



SNOWBE ONLINE Policy AC-18(1) Authentication and Encryption

Your name: Lunick Francois

**Authentication and
Encryption Policy - Version**

#1.0

DATE: 05/20/2024



This page intentionally left blank

Table of Contents

PURPOSE2

SCOPE.....2

DEFINITIONS.....2

ROLES & RESPONSIBILITIES2

POLICY.....3

EXCEPTIONS/EXEMPTIONS3

ENFORCEMENT4

VERSION HISTORY TABLE4

CITATIONS.....6

Purpose

- This policy is to make sure that all wireless access points and connections network are using strong authentication and encryption. That way the confidentiality and integrity of any data being transmitted over wireless networks is protected at all cost.

Scope

- All wireless access points and devices connecting to the network.

Definitions

Authentication: The process of verifying the identity of a user or device.

Encryption: Encoding information or data using keys to prevent unauthorized access.

WPA3: Wi-Fi Protected Access 3 which is used to protect wireless networks.

Roles & Responsibilities

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

IT Department: Responsible for managing strong authentication and encryption for all wireless access points and devices.

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

Policy

- **Encryption Standards:** All wireless networks must use WPA3 encryption. This will make sure that all data integrity and confidentiality is protected.
- **Authentication Standards:** Multi-factor authentication must be implemented for all wireless network access.

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	5/20/2024	Group 3	LF	Initial Draft

<Template Policy> – V 1.0

Status: ☒ Working Draft ☐ Approved ☐

Adopted Document owner:

DATE

This page intentionally left blank

Citations

<https://csf.tools/reference/nist-sp-800-53/r5/ac/ac-18/ac-18-1/>

<https://www.stigviewer.com/controls/800-53/AC-18>

[https://technology.ky.gov/policies-and-procedures/PoliciesProcedures/](https://technology.ky.gov/policies-and-procedures/PoliciesProcedures/ENT-201%20Enterprise%20Security%20Controls%20and%20Best%20Practices.pdf)

[ENT-201%20Enterprise%20Security%20Controls%20and%20Best%20Practices.pdf](https://technology.ky.gov/policies-and-procedures/PoliciesProcedures/ENT-201%20Enterprise%20Security%20Controls%20and%20Best%20Practices.pdf)

<https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment>

https://www.niap-ccevs.org/MMO/PP/ep_wlan_cli_v1.0-map_800-53r5_v3.pdf

[https://www.epa.gov/system/files/documents/2023-06/](https://www.epa.gov/system/files/documents/2023-06/information_security_access_control_procedure.pdf)

[information_security_access_control_procedure.pdf](https://www.epa.gov/system/files/documents/2023-06/information_security_access_control_procedure.pdf)

[https://www.tarleton.edu/technology/wp-content/uploads/sites/170/2022/07/Tarleton-](https://www.tarleton.edu/technology/wp-content/uploads/sites/170/2022/07/Tarleton-Security-Control-Standards-Catalog.pdf)

[Security-Control-Standards-Catalog.pdf](https://www.tarleton.edu/technology/wp-content/uploads/sites/170/2022/07/Tarleton-Security-Control-Standards-Catalog.pdf)