P2105 - HITRUST - Wireless Security

Contents

Purpose:

The purpose of this Wireless Security Policy is to provide and establish Executive level explicit direction to all individuals and entities with a set of guidelines and controls for securing wireless networks and devices within the organization. This policy aims to protect organizational data and resources from unauthorized access, interference, and potential security breaches associated with wireless communications, in alignment with HITRUST CSF requirements.

The Organization is responsible for overseeing the development, implementation, and maintenance of the Information Security Program and associated components.

Scope:

This policy applies to all implemented information systems and supporting infrastructure used to support and protect sensitive data (PHI). This applies to systems whether managed centrally or in a distributed fashion, and to all individuals and entities who intend to access information systems and data. Within this document, the phrase "information systems and data" includes all technology resources and systems, transactions, applications, platforms, networks, databases, and other information systems within Integrity's technological environment.

Statement:

Wireless Access Authorization

The organization ensures wireless access is explicitly approved and wireless access points and devices have appropriate (e.g., minimum of AES WPA2) encryption enabled for authentication and transmission.

Reference: 0502.09m1Organizational.5

Where a specific business need for wireless access has been identified the organization

- requires end points to encrypt traffic prior to transmitting information over a wireless network.

For devices that do not have an essential wireless business purpose, the organization

- disables wireless access in the hardware configuration (basic input/output system or extensible firmware interface).

Reference: 0506.09m1Organizational.11

Prior to authorizing the implementation of wireless access points, the organization changes

- vendor default encryption keys,
- default SNMP community strings on wireless devices,
- default passwords/passphrases on access points, and
- other security-related wireless vendor defaults, if applicable.

Reference: 0501.09m1Organizational.10

Location of Wireless Access Points

Wireless access points are placed in secure areas.

Reference: 0503.09m1Organizational.6

Quarterly Scans

Quarterly scans are performed to identify unauthorized wireless access points. Appropriate action is taken if any unauthorized access points are discovered.

Reference: 0505.09m1Organizational.11

Wireless Encryption Key Management

The organization changes wireless encryption keys anytime anyone with knowledge of the keys leaves the company or changes positions.

Reference: 0501.09m1Organizational.11

Use of Perimeter Firewalls

Perimeter firewalls are implemented and configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the covered and/or confidential data environment.

Reference: 0504.09m1Organizational.13

This Mobile Device Security policy is supported by the following procedures:

- *05 – HITRUST – Wireless Security Procedure*

The Organization - Integrity, LLC and applicable Business Units.

Policy Sections:

Policy Compliance

Section Name: Policy Compliance

Statement:

Compliance Measurement

The Integrity Security Governance Committee will verify compliance with this policy through various methods, including but not limited to, periodic walk-throughs, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Integrity Security Governance Committee in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A contractor found to have violated this policy may be subject to an immediate termination of the right to access Integrity's systems and may also include the termination of Integrity's engagement with the contractor's employer.

Policy References:

Related Procedure References:

Related Regulatory Information:

P2105 - HITRUST - Wireless Security		
Document Author	**Name:** **Title:** **Email:**	Sumit Dhawan Manager Cybersecurity Compliance Sumit.Dhawan@integrity.com
Document Owner	**Name:** **Title:** **Email:** **Approved Date:**	Matt Williams Senior Director Cybersecurity & Cloud Engineering CISO matthew.williams@integrity.com 2/24/2026
Legal Management Approval	**Name:** **Title:** **Email:** **Approved Date:**	Duncan McQueen Assistant General Counsel Duncan.McQueen@integrity.com 3/16/2026
Executive Management Approval	**Name:** **Title:** **Email:** **Approved Date:**	Harsh Singla Chief Product and Technology Officer Harsh.Singla@integrity.com 3/30/2026

Last Published Date: 3/30/2026

Document Version Number 2.0