



# SMB1001- 2026 - Level 2 Silver

## Policies and Procedures



CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Prepared for:  
Client Company

Prepared by:  
YourIT Company



## Table of Contents

---

- 1 - Purpose
- 2 - Scope
- 3 - Sanctions/Compliance
- 4 - Domain 1 - Technology Management - Technology Management
- 5 - Domain 2 - Access Management - Access Management
- 6 - Domain 3 - Backup and Recovery - Backup and Recovery
- 7 - Domain 4 - Policies, Processes and Plans - Policies, Processes and Plans
- 8 - Domain 5 - Education and Training - Education and Training

## Purpose

---

SMB1001:2026 is a multi-tiered cybersecurity certification standard comprising five levels, each progressively increasing in complexity and maturity. This structure allows SMBs to begin at the level that best matches their current context and cybersecurity posture. They are not required to complete all five levels, providing flexibility in how they approach their cybersecurity journey.

Level 1 focuses on establishing basic preventive controls, such as firewalls and antivirus software, to stop potential threats before they can harm your system.

Level 2 introduces more advanced preventive measures, adding layers of protection against more sophisticated threats.

Level 3 expands to a holistic risk management approach, where risks related to people, processes, and technology are identified, assessed, and addressed in a coordinated manner.

Levels 4 and 5 advance to more complex governance procedures. This involves formal rules and policies for managing cybersecurity, alongside best practices in risk management.

This structured approach ensures that cybersecurity improvements are achievable without overwhelming resources, helping businesses meet contract requirements without unnecessary investment.

## Scope

---

The Level 2 tier is targeted at organizations that have achieved basic cyber hygiene and are seeking to further improve their cyber hygiene. They are familiar with cyber hygiene and are shifting into developing policies and procedures to support their cyber hygiene.

The key objective of the Level 2 tier is to ensure organizations can start formalizing their cybersecurity practices. This tier focuses on building on the measures in the Level 1 tier while starting to add in policies to formalize and support cyber hygiene that are most affordable for SMBs. In this tier, the focus is on initial policies that are considered achievable and essential for organizations less familiar with cyber hygiene.

The security measures for this tier are organized into four (4) categories with fourteen (14) measures in total.



## Sanctions/Compliance

---

Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

## Domain 1 - Technology Management - Technology Management

<p>SMB1001-2026 - Level 2 - Silver</p> <p>Domain 1 - Technology Management</p> <p>Technology Management</p>	<p><b>Other Requirements</b></p> <p>N/A</p>
---	---

### Policy

The organization will implement internal controls to satisfy the following requirement:

Ensure secure technology lifecycle management by implementing practices for timely patching, updates, and security testing.

### Guidance

The objective of this domain is to ensure that the organization has implemented practices to manage the security of their technology over their lifecycle. This includes ensuring there are sufficient capabilities to manage technology securely, installing patches and updates in a timely manner and testing the security of the technology/system.

### Responsibilities

The Security Officer is responsible for ensuring the implementation of this policy.

### Related Internal Controls

- SMB1001-1.1.0.0-2026 - Engage Technical Support Specialist: Engage a technical support specialist for your organization

#### Procedure

- o Identify and contract a qualified technical support specialist or IT professional who can provide ongoing assistance with daily cybersecurity tasks and help implement certification requirements.
- o Establish a schedule for regular consultations or support sessions with the specialist to ensure timely management of IT security needs without requiring full-time engagement.
- o Maintain clear communication channels and documentation of support activities to track progress and address emerging cybersecurity issues promptly.

- SMB1001-1.2.0.1-2026 - Firewall Installation Configuration: Install and configure a firewall

#### Procedure

- o Install a firewall at all network connection points to the Internet, including on personal devices used for organizational purposes, and configure it to block unauthorized access while allowing necessary traffic.
- o Ensure that all devices have their firewalls enabled, network sharing disabled, and that firewall passwords are changed from defaults to complex, phrase-based passwords.
- o Review firewall configurations either through a second-person technical review if done internally or by obtaining a formal attestation from an external provider to confirm secure and best-practice settings.

- SMB1001-1.3.0.1-2026 - Antivirus Installation on Devices: Install antivirus software on all organization devices

#### Procedure

- o Deploy and activate anti-malware software on all organizational endpoints, ensuring it is configured to receive automatic updates.
  - o Configure mobile devices to restrict app installations to official app stores and verify that built-in security features are enabled and operational.
  - o Regularly audit devices to confirm antivirus software is installed, active, and set to update automatically without user intervention.
- SMB1001-1.4.0.0-2026 - Automatic Software Updates: Automatically install tested and approved software updates and patches on all organization devices

Procedure

- o Configure all organization-owned devices and approved personal devices to enable automatic installation of tested and approved software updates and patches for operating systems and applications.
  - o For software or operating systems that do not support automatic updates, establish a documented schedule for manual updates to be performed by IT personnel at least once every three months.
  - o Maintain records of update installations and monitor compliance to ensure all devices receive timely updates according to the defined schedule.
- SMB1001-1.5.0.0-2026 - Install TLS Certificates: Install TLS certificates on all public internet-facing websites

