YourIT!
Your Logo Goes Here

SMB1001-2026 - Level 5 Diamond

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 5 tier is targeted at organizations that have relatively mature cyber hygiene. They are very familiar with cyber hygiene and have implemented an advanced set of policies and procedures.

The key objective of the Level 5 tier is to extend the technical scope of the cyber hygiene.

This tier also amends existing measures defined in earlier tiers. Additional measures are also added to further protect the organization.

The security measures for this tier are organized into five (5) categories, with thirty-five (35) 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 5 - Diamond	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

- SMB1001-1.1.1.0-2026 - Engage Technical Support Specialist: Engage a technical support specialist for your organization

  Procedure
  - Identify and contract a qualified technical support specialist or IT service provider to assist with daily cybersecurity management and implementation of certification requirements, ensuring they have relevant expertise.
  - Develop and formalize a Service Level Agreement (SLA) with the chosen provider that specifies a maximum response time of 8 working hours for incident response support.
  - Regularly review and update the engagement terms and SLA to ensure ongoing alignment with organizational cybersecurity needs and incident response expectations.

- 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.

- SMB1001-1.7.0.1-2026 - Public Internet Resource Scanning: Ensure all public internet-facing resources are regularly scanned for vulnerabilities

  Procedure
  - Develop and maintain an inventory of all public internet-facing resources and classify them by risk level to determine appropriate scanning frequency based on sensitivity and criticality.
  - Implement a scheduled vulnerability scanning process that covers all identified resources according to their risk classification, ensuring scans occur at least weekly for high-risk, monthly for medium-risk, and quarterly for low-risk assets, with additional scans after significant changes.
  - If any public-facing resources are managed by external providers, obtain and document written confirmation that they perform regular vulnerability and malware scans in line with your organization's risk-based scanning schedule.

- SMB1001-1.8.0.0-2026 - Encrypt Important Data At-Rest: Ensure important digital data is encrypted at rest

  Procedure
  - Implement encryption protocols for all critical, confidential, sensitive, and personally identifiable data stored on servers, workstations, laptops, external storage devices, and cloud services to ensure data is protected at rest.
  - Configure personal devices used for business purposes to avoid local data storage by utilizing cloud-based storage solutions with secure access controls, and ensure these devices themselves are encrypted.
  - Regularly audit and verify that encryption measures are applied consistently across all storage locations containing important digital data to maintain compliance and data security.

- SMB1001-1.9.0.0-2026 - Application Execution Control: Implement application control

  Procedure
  - Develop and maintain a list of approved applications based on cryptographic hashes, publisher certificates, and trusted file paths, ensuring only these applications are permitted to execute on all organizational and personal devices.
  - Configure application control settings on all workstations and laptops to enforce execution restrictions using operating system features that validate applications against the approved list.
  - Regularly review and update the approved application list to accommodate new software requirements and remove unauthorized or outdated applications.

- SMB1001-1.10.0.0-2026 - Disable Untrusted Office Macros: Disable untrusted Microsoft Office macros

  Procedure
  - Configure Microsoft Office applications on all organizational devices to disable all macros or disable macros with notification, ensuring that enabling all macros is not permitted.
  - Regularly audit and verify macro settings on workstations, laptops, servers, and personal devices used for work to confirm compliance with the macro disabling policy.
  - Educate users about the risks of enabling macros and instruct them to report any prompts or requests to enable macros to the IT security team immediately.

- SMB1001-1.11.0.0-2026 - Penetration Vulnerability Testing: Conduct penetration, vulnerability and social engineering testing

  Procedure
  - Schedule an annual engagement with a qualified external provider to perform comprehensive penetration and vulnerability testing on your IT systems and infrastructure.
  - Include in the testing scope an assessment of employee susceptibility to social engineering attacks such as phishing, vishing, and attempts to bypass physical security controls.
  - Document the findings and remediation actions from each test cycle to track improvements and address identified weaknesses before the next annual assessment.

- SMB1001-1.12.1.0-2026 - Endpoint Detection and Response: (cont.)

  Procedure
  - Deploy Endpoint Detection and Response software on all organizational devices, including workstations, laptops, servers, and personal devices used to access company data, ensuring it continuously collects and analyzes endpoint activity.

- Configure the EDR solution to detect malicious behavior through behavioral analysis, enable automated or manual threat containment actions, support forensic investigations, and automatically update to maintain current threat intelligence.
- If internal Managed Detection and Response capabilities are not established, contract an external MDR provider with a formal Service Level Agreement that specifies response times for detection, investigation, and remediation aligned with any applicable cyber insurance requirements.

References

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

Domain 2 - Access Management - Access Management

SMB1001-2026 - Level 5 - Diamond	Other Requirements
Domain 2 - Access Management Access Management	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.

