Acceptable Use Policy — Last Revised: 02/02/2022	
Document Author	Name: Matthew Williams Title: Senior Director of Infrastructure & Information Security | CISO Email: matthew.williams@integritymarketing.com
Document Current Owner	Name: Matthew Williams Title: Senior Director of Infrastructure & Information Security |CISO Email: matthew.williams@integritymarketing.com
Document Approvers	Name: Harsh Singla Title: Chief Technology Officer Email: harsh.singla@integritymarketing.com Name: Steve Lundstrom Title: Senior Director of Software & Data Engineering Email: steve.lundstrom@integritymarketing.com Name: Matthew Williams Title: Senior Director of Infrastructure & Information Security | CISO Email: matthew.williams@integritymarketing.com

Acceptable Use Policy

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Integrity. These rules are in place to protect the employee and Integrity. Inappropriate use exposes Integrity to risks including virus attacks, compromise of network systems and services, and legal issues.

Information Security's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Integrity's established culture of openness, trust and integrity. Information Security is committed to protecting Integrity's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Integrity. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Integrity employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Scope

The concepts, policies, standards and initiatives within Integrity's Information Security Policy apply to Integrity and all of its Business Units. Each Business Unit must comply with the organization-wide information security program, associated policies, and standards as reviewed, approved and signed by the Chief Technology Officer at Integrity.

All Integrity employees are responsible for the security and protection of electronic information resources over which they have control. Resources to be protected include, and are not limited to: networks, computers, software, and data. The physical and logical integrity of these resources must be protected against threats such as unauthorized intrusions, malicious misuse, or inadvertent compromise.

Roles & Responsibilities

Role	Job Functions	Responsibilities
Chief Technology Officer	1. Responsible for the overall planning, coordination and execution of the Information Technology functions across Integrity and its Business Units 2. Oversees the operation, maintenance, and availability of Integrity's IT infrastructure and associated services 3. In collaboration with the CISO, protects Integrity information and infrastructure from external or internal threats and assures that Integrity complies with applicable statutory and regulatory requirements	• Lead the overall strategic planning, budget and decision management processes related to Information Technology and ensure it aligns with Integrity's business mission • Oversee the IT on-boarding process for new Business Units including installation and configuration of new information technology equipment • As an IRT (Incident Response Team) member, primarily responsible for recommending policy and technology changes after any security incident
Chief Information Security Officer	1. Assumes the role of Risk Manager as it relates to Information Security Risk. At the Administration or Business Unit levels, manages, develops, and implements risk management programs, policies, and procedures appropriate to the organization. 2. Ensures continuity of information security program efforts with the Chief Privacy Officer 3. Maintains overall responsibility for developing and delivering a comprehensive information security program that complements and supports relating privacy and regulatory programs and requirements 4. Leads Integrity's information security activities including security monitoring, vulnerability management, risk management, and incident response to support Integrity's Information Security program	• Responsible for the overall security risk management across Integrity and ensuring that Integrity's information security program is established and aligns with the mission and vision of Integrity and its Business Units. • Responsible for serving as the Information Security representative on the Executive Leadership team • Responsible for interacting with Senior and Executive Leadership as it relates to Information Security • Ensure enforcement of Information Security policies at Integrity and its Business Units • Establish processes to measure Information Security risk and periodically report risk to the Information Security Governance Committee • Lead the overall strategic planning and decision management processes related to Information Security Policy Development • As a risk manager, conduct site visits, analyze risks, and accordingly update and maintain the risk register to continuously improve processes • Responsible for the incident response program including the review and update of the incident response plan and leading the Incident Response Team in an incident response scenario
Chief Compliance Officer	Manage the implementation of, and compliance with, Integrity Marketing Group's Privacy Policies and Procedures that provide guidance for the protection and safeguarding of all data classified as Regulated in the organization's Data Classification and Retention Policy	• Responsible for the development, implementation, and oversight of privacy and compliance related programs • Responsible for serving as the compliance and privacy representative on the Executive Leadership team

		• Responsible for interacting with Senior and Executive Leadership as it relates to compliance and privacy • Receive, document and respond to requests, complaints, and reports of alleged violations (security breaches) • Provide guidance and information about privacy related matters
Information Security Governance Committee	1. Facilitate making organization-wide, data-driven decisions regarding development, maintenance, and enforcement of Information Security Policies 2. Develop and foster a culture of information literacy and sharing across all Business Units, thereby enabling users to make informed decisions.	• Responsible for the overall execution of the information security program, including authorization of decisions regarding access, usage and risk levels associated with data across Integrity • Develop and provide framework that allows all key security decisions to be reviewed by key stakeholders • Develop a security improvement roadmap based on inputs from more focused security teams like the Risk Management team or Incident Response team
Compliance Leaders	Responsible for updating and coordinating privacy compliance at each of Integrity Marketing Group's Business Units.	• Assumes the role of Chief Compliance Officer delegate in day-to-day operations of managing privacy and compliance programs • Contributes to the oversight of privacy related policies and procedures • Receive, document, and respond to requests, complaints, and reports of alleged violations (security breaches) • Provide guidance and information about privacy related matters
Site Privacy and Security Lead (Site Leaders)	1. Responsible for implementing the Integrity Marketing Group's HIPAA Privacy Program within the Business Units. 2. Responsible for implementing the Integrity Marketing Group's Information Security Program within the Business Units.	• Facilitating execution of information security initiatives as directed by the Information Security Committee • Data Governance, architecture, and management in conjunction with the Information Security Governance Committee • Develop and maintain privacy procedures in accordance with HIPAA Privacy Regulations and revise them periodically as required by changes in Integrity Marketing Group's HIPAA Privacy Program
Integrity IT Team	Perform security operations, information security threat analysis, and tools maintenance.	As leader of a team or individual performer: • Provide guidance to the Business Units to meet or maintain compliance with applicable policies, standards, baselines, guidelines, and laws. • Ensure security program operations and controls are being consistently performed or applied • Establishes procedures to oversee the acquisition of supplies and equipment schedules • Assess requirements for updates to security plans based on changes to business functions, technical vulnerabilities, and emerging threats

Business Unit IT Teams	1. Manages the operation of an information technology unit or area including computer hardware, software, networking, and telecommunications equipment. 2. Plans, organizes, and controls all aspects of the operation including supervision of respective Business Unit staff, prioritizing and assigning of the work, and coordinating activities with other Integrity Business Units.	• Provides technical support for all hardware and systems within the Business Unit • Recommends hardware acquisitions, the acquisition and maintenance of support equipment, and the contracting and procurement of new equipment and software for Integrity IT team approval

Policy Statement

General Use and Ownership

Integrity proprietary information stored on electronic and computing devices whether owned or leased by Integrity, the employee or a third party, remains the sole property of Integrity. You must ensure through legal or technical means that proprietary information is protected in accordance with the *Data Protection and Lifecycle Policy.*

Integrity employees and contractors have a responsibility to promptly report the theft, loss or unauthorized disclosure of Integrity proprietary information.

