SNOWBE ONLINE

SC-8 Transmission Confidentiality and Integrity

Version 2.0

02/25/2023

1. Purpose

This document outlines the policy and procedures for protecting company information systems and communications. This corresponds to the System and Communications Protection (SC) Control Family of the National Institute of Standards and Technology (NIST) Special Publication 800-53 (Revision 5)

2. Scope

This policy applies to the employees, Directors, volunteers, contractors, consultants, temporaries, and other workers at SnowBe Online, including all personnel affiliated with third parties with authorized access to any SnowBe Online information system.

3. Definitions

Authentication Mechanism:

- A mechanism that verifies user identities to ensure authorized persons can access the resources they need and to keep unauthorized persons from gaining access to resources.

Cryptographic Mechanisms (Cryptographic Modules):

- Any hardware, firmware, or software combination implements cryptographic functions such as encryption, decryption, digital signatures, authentication techniques, and random-number generation.

NIST:

- National Institute of Standards and Technology

OIT:

- Office of Information Technology

TLS:

- Transport Layer Security

4. Roles and Responsibilities

Chief Information Security Officer:

- Owns, executes, and enforces this Policy and Procedures.
- Implements security policies, standards, and controls.

Information Security Office:

- Protects information systems and assets against cybersecurity threats and vulnerabilities.
- Reviews all security logs and report exceptions to appropriate OIT teams.

Management:

- Ensures this Policy and Procedures are enforced.

SnowBe Personnel:

- Ensure data is stored only on OIT-approved devices, computers, and media.

5. Policy

1. Uses network monitoring tools and capabilities to detect and monitor suspicious network traffic.
2. Secures interfaces through network demarcation between the company and non-company controlled/public networks.
3. Implements standardized authentication mechanisms to:
    a. Authenticate users through Active Directory; and
    b. Authenticate devices using Active Directory, Multi-Factor Authentication, and identity/access controls.
4. 8.4.3.4. Implements secure protocols, Secure Shell/Transport Layer Security (TLS) and Internet Protocol Security (IPSec), for secure network management functions to:
    a. Cryptographic or Alternate Physical Protection SC8(1): Implement cryptographic mechanisms (see Definitions) to prevent unauthorized disclosure of information and detect information changes during transmission unless otherwise protected by alternative physical safeguards.
    b. Pre/Post Transmission Handling SC-8(2): Maintain information confidentiality and integrity during transmission and reception preparation.
5. Documents and retains on file a case-by-case risk management determination, for each type of confidential information, as to the appropriateness of its encrypted transmission to a party not served by the agency's internal network.
6. Ensures all communications that transfer sensitive and restricted data between web clients and servers employ the most current secure-transport protocol, including the latest version of TLS.
7. Addresses the risk involved in transferring different types of data and implements safeguards through the means of exchange used, such as through email, the internet, or the exchange of electronic media and portable media per the Data Exchange Policy.
8. Monitors for anomalies or known signatures via:
    a. Intrusion detection systems.
    b. Intrusion prevention systems.
    c. Network behavior analysis tools.

6. Exemption

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should expressly state the scope of the exception along with justification for granting the exception, the potential impact or risk

attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions, and a time frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

7. Enforcement

Employees who violate this policy may be subject to appropriate disciplinary action, including discharge and civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

Version History

Version #	Change Date	Document Owner	Approved By	Description
1.0	01/19/2020	SnowBe Online	SnowBe Online	First Draft
2.0	02/25/2023	SnowBe Online	SnowBe Online	Fixed version number spacing date missing on the cover page, formatting, and roles and responsibilities. Changed header to make it smaller

Citation

State of Maine