P2102 - HITRUST - Endpoint Protection Policy

Contents

Purpose:

The purpose of this Endpoint Protection Policy is to provide and establish Executive level explicit direction to all individual and entities for safeguarding organizational endpoints, including desktops, laptops, mobile devices, and servers, from security threats and vulnerabilities. This policy provides guidelines for implementing effective security controls, performing regular updates, and maintaining ongoing monitoring practices, in alignment with HITRUST CSF requirements.

The organization is responsible for overseeing the development, implementation, and maintenance of the The Organization's 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:

Controls Against Malicious Code

Technologies are implemented for the:

- timely installation of anti-malware protective measures,
- timely upgrade of anti-malware protective measures, and
- regular updating anti-malware protective measures, automatically whenever updates are available.

Periodic reviews/scans are required of the installed software and the data content of systems to identify and, where possible, remove any unauthorized software.

The organization employs anti-malware software that offers a centralized infrastructure that compiles information on file reputations or have administrators manually push updates to all machines.

After applying a malicious code detection and repair software update, automated systems verify that each system has received its signature update.

The checks carried out by the malicious code detection and repair software to scan computers and media include checking:

- any files on electronic or optical media, and files received over networks, for malicious code before use; and

- electronic mail attachments and downloads for malicious code before use or file types that are unnecessary for the organization's business before use;
- Web traffic, such as HTML, JavaScript, and HTTP, for malicious code;
- removable media (e.g., USB tokens and hard drives, CDs/DVDs, external serial advanced technology attachment devices) when inserted.

The check of electronic mail attachments and downloads for malicious code is carried out at different places (e.g., at electronic mail servers, desktop computers, and when entering the network of the organization).

Bring your own device (BYOD) users are not permitted. Personally owned devices are not allowed to access The Organization's information systems and associated networks. Personal devices are limited to the guest network.

Server environments for which the server software developer specifically recommends not installing host-based anti-virus and anti-spyware software are addressed via a network-based malware detection (NBMD) solution.

Reference: 0201.09j1Organizational.124

The organization configures malicious code and spam protection mechanisms to:

- perform periodic scans of the information system according to organization guidelines;
- perform real-time scans of files from external sources at endpoints and network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy; and
- block malicious code, quarantine malicious code, or send alerts to an administrator in response to malicious code detection.

Reference: 0217.09j1Organizational.7

Centrally Managed Spam Protection

Centrally managed spam protection mechanisms are employed at

- information system entry and exit points,
- workstations,
- servers, and
- mobile computing devices on the network.

Spam protection mechanisms detect and take action on unsolicited messages:

- transported by electronic mail,
- transported by electronic mail attachments,
- transported by Web accesses,
- transported by other common means, and
- inserted through the exploitation of information system vulnerabilities.

Malicious code and spam protection mechanisms are centrally managed and updated when new releases are made available in accordance with the organization's configuration management policy and procedures.

Reference: 0207.09j1Organizational.6

Regular Updates

The organization implements and regularly updates mobile code protection, including anti-virus and anti-spyware.

Reference: 0226.09k1Organizational.2

Additional Endpoint Protection Strategies

The organization augments endpoint protection strategies with additional solutions—including those built into the operating system if available—to mitigate exploitation of unknown vulnerabilities where traditional antivirus may be ineffective; and where applicable, target the solutions to protect commonly exploited applications (e.g., web browsers, office productivity suites, Java plugins).

Reference: 02962.09j1Organizational.5

Network Control Considerations

The organization applies a default-deny rule that drops all traffic via host-based firewalls or port filtering tools on its endpoints (workstations, servers, etc.), except those services and ports that are explicitly allowed.

Reference: 0265.09m1Organizational.2

User Responsibilities

All users are made aware of:

- the security requirements and procedures for protecting unattended equipment;
- their responsibilities for terminating active sessions when finished, unless they can be secured by an appropriate locking mechanism (e.g., a password protected screen saver);
- their responsibilities for logging-off mainframe computers, servers, and office PCs when the session is finished (e.g., not just switch off the PC screen or terminal); and
- their responsibilities for securing PCs or terminals from unauthorized use by a key lock or an equivalent control (e.g., password access) when not in use.

Reference: 0210.01g1Organizational.1

This Endpoint Protection program is supported by the following procedures:

- *02 - HITRUST - Endpoint Protection 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:

P2102 - HITRUST - Endpoint Protection Policy		
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