Integrity employees and contractors may access, use or share Integrity proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use and for following company guidelines as set forth in this document.

For security and network maintenance purposes, authorized individuals within Integrity may monitor equipment, systems and network traffic at any time.

Internet Usage

Using company computer resources to access the Internet for personal purposes, without approval from the user's manager and the IT department, may be considered cause for disciplinary action up to and including termination.

Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk. The company is not responsible for any loss of information, such as information stored in the wallet, or any consequential loss of personal property

Right to Monitor

Website Monitoring

The Information Technology Department shall monitor Internet use from all computers and devices connected to the corporate network. For all traffic the monitoring system must record the source IP Address, the date, the time, the protocol, and the destination site or server. Where possible, the system should record the User ID of the person or account initiating the traffic.

Access to Web Site Monitoring Reports

Computer Security Incident Response Team (CSIRT) members may access all reports and data if necessary to respond to a security incident. Internet Use reports that identify specific users, sites, teams, or devices will only be made available to associates outside the CSIRT upon written or email request to Information Systems from a Human Resources Representative.

Internet Use Filtering System

Unless otherwise specified by your manager and approved by Integrity Cybersecurity, the Information Technology Department shall block access to Internet websites and protocols that are deemed inappropriate for Integrity Marketing's corporate environment. The following protocols and categories of websites should be blocked:

- Adult/Sexually Explicit Material
- Gambling
- Hacking
- Illegal Drugs
- Peer to Peer File Sharing
- SPAM, Phishing and Fraud
- Spyware
- Tasteless and Offensive Content
- Violence, Intolerance and Hate

Internet Use Filtering Rule Changes

The Information Technology Department shall periodically review and recommend changes to web and protocol filtering rules.

Internet Use Filtering Exceptions

If a site is mis-categorized, employees may request the site be un-blocked by submitting a ticket to the Information Technology help desk. An IT employee will review the request and un-block the site if it is mis-categorized.

Employees may access blocked sites with permission if appropriate and necessary for business purposes. If an employee needs access to a site that is blocked and appropriately categorized, they must submit a request to their Human Resources representative. HR will present all approved exception requests to Information Technology in writing or by email. Information Technology will unblock that site or category for that associate only. Information Technology will track approved exceptions and report on them upon request.

Security and Proprietary Information

System level and user level passwords must comply with the Identity & Access Management Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 30 minutes or less. You must lock the screen or log off when the device is unattended.

Postings by employees from an Integrity email address to media sources is prohibited, unless posting is in the course of business duties and approved by Integrity Marketing.

Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware.

Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.

Computer workstations must be locked when workspace is unoccupied.
Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.

File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.

Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.

Unacceptable Use
The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Integrity authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Integrity-owned resources.
The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

<u>System and Network Activities</u>
The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Integrity.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Integrity or the end user does not have an active license is strictly prohibited.
- Accessing Integrity data, a server, or an account for any purpose other than conducting Integrity business, even if you have authorized access, is prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

- Introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using an Integrity computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any Integrity account.
- Effecting security breaches or disruptions of network communication.
- Port scanning or security scanning is expressly prohibited unless required and defined by job responsibilities.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network, or account.
- Introducing honeypots, honeynets, or similar technology on the Integrity network unless approved by Integrity Cybersecurity.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, Integrity employees to parties outside Integrity.

Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company".

Users should be aware that clear text E-mail is not a confidential means of communication. The company cannot guarantee that electronic communications will be private. Employees should be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Users should also be aware that once an E-mail is transmitted it may be altered. Deleting an E-mail from an individual workstation will not eliminate it from the various systems across which it has been transmitted.
Questions may be addressed to the IT Department. The following email and communication activities are prohibited:

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Use of unsolicited email originating from within Integrity's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Integrity or connected via Integrity's network.

- Using a personal email for any Integrity business is prohibited.
- Forwarding Integrity emails to a personal email account with the intent to conduct Integrity business is prohibited unless expressly approved by Integrity Cybersecurity.
- Acquisition, storage, and dissemination of data which is illegal, pornographic, or which negatively depicts race, sex or creed is specifically prohibited.
- The company also prohibits the conduct of a business enterprise, political activity, engaging in any form of intelligence collection from our facilities, engaging in fraudulent activities, or knowingly disseminating false or otherwise libelous materials
- Deliberate pointing or hyper-linking of company Web sites to other Internet/WWW sites whose content may be inconsistent with or in violation of the aims or policies of the company.
- Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libelous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.
- Unauthorized downloading of any shareware programs or files for use without authorization in advance from the IT Department and the user's manager.

Blogging and Social Media

- Blogging by employees, whether using Integrity's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Integrity's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Integrity's policy, is not detrimental to Integrity's best interests, and does not interfere with an employee's regular work duties. Blogging from Integrity's systems is also subject to monitoring.
- Integrity's Data Classification Policy also applies to blogging. As such, employees are prohibited from revealing any Integrity confidential or proprietary information, trade secrets or any other material covered by Integrity's Data Classification policy when engaged in blogging.
- Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Integrity and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Integrity's Employee Code of Conduct policy.
- Employees assume any and all risk associated with blogging.
- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Integrity's trademarks, logos and any other Integrity intellectual property may also not be used in connection with any blogging activity

Policy Compliance

Compliance Measurement

Integrity shall monitor all its Business Units for compliance with the Information Security Policy. To ensure that the Information Security Policy is applied consistently across Integrity, each year Integrity will require all its Business Units to report their status with respect to implementing and complying with the organization-wide information security program.

Exceptions
While deviation from security policies is discouraged, an exception process exists that allows for certain scenarios which cannot be effectively addressed within the constraints of Integrity's security policies and standards, to be managed effectively and within the scope of Integrity's stated business outcomes.

Any potential exceptions to the information security policies and associated standards should be evaluated based on the risk associated with the particular situation. This should include factors related to data classification, business objectives, regulatory and compliance matters, systems and processing criteria, and technology.

Exceptions to the policy must be evaluated by the Integrity Information Technology function in conjunction with collaboration and input from other functions at the Business Unit level. When evaluating any exceptions, consideration must be given to any relevant compensating controls or mitigating factors.

Requests for exceptions to a policy must be submitted in writing to the Integrity VP of Technology. Exceptions shall be permitted only upon receipt of written approval from the Integrity VP of Technology. Integrity Information Technology will retain documentation of currently permitted exceptions.

Non-Compliance
Violations of the Information Security Policy may result in appropriate disciplinary measures in accordance with local, state, and federal laws, as well as the Standards of Conduct for all Integrity employees.

All personnel covered by the Information Security Policy are obligated to report apparent violations of this program or its associated policies and standards. If the violation does not appear to be resolved in a timely manner, the Integrity VP of Technology must be notified by the person observing the violation.

