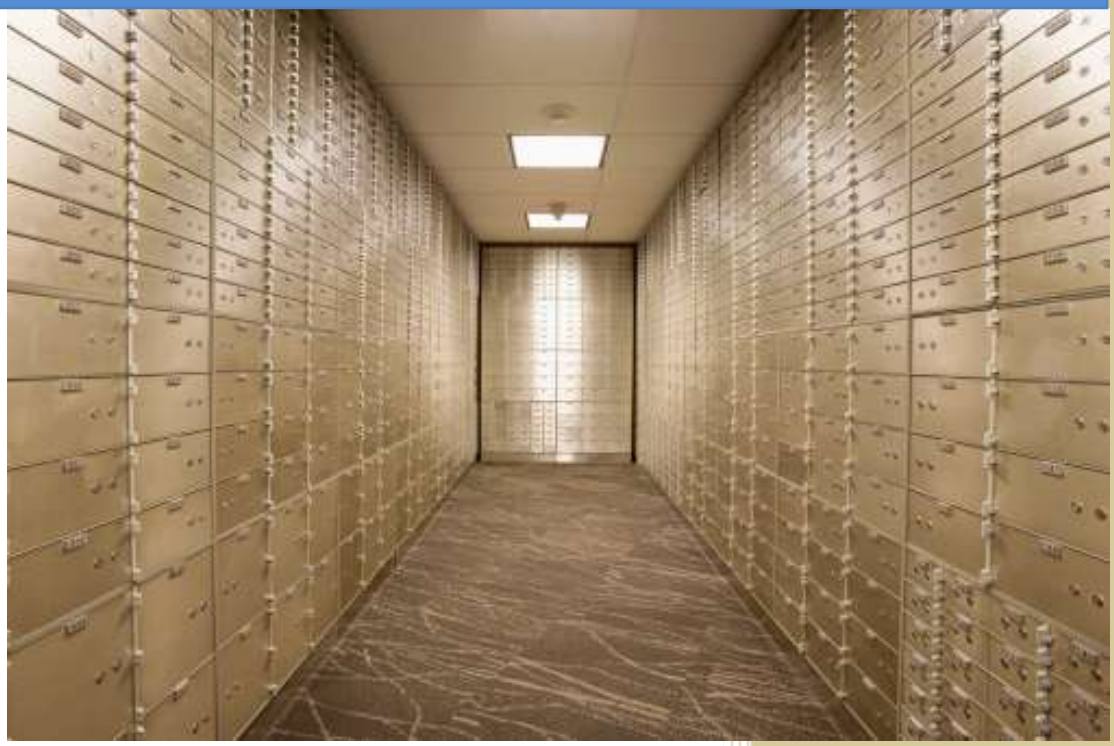
YourIT!
Your Logo Goes Here

SMB1001-2026 - Level 3 Gold

Policies and Procedures



Prepared for:
Client Company

Prepared by:
YourIT Company

Table of Contents

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 3 tier is targeted at organizations that have achieved advanced cyber hygiene and are seeking to further develop their cyber hygiene. They are familiar with cyber hygiene and are further implementing policies and procedures to develop a more mature cyber risk management approach. This includes developing their employee awareness of cyber threats.

The key objective of the Level 3 tier is to ensure organizations are developing clear policies to allow for proactive and regular management of their cyber hygiene. This tier focuses on further developing the policies defined in the Level 2 tier. In addition, some measures identified in earlier tiers are improved on in this tier to further enhance an organization's cyber hygiene. An additional measure is also added to develop cybersecurity awareness for employees.