- SMB1001-2.5.1.0-2026 - MFA on Employee Emails: Multi-factor authentication (MFA) on all employee email accounts

  Procedure
  - Configure all employee email accounts to require multi-factor authentication using an Authenticator App, phone device, or U2F device as the second factor, including administrator accounts.
  - Disable SMS, voice, text, and email methods as backup or recovery options for MFA, ensuring these are not available for any account.
  - If backup codes are provided, print them and store them securely in a physical location, avoiding any digital storage or transmission.

- SMB1001-2.6.1.0-2026 - MFA for Business Applications: MFA on all business applications and social media accounts

  Procedure
  - Configure all user and administrator accounts on cloud-based business applications and social media platforms to require MFA using an Authenticator App, phone device, or U2F device as the second factor.
  - Disable SMS, voice, text, and email methods for MFA backup or recovery options across all accounts to ensure compliance with the control.
  - If backup codes are provided, print them and store them securely in a physical location, avoiding any digital storage or transmission.

- 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.

- SMB1001-2.8.0.0-2026 - Remote Cloud Credential Management: Management of remote access cloud credentials

  Procedure
  - Configure cloud IAM policies to enforce the principle of least privilege for all accounts, including administrators, and regularly review these permissions to ensure they remain appropriate.
  - Store all remote access credentials, such as SSH keys, in a centralized, secure repository separate from user devices, and restrict access to this repository based on role and necessity.
  - Integrate cloud platform authentication with the organization's identity management system to enable MFA using authenticator apps or hardware tokens, explicitly disabling SMS, voice, text, and email as second-factor methods, and securely print and store any backup codes offline.

- SMB1001-2.9.1.0-2026 - MFA for Important Data: MFA where important digital data is stored

  Procedure
  - Configure all systems storing critical or sensitive data to require multi-factor authentication using an authenticator app, phone device, or U2F device as the second factor for all user and administrator accounts.
  - Disable SMS, voice, text, and email as backup or recovery methods for MFA, ensuring only approved second factors are used.
  - If backup codes are provided, print them and store them securely in a physical location, avoiding any digital storage of these codes.

- SMB1001-2.10.1.0-2026 - VPN Multi-Factor Authentication: MFA on VPN connections

  Procedure
  - Configure all VPN access points to require multi-factor authentication using only authenticator apps, phone devices, or U2F devices as the second factor, regardless of whether the connection originates from the internet or the corporate network.
  - Disable and prevent the use of SMS, voice calls, text messages, and email as methods for second-factor authentication or account recovery on VPN connections.
  - If backup codes are provided for MFA, ensure they are printed and stored securely in a physical location, avoiding any digital storage or transmission.

- SMB1001-2.11.1.0-2026 - RDP Multi-Factor Authentication: MFA on RDP connections

  Procedure
  - Configure all RDP access points to require multi-factor authentication using an authenticator app, phone device, or U2F device as the second factor, regardless of whether the connection originates from the internet or the corporate network.
  - Disable SMS, voice calls, text messages, and email as methods for MFA backup or recovery to ensure only approved second-factor methods are used.
  - If backup codes are provided, print them and store them securely in a physical location, ensuring they are never saved in any digital format.

- 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/

Domain 3 - Backup and Recovery - Backup and Recovery

SMB1001-2026 - Level 5 - Diamond	Other Requirements
Domain 3 - Backup and Recovery Backup and Recovery	N/A

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

Maintain operational continuity during incidents by implementing backup policies and recovery practices.

Guidance
The objective of this domain is to ensure that the organization has practices in place to continue operating during instances of downtime or cyber incidents. This includes ensuring that there are policies relating to maintaining backups for systems.

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

Related Internal Controls

- SMB1001-3.1.1.1-2026 - Backup and Recovery Strategy: Implement a backup and recovery strategy for important digital assets

  Procedure
  - Develop and document a backup schedule that includes daily backups of all critical and sensitive digital assets, ensuring at least one offline copy is created and stored securely in a location physically or logically isolated from the business network.
  - Maintain a detailed register of all backup files, including their storage locations and access permissions, and ensure backups are retained for a minimum of six months to support efficient recovery with minimal data loss.
  - Conduct annual restoration tests to verify that backups can be fully recovered to an operational state within acceptable downtime, and update the backup and recovery strategy based on test outcomes and organizational needs.

- SMB1001-3.2.0.0-2026 - Maintain Cyber Insurance: Purchase and maintain business or cyber insurance

  Procedure
  - Assess the organization's cyber risk exposure and identify the appropriate level of coverage needed for a business or cyber liability insurance policy.
  - Engage with insurance providers to obtain and maintain a policy that includes support and resources for responding to and recovering from cyber incidents.
  - Regularly review and update the insurance policy to ensure it remains adequate as the organization's cyber risk profile evolves.

References

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

Truncated Sample Document