References
- Data Classification Policy

Asset Management Policy — Last Revised: 02/02/2022	
Document Author	**Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com
Document Current Owner	**Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com
Document Approvers	**Name:** Harsh Singla **Title:** Chief Technology Officer **Email:** harsh.singla@integritymarketing.com **Name:** Steve Lundstrom **Title:** Senior Director of Software and Data Engineering **Email:** steve.lundstrom@integritymarketing.com **Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com

Asset Management Policy

Purpose

The purpose of this policy is to mandate requirements for developing and maintaining a complete inventory of Integrity Marketing Group's ("Integrity") Information Technology (IT) assets, and for establishing a process for management of IT assets across their service lifecycle, from the point of acquisition to disposal/destruction.

Scope

This policy applies to all employees of and contractors to Integrity who use or manage IT assets owned and/or managed by the organization, and all assets as defined below.

Definitions

Assets: Resources owned or managed by Integrity, including, but not limited to:

- Systems, such as endpoints, network devices, servers, mobile devices, applications, and other information systems
- Data, such as intellectual property, financial data, operational data, software licenses, and brand designs

Asset Lifecycle: The full cycle of a system, product, service, project, or other asset of the organization from conception through retirement

Asset Management: A set of business processes designed to manage the lifecycle and inventory of an organization's assets

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 implementing and managing a centralized asset management system that meets applicable regulatory, operational, and business requirements.

Business Unit IT: Business Unit IT Teams must ensure that the tracking and management of assets during their acquisition, distribution, use, and disposal adhere to Integrity asset management standards. They are also responsible for suggesting specific technologies during asset procurement processes (where applicable), and ensuring timely and appropriate disposal of IT assets.

Policy Statement

Integrity is committed to managing the lifecycle of its IT assets, and all employees have a responsibility to protect those assets, whether they are in use, storage, transit, or disposal. All IT assets should be protected against theft, mishandling, and accidental damage. Information about all IT assets should be maintained in a single asset inventory, in which asset information is tracked, managed, and audited throughout their lifecycle.

All assets should be tracked and linked back to the asset inventory to provide visibility into asset location, type, classification, and owner. This inventory informs operational and security related tasks, such as auditing, protection, responding to incidents, and risk management. Tracking of assets may be done via asset tagging or the use of another unique identifier. During asset onboarding, all asset information should be entered into the asset inventory, including the asset's unique identifier, its business function, and the minimum set of information as specified in Integrity's Asset Management Standard. When any asset is provisioned for use by an employee or third-party, that change in asset owner should also be reflected in the asset inventory.

Decisions about acquisition, maintenance, and disposal of assets should be prioritized based on each asset's criticality and business value. Classification of data assets is performed in accordance with Integrity's Data Classification Policy. Guidance for the assessment and management of other asset-related risk is outlined in Integrity's Risk Management Policy.

Integrity should maintain a process for the off-boarding of assets which includes the use of approved vendors. All disposal and destruction of assets should be performed in compliance with the organization's legal and regulatory environment.

All Integrity system assets should utilize software and operating systems that are vendor-supported and must be patched to address security vulnerabilities in accordance with the Threat & Vulnerability Management Policy. Information system assets should be retired no later than 3 months prior to the vendor's stated end of life date, or end of support for the product, whichever is earliest.

Policy Compliance

Compliance Measurement

The 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 assessments, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the 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.

References

- Risk Management Policy
- Data Classification Policy
- Threat & Vulnerability Management Policy

Business Continuity and Disaster Recovery Policy — Last Revised: 02/02/2022	
Document Author	**Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com
Document Current Owner	**Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com
Document Approvers	**Name:** Harsh Singla **Title:** Chief Technology Officer **Email:** harsh.singla@integritymarketing.com **Name:** Steve Lundstrom **Title:** Senior Director of Software and Data Engineering **Email:** steve.lundstrom@integritymarketing.com **Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com

Business Continuity and Disaster Recovery Policy

Purpose

This policy mandates the processes and technical measures necessary to support Integrity Marketing Group's ("Integrity") effort to continue business operations in the event of a disruption, and recover from disasters or other significant events.

Scope

This policy applies to all data handled in the course of Integrity's business operations, and all key business functions, processes, data and information systems in Integrity's technological environment.

Definitions

Business Continuity: Goals and strategies to allow the organization's mission and business processes to be sustained during and after a significant disruption

Disaster Recovery: Practices and activities for recovering one or more information systems in response to a significant disruption

Recovery Point Objective (RPO): The point in time at which data must be recovered after an outage

Recovery Time Objective (RTO): The overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or mission/business processes

Redundancy: The ability of a functional component, systems, or data to maintain or restore functionality during the occurrence of a single failure.

Golden Image: An archetypal version of a device that can be used as a template for standardizing various kinds of hardware

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 must define recovery processes, test those processes, update recovery processes from lessons learned, and oversee communication and recovery efforts in the event of a genuine disaster. The Integrity IT Team is responsible for architecting golden images for servers and endpoints. The Integrity IT Team must review and approve all processes for disaster recovery, oversee the efforts during any recovery scenario, and define RTOs and RPOs for systems under the Integrity IT Team's purview.

Business Unit IT: Business Unit IT Teams are responsible for defining RTOs and RPOs for systems under their purview, establishing redundancy of technologies and services in support of business continuity efforts, and for generating and maintaining golden images for servers and endpoints.

Policy Statement

In the event Business Continuity or Disaster Recovery plans are initiated, Integrity Marketing must plan to restore essential functions, as defined and agreed upon by Integrity Marketing IT, Cybersecurity, and the Business Unit, with 72 hours after the essential functions fail or otherwise stop functioning as usual.

Integrity Marketing must notify appropriate carriers if Business Continuity or Disaster Recovery measures are initiated.

Business Continuity: In support of business continuity goals, Integrity Marketing Group strives to achieve redundancy for systems and data. Activities required for building redundancy include the generation of periodic data backups to be stored offsite in data warehouses, and the upkeep of overall network availability through redundancy of routers, firewalls, switches, and other infrastructure devices. Integrity also develops and maintains redundancy of vendors, to avoid introducing additional risk by creating a single point of failure.

Considering business requirements and feasibility, Integrity shall maintain golden images for endpoints to be applied to new or compromised devices. The Integrity IT Team defines the applications and security protections that must be included in those images. Any exceptions must be approved by the Integrity Security Governance Committee. and must be tracked accordingly.

Considering business requirements and any applicable laws or regulations, the Integrity IT Team in collaboration with the Business Unit IT Teams must define RPOs for all data types, including any operational work in-progress, sales and marketing data, and any internal documentation or notes. Backups must be generated to ensure that the amount of lost data (measured in time from a potential failure occurrence to the last valid backup) will never exceed the established RPO for that data. Data backups are generated and maintained in accordance with Integrity's Data Protection and Lifecycle Policy and Data Classification and Retention Policy.

