SNOWBE ONLINE

AC-18 Wireless Access

Davon Richardson

Version #1

DATE: 05-14-2025

Table of Contents

PURPOSE 2

SCOPE 2

DEFINITIONS 2

ROLES & RESPONSIBILITIES 2

POLICY 3

EXCEPTIONS/EXEMPTIONS 5

ENFORCEMENT 6

VERSION HISTORY TABLE 7

CITATIONS 8

Purpose

The purpose of this policy is to state the standards for wireless access to SnowBe Online's network. Wireless access can be done securely if certain steps are taken to mitigate known risks. This policy outlines the steps the company wishes to take to secure its wireless infrastructure.

Scope

This policy covers anyone who accesses SnowBe Online's network via a wireless connection. The policy covers the wireless infrastructure of the network, including access points, routers, wireless network interface cards, and anything else capable of transmitting or receiving a wireless signal.

Definitions

Mac Address (Media Access Control Address) - The unique hardware address of a network interface card (wireless or wired). Used for identification purposes when connecting to a computer network.

SSID (Service Set Identifier) The name that uniquely identifies a wireless network.

WEP (Wired Equivalency Privacy) - A security protocol for wireless networks that encrypt communications between the computer and the wireless access point. WEP can be cryptographically broken with relative ease.

WiFi (Wireless Fidelity) - Refers to networking protocols that are broadcast wirelessly using the 802.11 family of standards.

Wireless Access Point - A central device that broadcasts a wireless signal and allows user connections. A wireless access point typically connects to a wired network.

Wireless NIC - A Network Interface Card (NIC) that connects to wireless, rather than wired, networks.

WPA (WiFi Protected Access) - A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. Newer and considered more secure than WEP.

Roles & Responsibilities

None

Policy

Physical Guidelines

Unless a directional antenna is used, a wireless access point typically broadcasts its signal in all directions. For this reason, access points must be located central to the office space rather than along exterior walls. Technology must be used to control the signal broadcast strength so that it is reduced to only what is necessary to cover the office space. Directional antennas must be used as necessary to focus the signal on areas where it is needed. Physical security of access points must be considered. Access points must be placed in secure areas of the office. Cabling to and from access points should be secured so that it cannot be accessed without difficulty.

Configuration and Installation

The following guidelines apply to the configuration and installation of wireless networks:

Security Configuration

- The Service Set Identifier (SSID) of the access point must be changed from the factory default. The SSID must be changed to something completely nondescript. Specifically, the SSID must not identify the company, the location of the access point, or anything else that may allow a third party to associate the access point's signal to the company.
- The SSID must not be broadcast. This adds a layer of security by requiring wireless users to know the SSID in order to connect to the network.
- The wireless access point must utilize Mac address filtering so that only known wireless NICs are able to connect to the wireless network.
- The wireless access point must not connect to the company's trusted network without a firewall or other form of access control separating the two networks.
- Encryption must be used to secure wireless communications. The strongest available algorithm must be used (i.e., WPA rather than WEP). Encryption keys must be changed and redistributed quarterly.
- Administrative access to wireless access points must utilize strong passwords.
- All logging features must be enabled on the company's access points.
- Wireless networking should require users to authenticate against a centralized server. These connections should be logged, with IT staff reviewing the log regularly for unusual or unauthorized connections.
- Wireless LAN management software should be used to enforce wireless security policies. The software must have the capability to detect rogue access points.

- Users accessing wireless networks must be provided a personal software firewall to secure their computers.

Installation

- Software and/or firmware on the wireless access points and wireless network interface cards (NICs) must be updated prior to deployment.
- Wireless networking must not be deployed in a manner that will circumvent the company's security controls.
- Wireless devices must be installed only by the company's IT department.
- Channels used by wireless devices must be evaluated to ensure that they do not interfere with company equipment.

Accessing Confidential Data

- Confidential data must not be accessed using the wireless network. Security controls should be implemented to specifically block this access.

Inactivity

- Users must disable their wireless capability when not using the wireless network. This will reduce the chances that their machine could be compromised from the wireless NIC.
- Inactive wireless access points must be disabled. If not regularly used and maintained, inactive access points represent an unacceptable risk to the company.
- Wireless access points must be disabled during non-business hours. This should be accomplished with management software rather than manually performed.

