P2009 - Network Policy

Contents

Purpose:

The purpose of this policy is to mitigate the risks associated with security threats to network resources, ensure secure and reliable network access and protect the integrity of Integrity Marketing Group's ("Integrity") networks. This policy outlines required processes and technological controls for securing Integrity's network infrastructure, and help ensure their reliability and integrity.

Scope:

This policy applies to all Integrity employees and third party vendors/contractors who connect to or manage any of Integrity's networked computing resources. This policy also applies to network devices and all devices which may be used by individuals for network access, including but not limited to: • Routers• Wireless Access points • Workstations• Laptops• Smartphones• Servers

Statement:

Roles & Responsibilities

Integrity Security Governance Committee: The Integrity Security Governance Committee is responsible for the development, implementation, maintenance, and enforcement of this policy. In addition the Security Governance Committee is responsible for performing risk assessments on acquired entities' network infrastructure, providing guidance to help IT teams securely implement and protect the organization's networks, and periodically auditing and testing the IT team's implementations of network technologies.

Integrity IT: Integrity IT Team is responsible for implementing the technologies for network protection and segmentation across all Integrity Marketing Group environments.

Business Unit IT: Business Unit IT Teams are responsible for supporting the Integrity IT Team in implementing technologies for network protection and segmentation.

Policy Statement:

Integrity Marketing Group must implement processes and controls for the protection of enterprise networks, in accordance with the security best practices below.

Network Access: Integrity network resources may be accessed or used only by authorized Integrity employees, third-party vendors/contractors or visitors. Users must only be provided with access to the network and network services that they have been specifically authorized to use.

Network Segmentation: All networks must be segregated using a combination of firewalls, VLANs, ACLs, network DMZs, and physical segmentation. Devices that have been identified as vulnerable and cannot be patched must be segregated from the rest of the network. Other logical groups of devices should be segmented into unique subnetworks as well, including groups of IoT devices, data centers, endpoints, and telephone systems. Guest networks must be separated from any internal enterprise networks.

Remote Access: Integrity develops and maintains security controls for remote access to the organization's networks in accordance with accepted best practices. If employees or contractors must access a company network remotely for a legitimate business purpose, that access must be granted through an Integrity Marketing IT-approved VPN.

Secure Configuration of Network Devices: Integrity maintains secure configurations of all network devices. Network devices must adhere to their standard secure configurations, unless approved by an exception. Integrity IT is responsible for defining secure configurations, providing support for initial deployment of all newly-issued corporate network devices, and verifying that all devices maintain configurations that meet established security criteria.

Data in Transit: Strong cryptography and security protocols must be utilized to safeguard sensitive data during transmission over open, public networks, in accordance with Integrity's Data Protection and Lifecycle Policy.

Outsourced Network Services: Security mechanisms, service levels, and management requirements of all network services must be identified and included in network services agreements.

Acquisitions: Risk assessments must be conducted to identify risks associated with any infrastructure acquired through a merger with, or acquisition of, another entity. Before integrating the network infrastructure of a newly acquired entity, Integrity IT must conduct due diligence to identify risks associated with the newly acquired infrastructure, and ensure risks are mitigated, remediated, or accepted. All risk assessments are performed in accordance with Integrity's Risk Management Policy.

Policy Compliance

Compliance Measurement

The Integrity Security Governance Committee will verify compliance to 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.

Network Infrastructure*: The interconnected components of an information system, including routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

Network Segmentation: The act or practice of splitting a computer network into subnetworks, using a variety of technologies and controls to separate those subnetworks from one another.

Firewall*: A gateway that limits access between networks in accordance with policy.

Virtual Local Area Networks: Any broadcast domain that is partitioned and isolated in a computer network at the data link layer, in which devices communicate as if they were attached to the same wire.

Data Link Layer*: Layer of the TCP/IP protocol stack that handles communications on the physical network components such as Ethernet.

Demilitarized Zone (DMZ)*: A host or network segment inserted as a "neutral zone" between an organization's private network and the Internet.

Virtual Private Network (VPN)*: A virtual network built on top of existing networks that utilizes tunneling and security controls to provide a secure communications mechanism for data transmitted between networks.

Access Control List (ACL)*: A list of permissions associated with an object, which specifies who or what is allowed to access the object and what operations are allowed to be performed on the object.

Policy Sections:

Policy References:

Document Name	Category	Document Author	Document Owner
P2012 - Risk Management Policy	2000 - Information Technology	Matthew R Williams	Matthew R Williams
P2004 - Data Classification Policy	2000 - Information Technology	Matthew R Williams	Matthew R Williams

P2009 - Network Policy		
Document Author	**Name:** **Title:** **Email:**	Matthew R Williams Senior Director, Cybersecurity & Cloud Engineering, CISO matthew.williams@integrity.com
Document Owner	**Name:** **Title:** **Email:** **Approved Date:**	Matthew R Williams Senior Director, Cybersecurity & Cloud Engineering, CISO matthew.williams@integrity.com 1/30/2025
Legal Management Approval	**Name:** **Title:** **Email:** **Approved Date:**	Duncan William McQueen Assistant General Counsel duncan.mcqueen@integrity.com 3/27/2025
Executive Management Approval	**Name:** **Title:** **Email:** **Approved Date:**	Harsh Singla Chief Technology Officer Harsh.Singla@integrity.com 4/8/2025

Last Published Date: 4/8/2025

Document Version Number 2.0