In order to test the organization's ability to continue business operations in the event of a disruption, business continuity processes should be evaluated at least yearly. This evaluation includes testing of infrastructure redundancy and employees' ability to complete their work remotely, if needed.

Disaster Recovery: Integrity Marketing Group develops and maintains procedures for Disaster Recovery. These processes include recovery of failing or compromised information systems by system criticality and the recovery of lost or corrupted data. Processes for determining the

criticality of individual assets are outlined in the organization's Asset Management Policy. The Security Governance Committee should ensure RTOs for the organization's information systems are formally defined and documented. In a recovery scenario, the IT teams will use these RTOs to prioritize affected systems for repair. In the event that Integrity must recover from any technological or security disaster, appropriate communications must be a part of those recovery efforts. Recovery activities must be communicated to all internal and external stakeholders, and public relations must be managed in order to protect and repair the organization's reputation.

All formal recovery planning and processes must be tested regularly to ensure their effectiveness. Lessons learned from both simulated and real disaster recovery efforts are documented, and used to improve future recovery processes and strategies.

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.

References

- Asset Management Policy

Data Classification Policy — Last Revised: 02/02/2022	
Document Author	**Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com
Document Current Owner	**Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com
Document Approvers	**Name:** Harsh Singla **Title:** Chief of Technology **Email:** harsh.singla@integritymarketing.com **Name:** Steve Lundstrom **Title:** Senior Director of Software and Data Engineering **Email:** steve.lundstrom@integritymarketing.com **Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com

Data Classification Policy

Purpose

The purpose of this policy is to define the risk-based approach for the categorization of data assets at Integrity Marketing Group ("Integrity"), and provide guidance for the appropriate retention of that data. This policy describes categories for classification of all data types, to help Integrity protect its data in a consistent and appropriate manner.

Scope

This policy applies to all of Integrity's data including electronic or printed data, and data at rest or in transit. Additionally, this policy applies to any data that is hosted or accessed by third party service providers.

Definitions

Data Type: A category of information that is stored or transmitted within Integrity Marketing Group's business environment. For example, licensing contracts, credit card numbers, third party intellectual property and brand logos would all be unique business data types.

Personally Identifiable Information (PII)*: A data type that includes any information about an individual that can be used to distinguish or trace an individual's identity. This includes data such as name, date and place of birth, social security number, driver identification, mother's maiden name, or biometric records as well as data that is linked or linkable to an individual, such as medical, educational, financial and employment information.

Protected Health Information (PHI) **: Individually identifiable health information that is transmitted by, or maintained in, electronic media or any other form or medium. This information must relate to 1) the past, present, or future physical or mental health, or condition of an individual; 2) provision of health care to an individual; or 3) payment for the provision of health care to an individual. If the information identifies or provides a reasonable basis to believe it can be used to identify an individual it is considered individually identifiable health information.

Payment Card Industry Data (PCI): A data type that includes all financial data related to individual credit, debit, or pre-paid cards, including primary account number, cardholder name, expiration date, magnetic strip data, and account pins.

* Definition taken from the Computer Security Resource Center Glossary: https://csrc.nist.gov/Glossary

** Definition taken from HIPAA Privacy Rule and Public Health Guidance from CDC and the U.S. Dept. of Health and Human Services: https://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm

Roles & Responsibilities

Integrity Security Governance Committee: The Integrity Security Governance Committee is responsible for the development, implementation, maintenance, and enforcement of this policy. The Security Governance Committee must approve all data classifications proposed by data owners, work in cooperation with compliance and legal counsel to generate data retention timelines, and ensure data retention efforts comply with this policy by conducting regular audits or assessments.

Integrity IT: Integrity IT Team is responsible for saving and backing up data in accordance with data retention requirements, and assigning data ownership to individuals responsible for each data type. They are also responsible for the implementation of any processes and controls required to protect the organization's data.

Data Owner: Data owners are responsible for evaluating and classifying the sensitivity of data with the approval of the Security Governance Committee. Additionally, they are responsible for developing and maintaining processes for the disposal of data after its retention period has expired.

Policy Statement

Data Classification

All data that is stored or transmitted by Integrity Marketing Group must be assigned a data classification type. The classification type is generated by its Data Owner, and can be one of the following four categories:

- **Regulated:** Data that Integrity Marketing Group is legally required to protect, and for which the organization is legally obligated to issue communications to internal or external stakeholders in the event of a breach. This includes PII, PHI, PCI, and brand information protected under non-disclosure agreements. Data should be classified as Regulated if loss of that data results in a violation of any statute, act, or law, constitutes a violation of confidentiality agreed to as a condition of possessing, producing or transmitting data, or requires Integrity to self-report to the government and/or provide public notice if the data is inappropriately accessed.

- **Confidential:** Data that is not regulated by a governing body, but would damage the financial success or reputation of Integrity Marketing Group if it were exposed. This includes organizational trade secrets, internal intellectual property, and third-party intellectual property.

- **Internal Use:** Information that is intended for use by internal employees or authorized contractors when conducting Integrity Marketing Group business and would not damage the financial success or reputation of Integrity Marketing Group if it were exposed. This includes information such as Human Resources on-boarding procedures, organizational charts, or internal policies and procedures.

- **Public:** Data that would not adversely affect Integrity Marketing Group if it became public, including descriptions of organizational business offerings on websites and brochures, or telephone numbers of Integrity's various business units intended for publication. This data type requires Marketing and/or Legal authorization to make publicly available.

Data Retention
Integrity's Data Owners should adhere to defined retention timelines for all types of Integrity Marketing Group data. These timelines mandate retention of internal data in compliance with the organization's legal and regulatory environment, and apply to both data stored on live systems and data preserved in backups. Integrity's Data Owners should develop and maintain processes for the disposal of data after its retention period has expired. The disposal of data should be performed securely and in accordance with Integrity's Data Protection 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.

References

- PCI Data Security Standards v3.2.1
- The Health Insurance Portability and Accountability Act of 1996
- Data Protection and Lifecycle Policy

Data Protection and Lifecycle Policy — Last Revised: 02/02/2022	
Document Author	**Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com
Document Current Owner	**Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com
Document Approvers	**Name:** Harsh Singla **Title:** Chief Technology Officer **Email:** harsh.singla@integritymarketing.com **Name:** Steve Lundstrom **Title:** Senior Director of Software and Data Engineering **Email:** steve.lundstrom@integritymarketing.com **Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com

Data Protection Policy

Purpose

This Data Protection Policy mandates proper protections around the access, transmission, and storage of all enterprise and personal data in Integrity Marketing Group's ("Integrity") environment, in order to support Integrity's adherence to legal and regulatory data protection obligations.

