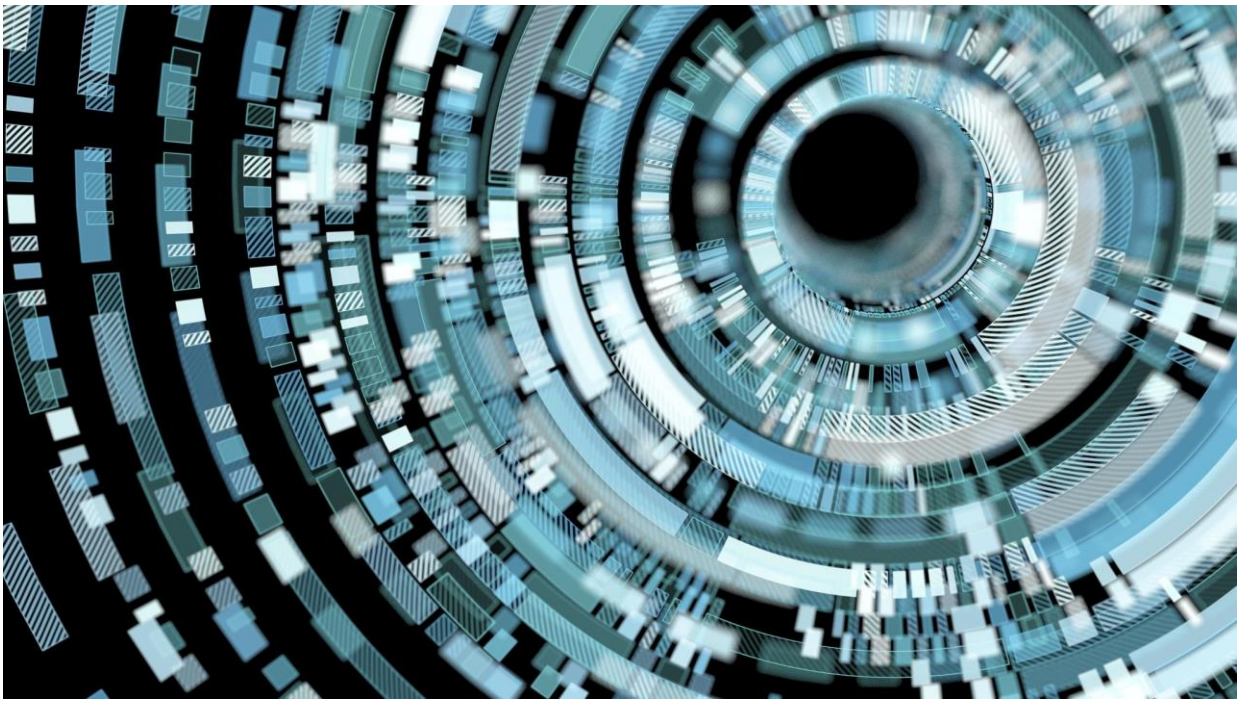
SNOWBE ONLINE

SC-28 – Protection of Information at Rest Policy



Joan V. Rodriguez Collazo
Project and Portfolio IV: Cybersecurity - Online
CYB349-O
Term C202210
Section 01

Version Date: 10.17.2022
Version Number: 1.0

TABLE OF CONTENTS

PURPOSE **1**
SCOPE **1**
DEFINITIONS **1**
Confidential Information 1
Personally Identifiable Information (PII) 1
Workforce Member 1
ROLES & RESPONSIBILITIES **2**
Chief Information Security Officer (CISO) 2
Workforce members 2
POLICY **2**
SC-28 – Protection of Information at Rest 2
SC-28(1) – Protection of Information at Rest | Cryptographic Protection 2
SC-28(3) – Protection of Information at Rest | Cryptographic Keys 2
EXCEPTIONS / EXEMPTIONS **3**
ENFORCEMENT **3**
VERSION HISTORY **3**
WORKS CITED **3**

PURPOSE

The purpose of this policy is to protect the confidentiality and integrity of the following information at rest: all sensitive information (i.e., data) stored either on company equipment and services or contractor-owned equipment.

It also calls for the implementation of cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on all equipment including internal or external hard disk drives, external USB drives, shared files/folders, storage area network devices, and databases for all sensitive information.

SCOPE

This policy covers all company or contractor-owned internal or external hard disk drives, external USB drives, shared files/folders, storage area network devices, and databases containing confidential information or personally identifiable information (PII).

DEFINITIONS

CONFIDENTIAL INFORMATION

Sensitive information wherein unauthorized disclosure could cause serious financial, legal, or reputational damage to SnowBe Online. May include personally identifiable information or confidential non-public information that relates to the nature of our business.

PERSONALLY IDENTIFIABLE INFORMATION (PII)

Information that can be used to distinguish an individual’s identity.

WORKFORCE MEMBER

Fulltime employees, part-time employees, affiliates, associates, contractors, and staff from third-party entities with access to data at SnowBe Online.

ROLES & RESPONSIBILITIES

CHIEF INFORMATION SECURITY OFFICER (CISO)

The CISO must determine roles and responsibilities for compliance and data governance personnel to support the implementation of this policy.

WORKFORCE MEMBERS

Workforce members are responsible for reading, understanding, and complying with policies, standards, and procedures based on the protection of all data at rest.

POLICY

SC-28 – PROTECTION OF INFORMATION AT REST

SnowBe Online shall encrypt sensitive information while at rest. If the information in the service provider environment cannot be encrypted, appropriate data isolation shall be implemented as a compensating control. System-related information requiring protection includes:

- *Configurations or rule sets for firewalls*
- *Intrusion detection and prevention systems*
- *Filtering routers*
- *Authenticator content*

Integrity protection will be achieved by implementing Write-Once-Read-May (WORM) technologies.

SC-28(1) – PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC PROTECTION

SnowBe Online will encrypt information on system components, media, data files, and client records.

SC-28(3) – PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC KEYS

A hardware-protected data store such as the Trusted Platform Module (TPM) will be used to protect cryptographic keys.

EXCEPTIONS / EXEMPTIONS

If compliance with this standard is not feasible or technically possible, or if a deviation from this policy is necessary to support a business function, entities shall request an exception through the Chief Information Security Officer's exception process.

ENFORCEMENT

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time.

Violations of this policy or failure to implement provisions of this policy may result in disciplinary action up to and including termination.

VERSION HISTORY

This section will contain a version history table.

Version	Change Date	Document Owner	Approved By	Description
1.0	10.17.2022	J. Rodriguez	J. Rodriguez	Working draft.

WORKS CITED

MDHHS. (2021, 06 01). *System and Communications Protection*. Retrieved from DHHS.Michigan.gov: https://dhhs.michigan.gov/OLMWEB/EX/AP/Public/APS/1360.pdf

NIST.gov. (n.d.). *NIST.gov*. Retrieved from SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS - NIST SP 800-53, REV. 5: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf