Fi Network
- ☐  **12** Secure Email Gateway (SEG)
- ☐  **13** System Auditing
- ☐  **14** Backup Solution
- ☐  **15** Testing The Backup Solution

AXXYS TECHNOLOGIES

- [ ]  16 Domain Name Server (DNS) Level Content Filtering
- [ ]  17 Endpoint Detection And Response (EDR)
- [ ]  18 Security Incident And Event Management (SIEM) Solution

System Hardening

- [ ]  19 Remove Unused Programs On All Systems
- [ ]  20 Group Policies, Single Sign-On And Active Directory
- [ ]  21 Secure Endpoint Configurations
- [ ]  22 Implement Perimeter Security
- [ ]  23 Institute A Patch Management Plan
- [ ]  24 Monitor Cloud Application Behavior
- [ ]  25 Define a Process For Identifying And Addressing Vulnerabilities
- [ ]  26 Vulnerability Management Program

Response

- [ ]  27 Incident Response Policy
- [ ]  28 Incident Response Procedures
- [ ]  29 Identify Roles And Responsibilities

Vulnerability Management and Assessment

- [ ]  30 Business Continuity And Disaster Recovery
- [ ]  31 Incorporate Lessons Learned

Privacy Program

01 Internal Privacy Policy

Your company should document an internal privacy policy that covers network usage (including email), employee and client/customer records, and acceptable use for internal and external systems. This policy should cover all connected devices including mobile devices and those used in work-from-home or hybrid work environments. If customers or vendors interact with your network or digital properties, then you will need a public-facing privacy policy as well.

02 Train Employees On Your Policy

Training employees on your privacy and usage policy is imperative. Make sure they understand what is allowed and what is not when it comes to network usage or accessing data.

03 Data Retention Policy

Create a policy with rules and controls for how long your company will retain data, how it will be stored, and how it will be protected while in your care. A clear Data Retention Policy will reduce the impact of any potential security incidents.

Security Program

04 Security Awareness Training Of Employees And Contractors

Train employees and contractors on the most common cybersecurity and physical security threats to the business. This training should fit the needs of your organization and include training on the aforementioned policies and procedures.

05 Phishing Awareness Training

Train team members on how to identify potential phishing attacks. Additionally, implement a phishing reporting policy and train on how these potential attacks should be reported to within your organization.

06 Clean Desk Policy

Require that employees keep confidential information like customer information or passwords out of sight at all times at their workstations. This policy is designed to protect customers and employees alike by protecting sensitive data from prying eyes and prevents inadvertent leaks from shared workplace photos.

07 Visitor Program

Implement a clear policy around visitors and guests at the workplace. From personal guests to potential clients, your visitor policy should outline what areas of an office a guest may access, any badge or escort requirements, and how to sign in and sign out visitors. Train team members on this policy.

08 Identify Digital Assets

On a regular basis, and no less than once a year, take inventory of all digital assets and network devices. Identify potential areas of risk and vulnerability and the accompanying impact on the business in the event of a data breach.

09 Multi-factor Authentication (MFA)

Institute multi-factor authentication on all network devices and applications, particularly those that handle sensitive data like customer information or business intellectual property. MFA can include the use of a second device, like a mobile phone, to confirm that a system login is valid.

Tools

10 Secure Remote Access

Utilizing a Virtual Private Network (VPN) creates a secure connection between users and your network. A VPN is critical if you allow network connections outside of the office (as with work from home environments or remote workers). Setting up secure remote access via VPN, secure application tunneling, or remote desktops can create new efficiencies but must be done in a way that puts security front and center.

11 Secure Wi-Fi Network

Wi-Fi connectivity in the office should be established with separate guest and employee networks, regular password rotation/resets, and firmware updates. Wireless access points that use default or weak passwords and are not regularly updated create an easily accessed entry-point to your entire network.

12 Secure Email Gateway (SEG)

An SEG will include anti-phishing technology, encryption, and data-loss prevention features to keep your email secure. Even with increasingly sophisticated attacks targeting email, an SEG should keep most attackers at bay.