Scope

This policy applies to data in all forms including electronic information, information stored in hard copy form, and information shared orally or visually through media such as telephone and video conferencing.

Definitions

Data Lifecycle: The data life cycle is the sequence of stages of a particular unit of data. This process begins when the data is first generated or captured, and ends when the data is no longer useful and has been archived and/or deleted

Controller: The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

Processor: A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

Roles & Responsibilities

Integrity Security Governance Committee: The Integrity Security Governance Committee is responsible for the development, implementation, maintenance, and enforcement of this policy. They are also responsible for approving a secure file transfer system for transmitting data outside the organization.

Data Owner: Data owners are responsible for defining protective measures for data based on its sensitivity as defined in the Data Classification Policy.

Integrity IT: The Integrity IT Team is responsible for the implementation of any processes and controls required for the protection of the organization's data, and for backing up data regularly.

Business Unit IT: Data owners are responsible for defining protective measures for data based on its sensitivity as defined in the Data Classification Policy.

Policy Statement

This policy addresses elements of the data lifecycle that warrant appropriate security measures. Integrity requires specific protections for each class of data outlined in the organization's Data Classification and Retention Policy. Specific solutions pertaining to the protection of Integrity's data, both corporate and retail, are architected by the Security Governance Committee, and

implemented by the Integrity IT Team. Additional details about specific solutions and implementations are described in Integrity's Data Protection Standard.

Storage

Data types owned by Integrity and stored on internal servers or client-facing devices, such as laptops, must be protected in accordance with their classifications.

- **Regulated:** Regulated data must be protected in accordance with all applicable laws and regulations and may not be stored on personal instances of third-party cloud storage applications. Regulated data must be encrypted at-rest and physically protected from unauthorized access.

  The amount of data stored and the period of storage are both limited to only what is necessary for performing core business activities.

- **Confidential:** Sensitive data must not be stored on open servers or file shares, and any servers or shares housing sensitive data must be physically protected from unauthorized access. Sensitive data must be encrypted at rest.

- **Internal:** Internal data may be stored on open file shares, but may not be stored in any location accessible to individuals outside the organization.

- **Public:** Public data may be stored digitally or in hard copy form, and in a public location.

Access

As a part of Integrity's efforts to protect data from unauthorized access, the organization only processes data necessary for an outlined business purpose. Employee access to that data is limited to only what is necessary for performing core business activities.

- **Regulated/Sensitive:** Regulated and Sensitive Data must only be accessible to employees who require that data for a legitimate business function, and are permitted to access that data by applicable laws and regulations. These data types require protections to enforce the Principle of Least Privilege, as described in the organization's Identity and Access Management Policy.

- **Internal:** Access to Internal Data must be moderated by a means of authorization (e.g. LDAP account login) to prevent access by individuals outside the organization. Where applicable, this access should be further limited by the Principle of Least Privilege, as described in the organization's Identity and Access Management Policy.

- **Public:** Public Data may be accessed freely by the general public, but the ability to edit Public Data must be restricted to employees of Integrity and approved by Marketing.

Transmission
Integrity also protects data in transit according to that data's classification.

- **Regulated/Sensitive:** Regulated and sensitive data must be transmitted using a strong encryption protocol, and may only be shared with external clients or partners through a secure file sharing system approved by the Information Security Governance Committee. Data of these types may not be transferred or shared using unapproved outside services (e.g. Google Drive, Dropbox, Box), and must be protected during transmission in compliance with any applicable laws or regulations.

- **Internal:** Internal data may be transferred or shared using the secure file sharing system described above, or using any additional outside services approved by the Information Security Governance Committee for transmission of internal data. Internal data may not be shared publicly.

- **Public:** Public data may be shared unencrypted through any form of electronic transmission but requires Marketing approval.

Backups
Integrity must backup enterprise data regularly, in accordance with approved timeframes, using approved methods for generation of secure backups, and stored securely in approved locations. This includes backups of all files and emails belonging to departing employees.

Disposal and Destruction
Paper copies of data should be shredded for disposal. Electronic data should be expunged, and digital media should be wiped clean of any residual data in accordance with internal requirements. Disposal of devices which store data must be performed in accordance with Integrity's Asset Management Policy.

Release of Information
The public release of any internal data requires the approval of the Security Governance Committee and must be compliant with all legal and regulatory requirements.

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.

References

- Data Classification Policy
- Identity and Access Management Policy
- Asset Management Policy
- NIST Special Publication 800-122: Guide to Protecting the Confidentiality of PII

Endpoint Protection Policy — Last Revised: 02/02/2022	
Document Author	**Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com
Document Current Owner	**Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com
Document Approvers	**Name:** Harsh Singla **Title:** Chief Technology Officer **Email:** harsh.singla@integritymarketing.com **Name:** Steve Lundstrom **Title:** Senior Director of Software and Data Engineering **Email:** steve.lundstrom@integritymarketing.com **Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com

Endpoint Protection Policy

Purpose

The purpose of this policy is to ensure implementation of controls on devices, Integrity Marketing Group (Integrity) and personal owned, to protect the confidentiality, integrity and availability of Integrity data. The objective is to reduce the risk of security breaches that could result from the connection and use of endpoint devices.

Scope

All Integrity employees or anyone performing work on behalf of Integrity (including contractors, consultants and volunteers) are subject to this policy. All workforce members and users, including third parties, who may have access or exposure to Integrity data are required to comply with this policy.

This policy covers all Endpoint devices connected to the internal Integrity network environment (includes networks of all Integrity Business Units) or which access Integrity data.

Definitions

Anti-Malware: Anti-malware is a type of software program designed to prevent, detect and remove malicious software (malware) on IT systems, as well as individual computing devices

End-of-Life System: An end-of-life (EOL) system is a system that does not receive continuing support, either because existing marketing, support and other processes are terminated, or it is at the end of its useful life

Full Disk Encryption: The process of encrypting all the data on the hard drive used to boot a computer, including the computer's operating system

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 Team: Integrity IT Team is responsible for maintaining an inventory of authorized and unauthorized software across Integrity. This includes deploying software inventory tools and also performing regular scans across their inventory for unauthorized software.

Business Unit IT: Business Unit IT Teams are responsible for establishing and ensuring standard secure configurations of software are being used across their business units within Integrity. They are also responsible for monitoring critical system files and reporting any unusual activity involving those critical files to the Integrity IT Team.

Policy Statement

Detection, prevention, and recovery controls to protect against malware must be implemented, combined with appropriate user awareness.

Anti-Malware: Business Unit IT Teams are required to ensure Integrity Marketing IT approved anti-malware software is actively running and cannot be disabled or altered by users, unless specifically authorized by Integrity Marketing IT management on a case-by-case basis for a limited time period.

Full Disk Encryption: Any portable endpoints that contain "Regulated" and "Confidential" data, as defined in the Data Classification policy, must have full disk encryption.