Audits

- The wireless network must be audited quarterly to ensure that this policy is being followed. Specific audit points should be: location of access points, signal strength, SSID, SSID broadcast, and use of strong encryption.

Applicability of Other Policies

- This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

Authentication and Encryption

- Wireless networking capabilities represent a significant potential vulnerability that can be exploited by adversaries. To protect systems with wireless access points, strong authentication of users and devices along with strong encryption can reduce susceptibility to threats by adversaries involving wireless technologies.

Disable Wireless Networking

- Wireless networking capabilities that are embedded within system components represent a significant potential vulnerability that can be exploited by adversaries. Disabling wireless capabilities when not needed for essential organizational missions or functions can reduce susceptibility to threats by adversaries involving wireless technologies.

Restrict configurations By Users

- Organizational authorizations to allow selected users to configure wireless networking capabilities are enforced, in part, by the access enforcement mechanisms employed within SnowBe Online systems.

Antennas and Transmission power Levels

- Actions that may be taken to limit unauthorized use of wireless communications outside of organization-controlled boundaries include reducing the power of wireless transmissions so that the transmissions are less likely to emit a signal that can be captured outside of the physical perimeters of the organization, employing measures such as emissions security to control wireless emanations, and using directional or beamforming antennas that reduce the likelihood that unintended receivers will be able to intercept signals. Prior to taking such mitigating actions, organizations can conduct periodic wireless surveys to understand the radio frequency profile of organizational systems as well as other systems that may be operating in the area.

Exceptions/Exemptions

Anyone will initiate an exception request by contacting the IT department for Request an Exception to a Security Policy, Standard, or Procedure item, which can guide users through the policy exception request process as follows:

1. Once the form is submitted, the request is assigned to the IT Compliance team to review.
2. An IT Compliance team member works with the user to
    - assess the risks created by the exception,

- evaluate potential alternatives,
- provide recommendations, and
- determine the appropriate departmental and if applicable, the data steward's approval(s), the user needs to obtain,

3. Once the appropriate approvals are obtained, the IT Compliance team member will reply via email with documented approval or denial of the request (along with request details) to the requestor and/or user for whom the exception was requested, copying the department head/chair and vice president/dean approvers, as well as company Audit.

4. If the exception is granted and approval is obtained, the IT Compliance member will provide the user with any additional assistance as needed, such as coordinating with the relevant data steward(s) or other individual(s) who have a role in fulfilling the exception request.

5. If the exception is not granted, SnowBe Online Information Security will work with the user to define a reasonable deadline for compliance.

6. If the exception is not granted, the user may appeal the decision to the Chief Information Officer (CIO)

7. The user will be notified prior to expiration that the exception duration is ending. The user must then submit a new exception request or notify InfoSec that the exception is no longer needed.

Enforcement

Violations of any SnowBe Online policy include, but are not limited to: accessing data to which the individual has no legitimate right; enabling unauthorized individuals to access data; disclosing data in a way that violates applicable policy, procedures, or relevant regulations or law; inappropriately modifying or destroying data; inadequately protecting restricted data. Any violation of these policies may result in network removal, access revocation, corrective or disciplinary action, civil or criminal prosecution, and termination of employment.

<Template Policy> – V 1.0
Status: ✠ Working Draft ☐ Approved ☐ Adopted
Document owner:
DATE

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
V1	May 10, 2025	Davon Richardson	Davon Richardson	Exceptions/Exemptions & Enforcement
V2	May 14, 2025	Davon Richardson	Davon Richardson	Purpose/Scope/Defintions/Roles & Responsibilities/Policies

Citations

University Of Virginia
Exemptions
https://security.virginia.edu/exceptions

Bowie State University
Enforcement
https://www.bowiestate.edu/files/resources/information-security-public.pdf

City Of Jonesboro
Purpose
Scope
Definitions
Roles and Responsibilities
Policy
https://www.jonesboro.org/DocumentCenter/View/4257/Wireless-Access-Policy-PDF