13 System Auditing

Enable logging across your network. Periodically review the logs to identify potential attack surfaces and even ongoing breaches. Many software and network providers include built-in reporting solutions to make accessing the logs simple.

14 Backup Solution

A robust backup solution can restore your business operations quickly in the event of a cyberattack. Remote (or even air-gapped) backups can mitigate the risk of ransomeware attacks and give your business continuity in the event of a breach.

15 Testing the Backup Solution

Regular verification of backups and regular testing of backup restoration further ensures that your data can be restored with minimal issues or data loss in the event of a breach.

16 Domain Name Server (DNS) Level Content Filtering

Content filtering at the DNS level can protect your network from SPAM or nefarious data packets. From adult content to suspicious IPs and activity, DNS-level content filtering will keep brute force and executable attacks away from your network.

17 Endpoint Detection And Response (EDR)

EDR means continuous monitoring and response to advanced threats. Threats that happen post-firewall or via authenticated users can be recognized and handled by an appropriate EDR solution.

18 Security Incident And Event Management (SIEM) Solution

SEIM solutions collect all alerts and security logs from connected devices to help identify potentially malicious behavior.

System Hardening

19 Remove Unused Programs On All Systems

Regularly audit which applications and systems are in use, including SaaS and PaaS tools. Remove or cancel any applications that are not in use as each connected application is a potential target for hackers seeking to do your business harm.

20 Group Policies, Single Sign-On And Active Directory

Instituting user policies by using Group Policy Objects (GPO), Microsoft Active Directory, or Single Sign-On gives administrative control over application and data access across your organization. Having these policies in place provides a layer of protection against not only external hackers but also disgruntled employees and other bad actors.

21 Secure Endpoint Configurations

Close unused ports and secure ports in use with firewalls and strong access controls. Endpoints are the literal entryway for bad actors intent on breaching your systems. Protecting these endpoints is a primary task in securing your network.

22 Implement Perimeter Security

Firewalls, VPNs, routers, and Intrusion Detection and Prevention systems should be installed, monitored, and regularly updated.

23 Institute A Patch Management Plan

The majority of software patches include a security element so leaving devices unpatched is dangerous. Plan for software updates and patch management by making it a regularly scheduled process that is the specific responsibility of a team or team member.

24 Monitor Cloud Application Behavior

Abnormal and anomalous behavior on cloud-based applications like Office 365 or your ERP system can be a sign of a bad actor. A number of software solutions exist to monitor applications and connected devices and notify your team in the event of abnormal activity.

25 Define a Process for Identifying And Addressing Vulnerabilities

When a vulnerability is detected or uncovered, it must be addressed in a timely manner. From unpatched systems to ongoing DDoS attacks, having a framework for how to respond to and address attempted attacks is critical.

26 Vulnerability Management Program

The software in use by your organization will include occasional “Bugs.” These bugs can often be exploited and compromise your network. Institute a plan for how to address software-based vulnerabilities with the software publisher. If a publisher will not address a Bug or provide support, consider replacing the software.

Response

27 Incident Response Policy

Set a policy for responding to any incident across the network. The policy should set the standard for employee and management behavior including severity rating of the incident, corrective action or remediation report framework, the scope of the policy, and the purpose and expected outcomes of following the policy.

28 Incident Response Procedures

A strict set of steps to follow in the event of an incident makes up the incident response procedures. This “playbook” for your Incident Response Policy will guarantee uniformity and consistency in how you address incidents.

29 Identify Roles And Responsibilities

The exact stakeholders and roles impacted by an incident should be identified and communicated with in the event of an incident. Guidelines around the identification and communication process will streamline incident response and reduce negative impacts.

Vulnerability Management and Assessment

30 Business Continuity And Disaster Recovery

Establish and test your business continuity and disaster recovery plan. This plan should touch not just technology and IT, but also HR, operations, finance, and other key components of your business. The continuity and disaster recovery plan should include a restore point objective (RPO) and restoration time objective (RTO).

31 Incorporate Lessons Learned

Planning, testing, and response will produce significant information and lessons for your entire business. Take note of what is learned, what works, and what needs to be improved. Incorporate these plans into the policies and guidelines above. Security is constantly evolving. Remain vigilant.