End-of-Life Systems: Endpoints running End-of-Life operating systems or software must be retired. Any endpoints running end-of-life system that cannot be retired due to a business need must have a documented justification approved by the Integrity Security Governance Committee and be isolated from the rest of the Integrity network.

Mobile Devices: A documented process must exist for management of the risks introduced by using mobile devices. All mobile devices connecting to Integrity's network or accessing Integrity data must follow the requirements set forth in the Acceptable Use Policy. All Integrity-owned mobile devices must be centrally managed by the Integrity IT Team.

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.

References

- Acceptable Use Policy
- Data Classification Policy

Identity & Access Management Policy — Last Revised: 02/02/2022	
Document Author	**Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com
Document Current Owner	**Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com
Document Approvers	**Name:** Harsh Singla **Title:** Chief Technology Officer **Email:** harsh.singla@integritymarketing.com **Name:** Steve Lundstrom **Title:** Senior Director of Software and Data Engineering **Email:** steve.lundstrom@integritymarketing.com **Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com

Identity and Access Management Policy

Purpose

The purpose of this policy is to mandate requirements for access management controls across the technological environment at Integrity Marketing Group ("Integrity"). This policy will aid Integrity in managing access to its information systems.

Scope

This policy applies to all information systems used throughout Integrity, whether managed centrally or in a distributed fashion, and to all individuals and entities who intend to access Integrity's 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.

Definitions

Authentication*: The process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system *

Authorization*: The granting or denying of access rights to a user, program, or process

Multi-Factor Authentication*: Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/personal identification number (PIN)); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

Principle of Least Privilege*: The security objective of granting users only those accesses they need to perform their official duties

Privileged Access Management (PAM)*: The process of managing and protecting credentials to accounts that have some level of administrative access to devices or systems, including local administrator accounts and superusers

Superuser*: A user that is authorized (and, therefore, trusted) to perform administrator-related functions that ordinary users are not authorized to perform

Temporary Privileged Account: An account issued to a non-privileged user for a pre-defined period of time, after which the credentials are changed to prevent future access

* - Definition taken from the Computer Security Resource Center Glossary: https://csrc.nist.gov/Glossary

Roles & Responsibilities

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

Data / Application Owner: The data or application owner is responsible for approving access to an organization's electronic data, and for enforcing protections to maintain the completeness, accuracy, validity, and integrity of the data or application environment.

Integrity IT: The Integrity IT Team serves as Data Custodian for systems under their purview and is responsible for administration of access control for the individual data, applications, and systems.

Business Unit IT: Business Unit IT Teams serve as Data Custodian for systems under their purview and are responsible for administration of access control for the individual data, applications, and systems.

Policy Statement

Any user who requests access to Integrity's information systems and data must have their identity authenticated, and further restricted in alignment with segregation of duties defined by the business. Access to data classified as "*Regulated*" and "*Confidential*" must be strictly limited following the Principle of Least Privilege.

The organization's access controls consider the risk level of the underlying information systems and data, and the locations from which users may request access, differentiating between internal network access or external network access.

Integrity shall maintain a process for user account provisioning, which includes creation of unique credentials for new users, modification of a user's access privileges in the event of a change in that user's role, and removal of a user's access privileges upon termination. Provisioning of user accounts must also adhere to the Principle of Least Privilege. If a user requires access to information beyond what their permissions allow, that request for access must be proposed to, and approved by, Integrity's Data / Application Owner. If this expanded access is granted, the user will be issued a temporary privileged account to prevent continued privileged access beyond the current business need.

Account credentials on all new systems or applications must be changed from default usernames and passwords immediately after first login. Elevated access privileges (e.g. administrative access rights) may only be provisioned to users as needed for legitimate business purposes, and the elevation of access privileges and provisioning of temporary privileged accounts must be conducted in accordance with Privileged Access Management (PAM) best practices.

When temporary privileged account credentials are issued to a user, the account password must be changed after that user has completed the business task for which the privileged account was

needed. Privileged account passwords must be complex, with a 15 character minimum. Users with access to privileged accounts must use their normal, least privileged account for their day-to-day job functions, and only utilize their privileged administrative account as needed.

Periodic audits of individual access rights must also be performed, either manually or with an automated tool. These periodic audits will review access permissions granted to users to help ensure that no individual can access information systems and data beyond what is necessary for a legitimate business purpose, and user access remains sufficiently restricted over time.

Enhanced security is also required for managing remote access to Integrity's network. Requirements for remote network access are outlined in the organization's Network Protection Policy.
Integrity shall also maintain a process for managing physical access to its information systems and data. Physical access to databases, servers, and other systems is limited to appropriate personnel .

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.

References

- Data Classification Policy
- Network Policy

Information Security Policy — Last Revised: 02/02/2022	
Document Author	**Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com
Document Current Owner	**Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com
Document Approvers	**Name:** Harsh Singla **Title:** Chief Technology Officer **Email:** harsh.singla@integritymarketing.com **Name:** Steve Lundstrom **Title:** Senior Director of Software and Data Engineering **Email:** steve.lundstrom@integritymarketing.com **Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com

Information Security Policy

Purpose

The Information Security Policy provides a structure for developing an organization-wide information security program comprised of a set of policies, standards, and practices that serve as the basis to assure information security for Integrity Marketing Group ("Integrity") and all of its Business Units. The Information Security Policy at Integrity defines the fundamental principles for the protection of information resources and the proper controls needed to ensure compliance with internal and external regulations to uphold Integrity's security posture and reputation.

The Information Security Policy states Integrity's responsibility for securing information assets and its delegation of that responsibility to Integrity's Business Units. The Information Security Policy and program reflects Integrity's commitment to protect the confidentiality, integrity and availability of information assets.

Scope

The concepts, policies, standards and initiatives within Integrity's Information Security Policy apply to Integrity and all of its Business Units. Each Business Unit must comply with the organization-wide information security program, associated policies, and standards as reviewed, approved and signed by the Vice President of Technology at Integrity.

All Integrity employees are responsible for the security and protection of electronic information resources over which they have control. Resources to be protected include, and are not limited to: networks, computers, software, and data. The physical and logical integrity of these resources must be protected against threats such as unauthorized intrusions, malicious misuse, or inadvertent compromise.

Integrity and its Business Units are able to develop more stringent local policies and standards that address specific local issues. Business Units may develop policies and procedures tailored to their environment that address areas not covered by organization-wide policies. If a Business Unit chooses to keep or develop information security policies or procedures of its own, those policies and standards are valid to the extent that they are more stringent than the requirements contained in the Integrity policies and standards, which constitute the mandatory baseline.

