

---

## **P2104 - HITRUST - Mobile Device Security**

## Contents

|                                      |   |
|--------------------------------------|---|
| Purpose:.....                        | 3 |
| Scope:.....                          | 3 |
| Statement:.....                      | 3 |
| Policy Sections:.....                | 4 |
| Policy Compliance .....              | 4 |
| .....                                | 5 |
| Policy References:.....              | 6 |
| Related Procedure References:.....   | 6 |
| Related Regulatory Information:..... | 6 |

---

## Purpose:

The purpose of this Mobile Device Security Policy is to provide and establish Executive level explicit direction to all individuals and entities to follow the secure management and protection of mobile devices, including smartphones, tablets, and laptops, used within the organization. This policy aims to mitigate the security challenges associated with mobile devices, such as data loss, unauthorized access, and malware threats 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:

### Use of Encryption in Mobile Computing

The organization identifies and encrypts mobile devices and mobile computing platforms that process, store, or transmit sensitive information.

*Reference: 04.01x1Organizational.5*

### Monitoring of Mobile Devices

The organization monitors for unauthorized connections of mobile devices.

*Reference: 0403.01x1Organizational.5*

### Mobile Device Security Control

The organization prohibits the circumvention of built-in security controls on mobile devices.

*Reference: 0429.01x1Organizational.5*

### Teleworking Considerations

Suitable protection of the teleworking site is in place to protect against the theft of equipment and information, the unauthorized disclosure of information, unauthorized remote access to the organization's internal systems, or misuse of facilities.

**Reference: 0415.01y1Organizational.10**

Prior to authorizing teleworking:

1. the physical security of the teleworking site is evaluated (e.g., of the building and local environment), and
2. threats/issues associated with the physical security of the teleworking site are addressed.

**Reference: 0407.01y1Organizational.4**

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

- 04 – HITRUST – Mobile Device 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:**

## P2104 - HITRUST - Mobile Device Security

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

**Last Published Date:** 3/30/2026

**Document Version Number** 2.0