P2015 - Threat and Vulnerability Management Policy

Contents

Purpose:

The purpose of this policy is to establish requirements around Integrity Marketing Group's ("Integrity") Threat and Vulnerability Management activities, and enable consistent management of threats and vulnerabilities across the organization.

Scope:

This policy applies to all information systems and data owned, operated, or otherwise utilized by Integrity.

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 ensuring vulnerability management practices are in place and conducted on a regular basis in accordance with this policy.

Business Owners: Business Owners are responsible for understanding, and serving as the point-of- contact for, specific assets within Integrity's technological environment.

Integrity IT: The Integrity IT Team is responsible for threat intelligence gathering and dissemination efforts, including the monitoring of global services and forums that provide updates on prominent and growing security threats. The Integrity IT Team is also responsible for vulnerability management efforts, including vulnerability scanning, criticality assessment, and patch management. Integrity IT will serve in a role that ensures facilitation and collaboration amongst all Integrity Marketing Group teams.

Business Unit IT: The Business Unit IT Teams are responsible for remediation of vulnerabilities on systems for which they are responsible.

Contractors and Third Parties: All contractors and third party vendors are responsible for notifying Integrity of any vulnerabilities in their products when they are discovered. As applicable, they are also responsible for providing patches for identified vulnerabilities in their devices/software, including support for necessary operating system upgrades.

Policy Statement

Threat Intelligence: Threat intelligence includes processes for gathering and analyzing information about prevalent or newly discovered attacks or exploits. The Integrity IT Team maintains a body of sources for threat intelligence gathering. These sources can include paid services from threat intelligence providers, and/or free forums and communities available on the Internet. Information collected through threat intelligence activities can provide Integrity with insight into commonly targeted systems, attack vectors, exploits, or newly discovered Indicators of Compromise (IOC). Reports on gathered intelligence must be passed periodically to the IT teams, so that reported IOCs can be used to inform security monitoring and risk management activities.

Vulnerability Management: The Integrity IT Team must conduct regular, quarterly vulnerability scans to identify security weaknesses in the organization's systems, devices, and network. These scans report on identified vulnerabilities and assign them a Common Vulnerability Scoring System (CVSS) Base Score. Criticality levels and recommended remediation windows for Base Score ranges are described in the table below. Based on these reported CVSS scores and knowledge of Integrity's technological environment, IT teams are responsible for prioritizing the identified vulnerabilities. Risk Management processes should be followed in order to evaluate any vulnerabilities that cannot be remediated in a timely manner.

Criticality Level	CVSS Base Score Range	Remediation Window
Critical	90.-10.0	Not to exceed 7 days or shortest possible window
High	7.0-8.9	Not to exceed 30 days or shortest possible window
Medium/Moderate	4.0-6.9	Not to exceed 90 days or shortest possible window
Low/Informational	0.1-3.9	Determined on a case by case basis

Patch Management: Integrity's IT teams are responsible for security patching of systems. Based on the prioritization described above, the IT teams must apply security patches and updates to systems in order to mitigate the risk of exploitation of any existing vulnerabilities. Vulnerabilities must be patched within the remediation window associated with their criticality level. No user may disable or tamper with the patching process or configuration of security updates on the organization's systems.

All systems must be patched to remain in compliance with this policy. Any systems that cannot be patched in the appropriate remediation timeline requires an exception. Unserviceable systems that have been granted an exception may be used for no more than one year. New systems that cannot be patched in accordance with this policy may not be purchased for use by the organization.

Penetration Testing: Penetration testing must be performed regularly both internally and by a third party. Any additional vulnerabilities identified by penetration testing will be handled by IT as part of overall vulnerability management.

Threat*: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Vulnerability*: Any weakness in an information system, system procedures, internal controls, or implementation that can be exploited or triggered by a threat source.

Vulnerability Scanning: A technique used to identify devices, device attributes, and associated vulnerabilities.

Vulnerability Analysis*: Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Penetration Testing*: Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network, often involving issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers.

Patch Management*: The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions.

Threat Intelligence: The aggregation of knowledge about prominent and emerging security exploits that can be used to inform decisions about how to expand and improve Integrity's overall security program.

Indicators of Compromise (IOC): Artifacts that are observed on a network or in an operating system that increases confidence that the network or system has been compromised by a threat actor. These include virus signatures and IP addresses, MD5 hashes of malware files, or URLs and domain names of botnet command and control servers.

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:

P2015 - Threat and Vulnerability 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