Roles & Responsibilities

Role	Job Functions	Responsibilities
Chief Technology Officer	1. Responsible for the overall planning, coordination and execution of the Information Technology functions across Integrity and its Business Units 2. Oversees the operation, maintenance, and availability of Integrity's IT infrastructure and associated services 3. In collaboration with the CISO, protects Integrity information and infrastructure from external or internal threats and assures that Integrity complies with applicable statutory and regulatory requirements	• Lead the overall strategic planning, budget and decision management processes related to Information Technology and ensure it aligns with Integrity's business mission • Oversee the IT on-boarding process for new Business Units including installation and configuration of new information technology equipment • As an IRT (Incident Response Team) member, primarily responsible for recommending policy and technology changes after any security incident
Chief Information Security Officer	1. Assumes the role of Risk Manager as it relates to Information Security Risk. At the Administration or Business Unit levels, manages, develops, and implements risk management programs, policies, and procedures appropriate to the organization. 2. Ensures continuity of information security program efforts with the Chief Privacy Officer 3. Maintains overall responsibility for developing and delivering a comprehensive information security program that complements and supports relating privacy and regulatory programs and requirements 4. Leads Integrity's information security activities including security monitoring, vulnerability management, risk management, and incident response to support Integrity's Information Security program	• Responsible for the overall security risk management across Integrity and ensuring that Integrity's information security program is established and aligns with the mission and vision of Integrity and its Business Units. • Responsible for serving as the Information Security representative on the Executive Leadership team • Responsible for interacting with Senior and Executive Leadership as it relates to Information Security • Ensure enforcement of Information Security policies at Integrity and its Business Units • Establish processes to measure Information Security risk and periodically report risk to the Information Security Governance Committee • Lead the overall strategic planning and decision management processes related to Information Security Policy Development • As a risk manager, conduct site visits, analyze risks, and accordingly update and maintain the risk register to continuously improve processes • Responsible for the incident response program including the review and update of the incident response plan and leading the Incident Response Team in an incident response scenario
Chief Compliance Officer	Manage the implementation of, and compliance with, Integrity Marketing Group's Privacy Policies and Procedures that provide guidance for the protection and safeguarding of all data classified as Regulated in the organization's Data Classification and Retention Policy	• Responsible for the development, implementation, and oversight of privacy and compliance related programs • Responsible for serving as the compliance and privacy representative on the Executive Leadership team

		• Responsible for interacting with Senior and Executive Leadership as it relates to compliance and privacy • Receive, document and respond to requests, complaints, and reports of alleged violations (security breaches) • Provide guidance and information about privacy related matters
Information Security Governance Committee	1. Facilitate making organization-wide, data-driven decisions regarding development, maintenance, and enforcement of Information Security Policies 2. Develop and foster a culture of information literacy and sharing across all Business Units, thereby enabling users to make informed decisions.	• Responsible for the overall execution of the information security program, including authorization of decisions regarding access, usage and risk levels associated with data across Integrity • Develop and provide framework that allows all key security decisions to be reviewed by key stakeholders • Develop a security improvement roadmap based on inputs from more focused security teams like the Risk Management team or Incident Response team
Compliance Leaders	Responsible for updating and coordinating privacy compliance at each of Integrity Marketing Group's Business Units.	• Assumes the role of Chief Compliance Officer delegate in day to day operations of managing privacy and compliance programs • Contributes to the oversight of privacy related policies and procedures • Receive, document and respond to requests, complaints, and reports of alleged violations (security breaches) • Provide guidance and information about privacy related matters
Site Privacy and Security Lead (Site Leaders)	1. Responsible for implementing the Integrity Marketing Group's HIPAA Privacy Program within the Business Units. 2. Responsible for implementing the Integrity Marketing Group's Information Security Program within the Business Units.	• Facilitating execution of information security initiatives as directed by the Information Security Committee • Data Governance, architecture, and management in conjunction with the Information Security Governance Committee • Develop and maintain privacy procedures in accordance with HIPAA Privacy Regulations and revise them periodically as required by changes in Integrity Marketing Group's HIPAA Privacy Program
Integrity IT Team	Perform security operations, information security threat analysis, and tools maintenance.	As leader of a team or individual performer: • Provide guidance to the Business Units to meet or maintain compliance with applicable policies, standards, baselines, guidelines, and laws. • Ensure security program operations and controls are being consistently performed or applied • Establishes procedures to oversee the acquisition of supplies and equipment schedules

		• Assess requirements for updates to security plans based on changes to business functions, technical vulnerabilities, and emerging threats
Business Unit IT Teams	1. Manages the operation of an information technology unit or area including computer hardware, software, networking and telecommunications equipment. 2. Plans, organizes, and controls all aspects of the operation including; supervision of respective Business Unit staff, prioritizing and assigning of the work, and coordinating activities with other Integrity Business Units.	• Provides technical support for all hardware and systems within the Business Unit • Recommends hardware acquisitions, the acquisition and maintenance of support equipment, and the contracting and procurement of new equipment and software for Integrity IT team approval

Policy Statement

All employees, contractors, and temporary or part-time workers, are responsible for ensuring that Integrity's information assets are used only in proper pursuit of the organization's operations; information is not improperly disclosed, modified, or endangered; and access to Integrity information resources is not made available to unauthorized personnel.
The Information Technology teams, and site leadership at each Integrity Business Unit, are responsible for following and enforcing the appropriate security controls as determined by Integrity Marketing IT. Business Unit IT Teams must evaluate all stored information, applications, and information systems to ensure compliance with the appropriate controls required to protect the information asset on the basis of its value to Integrity.

The Integrity Information Security Policy is intended to be a living document that must be periodically updated in order to maintain alignment with relevant developments around cybersecurity threats, risks, and compliance matters faced by the organization.

Policy Compliance

Compliance Measurement
Integrity shall monitor all its Business Units for compliance with the Information Security Policy. To ensure that the Information Security Policy is applied consistently across Integrity, each year Integrity will require all its Business Units to report their status with respect to implementing and complying with the organization-wide information security program.

Exceptions
While deviation from security policies is discouraged, an exception process exists that allows for certain scenarios which cannot be effectively addressed within the constraints of Integrity's security policies and standards, to be managed effectively and within the scope of Integrity's stated business outcomes.

Any potential exceptions to the information security policies and associated standards should be evaluated based on the risk associated with the particular situation. This should include factors related to data classification, business objectives, regulatory and compliance matters, systems and processing criteria, and technology.

Exceptions to the policy must be evaluated by the Integrity Information Technology function in conjunction with collaboration and input from other functions at the Business Unit level. When evaluating any exceptions, consideration must be given to any relevant compensating controls or mitigating factors.

Requests for exceptions to a policy must be submitted in writing to the Integrity VP of Technology. Exceptions shall be permitted only upon receipt of written approval from the Integrity VP of Technology. Integrity Information Technology will retain documentation of currently permitted exceptions.

Non-Compliance
Violations of the Information Security Policy may result in appropriate disciplinary measures in accordance with local, state, and federal laws, as well as the Standards of Conduct for all Integrity employees.