Procedure

- o Obtain TLS certificates from a trusted Certificate Authority and configure them on all public internet-facing web servers to enable secure HTTPS connections.
  - o Regularly verify that all public websites have valid, unexpired TLS certificates installed and replace any certificates before they expire.
  - o Ensure that web server configurations enforce the use of TLS protocols and disable insecure protocols such as SSL or outdated TLS versions.
- SMB1001-1.6.0.1-2026 - Server Update Management: Ensure all servers are updated and patched

Procedure

- o Establish and document a maintenance schedule that ensures all servers, including on-premise, cloud-hosted, and externally provided servers, are reviewed and updated at least every six months, with critical patches applied within 14 days of release.
- o Include operating system updates and all essential software or applications in the patching routine to maintain server functionality and security.
- o If patching is outsourced, obtain written confirmation from the provider that their update process meets these timing and scope requirements and includes notification procedures before and after patching activities.

## References

- Dynamic Standards International - <https://dsi.org/>

## Domain 2 - Access Management - Access Management

<p>SMB1001-2026 - Level 2 - Silver</p> <p>Domain 2 - Access Management</p> <p>Access Management</p>	<p><b>Other Requirements</b></p> <p>N/A</p>
---	---

### Policy

The organization will implement internal controls to satisfy the following requirement:

Enforce authorized access through strong authentication practices, including multi-factor authentication.

### Guidance

The objective of this domain is to ensure that the organization has practices in place to ensure that only authorized access is allowed to the organization's systems. This includes ensuring that multi-factor authentication is enabled in addition to other authentication practices.

### Responsibilities

The Security Officer is responsible for ensuring the implementation of this policy.

### Related Internal Controls

- SMB1001-2.1.0.1-2026 - Maintain Strong Password Hygiene: Ensure strong password hygiene is maintained

#### Procedure

- Reset all default passwords on new devices before deployment and enforce password changes on all devices, including personal ones used for work, to comply with organizational security standards.
- Implement a password policy requiring long, unique, and unpredictable passwords that have not appeared in known data breaches, and ensure passwords are updated at least annually or immediately following any suspected or confirmed security incident.
- Secure all networking devices, including personal Wi-Fi used for work, with strong passwords and enforce password expiry policies to maintain ongoing password hygiene.

- SMB1001-2.2.0.0-2026 - Restrict Employee Admin Privileges: Ensure employee accounts do not have administrative privileges

#### Procedure

- Review all employee user accounts regularly to verify that administrative privileges are only assigned to those with a legitimate business need to install software or perform system changes.
- Configure user account permissions to restrict installation rights, ensuring that standard users cannot elevate their privileges on both local machines and domain environments.
- Implement a process for requesting and approving administrative access, and promptly remove such privileges when they are no longer required.

- SMB1001-2.3.0.0-2026 - Individual Employee Accounts: Ensure employees have individual user accounts

#### Procedure

- Assign a unique username and password to each employee for accessing all organizational systems, including workstations, laptops, servers, and cloud services.

- Implement a policy that explicitly prohibits sharing of usernames and passwords among employees and regularly communicate this policy to all staff.
  - Monitor and audit login activities to ensure that individual accounts are used exclusively by their assigned employees and investigate any anomalies promptly.
- SMB1001-2.4.0.1-2026 - Enterprise Password Manager: Implement a password manager system

Procedure

- Deploy a centrally managed password manager for all users with privileged access, ensuring it enforces multi-factor authentication and role-based access controls to restrict permissions appropriately.
  - Configure the password manager to allow secure credential sharing when necessary, maintain detailed audit logs of access and modifications, and integrate with existing data loss prevention or cloud security tools where possible.
  - Conduct regular training sessions for all users on secure credential practices, emphasizing the dangers of password reuse, recognizing phishing attempts, and proper use of the password manager according to organizational policies.
- SMB1001-2.5.0.0-2026 - Email Account Multi-Factor Authentication: Multi-factor authentication (MFA) on all employee email accounts

Procedure

- Configure the email system to require multi-factor authentication for all user accounts, ensuring that a second form of verification is mandatory during login.
- Verify that all administrator email accounts have MFA enabled and regularly audit these accounts to confirm compliance.
- Provide training and support to employees on how to set up and use MFA to reduce login issues and enhance security awareness.

- SMB1001-2.12.0.0-2026 - Email Authentication Controls: Email Authentication and Anti-Spoofing

Procedure

- Publish and maintain SPF records for all domains authorized to send organizational email, ensuring they accurately reflect current sending sources.
- Regularly review and update SPF configurations in coordination with technical support to accommodate changes in email infrastructure or third-party services.
- Monitor email delivery and spoofing reports to verify SPF effectiveness and promptly address any authentication failures or anomalies.

**References**

- Dynamic Standards International - <https://dsi.org/>

**Truncated Sample Document**