The security measures for this tier are organized into five (5) categories. There are twenty-two (22) 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

SMB1001-2026 - Level 3 - Gold	Other Requirements
Domain 1 - Technology Management Technology Management	N/A

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
  - 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.
  - 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.
  - 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
  - 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.
  - Ensure that all devices have their firewalls enabled, network sharing disabled, and that firewall passwords are changed from defaults to complex, phrase-based passwords.
  - 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

- Deploy and activate anti-malware software on all organizational endpoints, ensuring it is configured to receive automatic updates.
- Configure mobile devices to restrict app installations to official app stores and verify that built-in security features are enabled and operational.
- 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
  - 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.
  - 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.
  - 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
  - Obtain TLS certificates from a trusted Certificate Authority and configure them on all public internet-facing web servers to enable secure HTTPS connections.
  - Regularly verify that all public websites have valid, unexpired TLS certificates installed and replace any certificates before they expire.
  - 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
  - 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.
  - Include operating system updates and all essential software or applications in the patching routine to maintain server functionality and security.
  - 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.

- SMB1001-1.12.0.0-2026 - Endpoint Detection Response: Implement Endpoint Detection and Response (EDR)

  Procedure
  - Deploy Endpoint Detection and Response software on all organizational workstations, laptops, and servers, ensuring it continuously collects and analyzes data such as process execution, network connections, and file changes.
  - Configure the EDR solution to detect threats based on behavioral patterns, enable automated or manual containment actions, and support forensic investigations with historical data access.
  - Set the EDR software to automatically update its software and threat intelligence definitions, and establish alerting mechanisms that notify designated technical personnel for prompt incident review and response.

References

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

Domain 2 - Access Management - Access Management

SMB1001-2026 - Level 3 - Gold Domain 2 - Access Management Access Management	Other Requirements N/A

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.

- SMB1001-2.4.1.1-2026 - Password Manager Implementation: Implement a password manager system

  Procedure
  - Deploy a centrally managed password manager for all employees who handle multiple credentials or access various systems, ensuring it supports role-based access control, comprehensive auditing, secure credential sharing, and requires multi-factor authentication for access.
  - Integrate the password manager with existing Data Loss Prevention or Cloud Access Security Broker tools where feasible, and provide mandatory training for all users on password reuse avoidance, phishing recognition, credential management basics, and proper use of the password manager in line with organizational policies.
  - For users with a single corporate identity, implement strong authentication methods such as Single Sign-On, passwordless authentication, or multi-factor authentication with phishing-resistant tokens to maintain secure access without requiring a password manager.

- 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.

- SMB1001-2.6.0.0-2026 - MFA for Business Applications: MFA on all business applications and social media accounts

  Procedure
  - Configure all business applications and social media accounts to require multi-factor authentication for both user and administrative logins, ensuring that the second factor is independent of the primary password.
  - Regularly review and update authentication settings to enforce MFA on any new or existing cloud-hosted applications and social media platforms used by the organization.
  - Provide training and support to users on how to set up and use MFA effectively to maintain secure access to all business-related accounts.

- SMB1001-2.7.0.1-2026 - RDP Over VPN Only: Ensure Remote Desktop Protocol (RDP) occurs only over Virtual Private Network (VPN) connections

  Procedure
  - Configure all Remote Desktop Protocol (RDP) access to require connection through a centrally managed Virtual Private Network (VPN) or an application-based proxy to ensure secure and controlled entry points.
  - Restrict RDP access permissions to the minimum necessary users and roles, applying the principle of least privilege to limit exposure and potential misuse.
  - Implement multi-factor authentication (MFA) for all VPN or proxy connections used for RDP access to add an additional layer of security beyond just username and password.

- SMB1001-2.12.1.0-2026 - Email Authentication Controls: Email Authentication and Anti-Spoofing

  Procedure
  - Publish and maintain SPF records in DNS that list all authorized email-sending services for each organizational domain, ensuring the records are valid and up to date.
  - Enable DKIM signing on all outbound emails using cryptographic keys of at least 1024 bits, preferably 2048 bits, to verify message integrity and authenticity.
  - Implement a DMARC policy in DNS with a reporting address, setting the policy to reject or quarantine unauthorized emails, and regularly review DMARC reports to fine-tune the policy and prevent legitimate email from being blocked.

References
- Dynamic Standards International - https://dsi.org/

Truncated Sample Document