# SNOWBE ONLINE Policy AC-17(2) Protection of Confidentiality and Integrity using Encryption

**Your name: Lunick Francois**

**Protection of Confidentiality**

**and Integrity using Encryption**

**Policy - Version #1.0**

**DATE: 05/19/2024**

This page intentionally left blank

## Table of Contents

## Purpose

- This policy is to make sure that all data that is is being transmitted remotely across the network is protected and safe by using encryption. Encrypting the the data in transit is to maintain the confidentiality and integrity of the data.

## Scope

- All remote access connections.
- Any data being transmitted within the network.

## Definitions

**Confidentiality**: Making sure that all information is only accessed by those authorized.
**Encryption**: Encoding information or data using keys and only those with the key to decrypt it can access that information.
**Integrity**: Making sure that all data is accurate and complete without any changes made without permission.

## Roles & Responsibilities

**Employees/Contractors**: Making sure that all things done remotely is complying with this encryption policy.

**IT Department**: Responsible for managing encryption solutions.

**Managers**: Makes sure that the whole team is in compliance with the encryption policy.

## Policy

- **Encryption Standards**: Use of AES-256 encryption for all data that is being transmitted remotely.
- **Regular Audits**: Periodic audits to make sure everyone is in ensure compliance with the encryption standards.

## Exceptions/Exemptions

**If you believe you should be exempt from certain policies or procedures, please follow the steps below to submit a request for review:**

How to Request an Exception:
Submit an exception request via the IT Service Desk, providing detailed information about the reason for the exception. Once you log into the service desk, you will be prompted for the information that is relevant to your request. Ensure that all pertinent data or documentation necessary is submitted along with the request for quicker review process.

Why it is Being Requested:
Clearly explain why the exception is necessary and how it benefits SnowBe. Please be as detailed as possible.

Who Can Approve It:
Exceptions can only be approved by the Chief Information Security Office (CISO) or a designated representative or member of leadership.

How long the exception/exemption will be in place: __ days/ weeks

**Exceptions may be temporary or permanent, as indicated in the approval section.**

## Enforcement

Violations of this policy may result in disciplinary actions up to and include termination or employment or contract. The enforcement measures include:

- Verbal or written warnings
- Suspension or revocation of IT system access.
- Legal actions for intentional violations.

## Version History Table

| Version # | Implementation Date | Document Owner | Approved By | Description |
|---|---|---|---|---|
| 1.0 | 5/19/2024 | Group 3 | LF | Initial Draft |
| | | | | |
| | | | | |
| | | | | |

This page intentionally left blank

## Citations

https://csf.tools/reference/nist-sp-800-53/r5/ac/ac-17/ac-17-2/

https://www.stigviewer.com/controls/800-53/AC-17

https://old.unifiedcompliance.com/products/search-controls/control/00562/

https://wayfinder.digital/FedRAMP/AC017-FedRAMP.html

https://csrc.nist.gov/CSRC/media/Projects/risk-management/800-53%20Downloads/800-53r5/SP_800-53_v5_1-derived-OSCAL.pdf

https://www.gsa.gov/system/files/Access-Control-(AC)-[CIO-IT-Security-01-07-Rev-5]-08-18-2022.pdf

https://www2.ed.gov/fund/contract/about/acs/2023-ac-access-control-standard.pdf