P2108 - HITRUST - Network Protection Policy

Contents

Purpose:

The purpose of the Network Protection policy is to provide and establish Executive level explicit direction to all individuals and entities to follow defined and enforced security measures that protect network infrastructure from threats and vulnerabilities, ensuring the confidentiality, integrity, and availability of information systems, 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:

Network Management

The organization, at a minimum:

- determines who is allowed to access which network and networked services;
- specifies the means that can be used to access networks and network services (e.g., the conditions for allowing access to a remote system);
- manages all enterprise devices remotely logging into the internal network, with remote control of their configuration;
- manages all enterprise devices remotely logging into the internal network, with installed software;
- manages all enterprise devices remotely logging into the internal network, with patch levels;
- publishes minimum security standards for access to the enterprise network by third-party devices (e.g., subcontractors/vendors);
- performs a security scan before allowing access;
- identifies the ports necessary for business and provides the rationale–or identifies compensating controls implemented–for those protocols to be non-secure;
- identifies the services necessary for business and provides the rationale–or identifies compensating controls implemented–for those protocols to be non-secure; and
- identifies the similar applications (e.g., protocols) necessary for business and provides the rationale–or identifies compensating controls implemented–for those protocols to be non-secure.

Reference: 0802.01i1Organizational.2

Security Gateways

Security gateways (e.g., a firewall) are used between the internal network, external networks (Internet and third-party networks), and any demilitarized zone (DMZ).

An internal network perimeter is implemented by installing a secure gateway (e.g., a firewall) between two interconnected networks to control access and information flow between the two domains.

This gateway is capable of enforcing security policies, being configured to filter traffic between these domains, and blocking unauthorized access in accordance with the organization's access control policy.

Wireless networks are segregated from internal and private networks.

The organization requires a firewall between any wireless network and the covered and/or confidential information systems environment.

Reference: 0805.01m1Organizational.12

At managed interfaces, network traffic is denied by default and allowed by exception (i.e., deny all, permit by exception).

The organization restricts the ability of users to connect to the internal network in accordance with the access control policy and the requirements of its business applications.

Reference: 0814.01n1Organizational.12

The organization uniquely identifies and authenticates network devices that require authentication mechanisms before establishing a connection. Network devices that require authentication mechanisms use shared information (e.g., MAC or IP address) to control remote network access and access control lists to control remote network access.

Reference: 0820.01k1System.3

The organization ensures that security gateways (e.g., a firewall) are used to validate source and destination addresses at internal and external network control points.

The organization designs and implements network perimeters so that all outgoing network traffic to the Internet must pass through at least one application layer filtering proxy server.

The application-layer filtering proxy supports:

- decrypting network traffic,
- logging individual TCP sessions,
- blocking specific URLs, domain names, and IP addresses to implement a disallow list, or applying lists of allowed sites that can be accessed through the proxy while blocking all other sites.

The organization forces outbound traffic to the Internet through an authenticated proxy server on the enterprise perimeter.

Internal directory services and internal IP addresses are protected and hidden from any external access.

Requirements for network routing control are based on the access control policy.

Reference: 0815.01o1Organizational.1

For public-facing web applications, application-level firewalls are implemented.

If a public-facing application is not web-based, the organization implements a network-based firewall specific to the application type.

If the traffic to the public-facing application is encrypted, the device either sits behind the encryption or is capable of decrypting the traffic prior to analysis.

Reference: 0808.10b2System.3

Intrusion Detection Systems

Technical tools such as intrusion detection systems (IDS)/intrusion prevention systems (IPS) are implemented and operating at the network perimeter and key points within the network.

Implemented and operating technical tools include IDS and IPDS deployed on the wireless side of the firewall (WIDS).

The IDS/IPS is updated on a regular basis, including the engines, baselines and signatures.

Reference: 0825.09m1Organizational.14

Application Sensitivity

The sensitivity of an application is explicitly identified and documented by the application/system owner.

Reference: 0816.01w1System.1

Malicious Addresses

The organization prevents enterprise assets from accessing known malicious addresses and domains on the Internet (for example by means of browser configurations, DNS sinkholing, and/or use of a subscription service), unless there is a clear, documented business need and the organization understands and accepts the associated risk.

Reference: 08.09m1Organizational.8

Network Service Provider

The ability of the network service provider to manage agreed services in a secure way is determined and regularly monitored. The right to audit is agreed by management for each network service provider.

The security arrangements necessary for particular network services' security features, service levels, and management requirements, are identified and documented.

Reference: 0835.09n1Organizational.1

This Network Protection Policy is supported by the following procedures:

- *08 – HITRUST – Network Protection Procedure*

The Organization - Deft Research LLC, Integrity LLC

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:

P2108 - HITRUST - Network 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