P2014 - Third-Party Risk Management Policy

Contents

Purpose:..... 3
Scope:..... 3
Statement:..... 3
Policy Sections:..... 4
Policy Compliance 4
..... 5
Policy References:..... 6

Purpose:

The purpose of this policy is to mitigate the risks associated with third-party vendors. This policy extends the scope of Integrity Marketing Group's (Integrity) cybersecurity activities and formal processes to the organization's vendors, third-party suppliers and service providers, addressing additional risks associated with vulnerabilities that may be introduced upstream in the supply chain and outlining the requirements to maintain the health of Integrity's supply chain security posture.

Scope:

This policy applies to all third-party vendors, supplier and service providers utilized by Integrity and all associated devices or services managed by third-party providers.

Statement:

Roles & Responsibilities

Integrity Security Governance Committee: The Integrity Security Governance Committee is responsible for the development, implementation, maintenance, and enforcement of this policy.

Integrity IT: The Integrity IT Team is responsible for integrating technologies and services purchased from third party vendors, implementing protections and controls around those, and conducting initial and periodic risk assessments of vendors when delegated by the Integrity Security Governance Committee, the Chief Compliance Officer, or other Integrity representatives. In addition Integrity IT will provide third-party risk management guidance to the Business Units including an approved vendors list, a vendor questionnaire and risk assessment framework, and vendor risk management best-practices.

Business Unit IT: Business Unit IT Teams are responsible for implementing and enforcing the required security controls for third party technologies and services under their purview.

Policy Statement

Integrity Marketing Group must adhere to the third-party risk management practices and processes defined below.

Vendor Inventory: In order to manage risk associated with third party vendors, Integrity maintains an inventory of vendors whose devices or services are being used in Integrity's technological environment. Inventorying of vendors is outlined in Integrity's Asset Management Policy, and that inventory must be used to prioritize vendors according to criticality of service provided. This ranked vendors and services inventory will inform risk management and disaster recovery activities.

Risk Assessment: Before entering into any new contractual arrangement with a vendor or third- party, a risk assessment of the desired vendor or third-party must be conducted to assure that vendor's security posture follows industry best practices, and aligns with Integrity's organizational risk tolerance. Existing critical vendors must also be reassessed periodically to ensure continued demonstration of satisfactory security controls. Integrity IT will provide guidance for

performing these assessments, as outlined in Integrity's Risk Management Policy.

Information Security Agreement: In addition to regularly assessing vendors, Integrity leverages contracts with vendors and third-party providers to require that those vendors maintain security measures commensurate with protections required by Integrity's information security activities as a whole. Where possible, these contracts must also mandate disclosure of vulnerabilities and timely breach notifications between both parties. Any terms or stipulations agreed upon by Integrity and a third-party business partner must be formalized in an ISA.

Business Continuity and Disaster Recovery Plan: Vendors and third-party providers who play a role in incident response and disaster recovery activities should be considered in incident response and disaster recovery planning. Testing of those response and recovery plans must include vendors and partners, where applicable.

Information Security Agreement (ISA): A document that regulates security-relevant aspects of an intended business relationship between two entities. It regulates the security interface between any two systems operating under two different distinct authorities, and any systems or services provided by one entity for use by the other.

Policy Sections:

Policy Compliance

Section Name: Policy Compliance

Statement:

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.

Policy References:

Document Name	Category	Document Author	Document Owner
P2002 - Asset Management	2000 - Information Technology	Jeremy Hart	Matthew R Williams
P2012 - Risk Management Policy	2000 - Information Technology	Matthew R Williams	Matthew R Williams

P2014 - Third-Party Risk Management 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