SNOWBE ONLINE

Policy# RA-2026-01

REMOTE ACCESS POLICY

Group 2-2
Therasa Antoine
Version 1.0
Date 01/12/2026

Table of Contents

- **Purpose** This will help to establish the policies and procedures for the protection of the security system as well as operational management features. This is to protect all assets as far as personal information and credit card data. You must ensure that a secure VPN as well as Multifactor authentication is available so that access will be on a private secure network.

  Scope All occupant that will need to use any software or information on the SnowBe Network Database must use the secure VPN for access along with 2 Multifactor authentications for access to be granted. All rules and regulations must be adhered to while occupying the remote network and software.

- **Definitions-**

  VPN- '(Virtual Private Network) creates a secure encrypted network by making sure you IP address isn't shown which help keep away threats and most malice intent.

  Remote Access Control- the rules that are set which only allows authorized users to connect and access files, data and all other work resources.

  Network Configuration-the process of setting up hardware and ensuring that the network and software are working together i.e. router switches to keep the most secure access. Helps the data travel within the network while still being secure.

Roles & Responsibilities

IT Manager-Handles all IT issues and for all departments and management staff.

Technical Staff- maintaining all troubleshoot and security measures in

For the entire personnel.

Employees and contractors to follow all rules and to report all incidents within a timely manner

Policy

Remote access is only available for employees who has been approved to have access to the system

Secure Connection- the access must be with an approved VPN with encryption making sure they are compliance with the rules and regulations. 2 Factor authentication will be a required protocol to gain access.

Access Controls- All controls must be analyzed and assessed for malice activity and regularly monitored so that all unwanted traffic is reviewed.

Prohibited operations- No sharing of any information for the possibility of any threats or unauthorized access.

Monitoring and Reporting- any suspicious intent should be immediately to the head of IT Security to properly access the situation to be proactive for future situations.

Exceptions/Exemptions

No exceptions or exemptions to this policy are permitted. Due to the sensitive nature of remote access and the potential risk it poses to organizational systems, data, and regulated information, all users are required to comply fully with this policy without deviation.

Any failure to adhere to the requirements of this policy may result in the immediate revocation of remote access privileges, disciplinary action in accordance with organizational procedures, and, where applicable, legal or regulatory sanctions. This zero-exception approach ensures consistent enforcement and maintains the security and integrity of organizational resources.

Enforcement

Non-compliance with this policy may result in the immediate suspension or permanent loss of remote access privileges. Such actions are taken to protect organizational systems, data, and resources from potential security risks and to maintain the integrity of operations.

In addition, violations may lead to disciplinary measures in accordance with organizational policies and procedures, up to and including termination of employment or contracts. Where applicable, non-compliance may also result in legal or regulatory sanctions under relevant laws, standards, or contractual obligations.

-

Version History Table Policy **NIST SP 800-53:** RA-3 (Risk Assessment), PL-2 (System Security Plan)

- **NIST Risk Management Framework (RMF)** – Categorize, Select, Implement, Assess, Monitor
- **PCI DSS:** Requirement 12.2 (Risk Assessment)
- **ISO/IEC 27001:2022:** A.5.4 Information Security Risk Management

Version #	Implementation Date	Document Owner	Approved By	Description
RA-				

Citations

https://auditboard.com/blog/pci-dss-requirements

https://www.nist.gov/system/files/documents/2021/05/05/NIST-Privacy-Framework-V1.0-Core-PDF.pdf