All personnel covered by the Information Security Policy are obligated to report apparent violations of this program or its associated policies and standards. If the violation does not appear to be resolved in a timely manner, the Integrity VP of Technology must be notified by the person observing the violation.

References

- Asset Management Policy
- Risk Management Policy

Network Policy — Last Revised: 02/02/2022	
Document Author	**Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com
Document Current Owner	**Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com
Document Approvers	**Name:** Harsh Singla **Title:** Chief Technology Officer **Email:** harsh.singla@integritymarketing.com **Name:** Steve Lundstrom **Title:** Senior Director of Software and Data Engineering **Email:** steve.lundstrom@integritymarketing.com **Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com

Network Policy

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

Definitions

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.

* - Definition taken from the Computer Security Resource Center Glossary: https://csrc.nist.gov/Glossary

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.

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 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.

References

- Data Protection and Lifecycle Policy
- Risk Management Policy

Password Protection Policy — Last Revised: 02/02/2022	
Document Author	**Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com
Document Current Owner	**Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com
Document Approvers	**Name:** Harsh Singla **Title:** Chief Technology Officer **Email:** harsh.singla@integritymarketing.com **Name:** Steve Lundstrom **Title:** Senior Director of Software & Data Engineering **Email:** steve.lundstrom@integritymarketing.com **Name:** Matthew Williams **Title:** Senior Director of Infrastructure & Information Security **Email:** matthew.williams@integritymarketing.com

Password Protection Policy

Purpose

The purpose of this policy is to establish a standard for creation of strong passwords and the protection of those passwords.

Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Integrity Marketing Group facility, has access to the Integrity Marketing Group network, or stores any non-public Integrity Marketing Group information.

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

Password Creation

All user-level and system-level passwords must conform to the Identity and Access Management Policy.

User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges. In addition, it required for all active accounts that some form of multi-factor authentication is used for any privileged accounts

Password Change

Passwords should be changed every 180 days or when there is reason to believe a password has been compromised.

Password cracking or guessing may be performed on a periodic or random basis by the Cybersecurity Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Identity and Access Management Policy.

Passwords that have been identified as compromised will be subject to a password hash comparison.

Password Protection

Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, Confidential Integrity Marketing Group information.

Passwords must not be inserted into email messages, or other forms of electronic communication, nor revealed over the phone to anyone.

Passwords may be stored only in “password managers” authorized by the Integrity Cybersecurity team.

Any user suspecting that his/her password may have been compromised must report the incident to Integrity Cybersecurity and change all passwords.

Application Development

Application developers must ensure that their programs contain the following security precautions:

Applications must support authentication of individual users, not groups.

Applications must not store passwords in clear text or in any easily reversible form.

Applications must not transmit passwords in clear text over the network.

Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

Multi-Factor Authentication
Multi-factor authentication is required for all active accounts and should be used whenever possible

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.

References

Physical Security Policy — Last Revised: 02/02/2022	
Document Author	**Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com
Document Current Owner	**Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com
Document Approvers	**Name:** Harsh Singla **Title:** Chief Technology Officer **Email:** harsh.singla@integritymarketing.com **Name:** Steve Lundstrom **Title:** Senior Director of Software and Data Engineering **Email:** steve.lundstrom@integritymarketing.com **Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com

Physical Security Policy

Purpose

The purpose of this policy is to ensure the confidentiality, integrity, and availability of Integrity Marketing Group's ("Integrity") information and systems located in approved facilities (e.g., business centers, data centers, etc.). This policy outlines the physical security measures to monitor and control physical access to Integrity premises and facilities housing Integrity information and technology systems. This policy aims to reduce and mitigate the risks of unlawful or unauthorized physical intrusion at Integrity.

Scope

This policy is applicable to all Integrity employees, contractors and third party vendors who have physical access to Integrity facilities, information resources, and systems. This policy is also applicable to rented, leased, or owned building/office space occupied by Integrity entities for the purpose of conducting normal day to day operations.

Definitions

Public Zone: Area within Integrity and its Business Units which is accessible to the public, including employees and guests. Data classified as Public as per the organization's Data Classification Policy shall be held at this zone.

Restricted Zone: Area within Integrity and its Business Units which is accessible to employees who have undergone background checks within Integrity and/or guests who have received authorization from the appropriate Business Unit Site Leader.

Confidential Zone: Area within Integrity and its Business Units where data classified as Regulated, as per the organization's Data Classification Policy, is held. This area shall be only accessible to workforce members who have privileged access to Regulated Data, as approved by the Business Unit Site Leaders.

Roles & Responsibilities

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

Site Leaders: Business Unit Site Leaders oversee the physical security access control and identity and access management processes and operations at their respective Integrity locations. Site Leaders are responsible for granting employees and visitors, access to Integrity's approved locations, as well as administering provisioning and de-provisioning of physical access for all employees and guests.

Integrity IT: Integrity IT Team is responsible for planning, developing, and updating the Integrity physical security program. With the help of Business Unit Site Leaders and other Business Unit stakeholders, Integrity IT Team oversees the implementation of the processes, operations and controls that support the physical security program. During the acquisition and integration of a new Business Unit, Integrity IT also provides the technical support and resources necessary for the implementation of new physical security equipment and technology.

Policy Statement

Integrity Marketing Group must implement processes and controls to protect the physical security of its approved facilities, in accordance with the security best practices below.

The organization's physical security access controls shall take into account the risk level of the underlying information systems and data, differentiating between three separate physical security zones (Public, Restricted, and Confidential).

Integrity shall identify all physical entry points to each of its Business Units. All Restricted and Confidential Zones shall be protected by badge reader system or similar technology. All employees and authorized guest users must wear badges at all times to indicate affiliation with Integrity.

Integrity shall, at a minimum, monitor all entry points to Confidential Zones by installing closed circuit television (CCTV) cameras that provide digitally recorded visual coverage of these zones. Cameras should be positioned to capture all ingress and egress points, capturing an inside view of the Confidential Zone as well as a view of outside the zone. Where feasible, Integrity recommends the installation of CCTV for all Restricted Zones as well. CCTV video recordings shall be stored for a minimum of 90 days.

Integrity shall install an alarm system for Confidential Zones that would send an alert to the Site Leaders and other responders in case of any unauthorized access. Integrity also recommends the installation of environmental hazards alarm systems, such as humidity and smoke sensors, particularly for Confidential zones housing hardware and other physical technology equipment.

Visitors, or Integrity facility users designated as guests, must be accompanied by an Integrity workforce member at all times. Visitor badges must be different from a regular employee badge thereby indicating that the badge holder is not an employee.

A lost badge must be reported to the Site Leaders immediately and it should be temporarily deactivated. A temporary visitor badge shall be issued to the said employee till a new permanent badge is issued and activated.

Depending upon feasibility, Integrity shall take measures to prevent tailgating in Restricted and Confidential zones within their data centers by installing physical deterrents at appropriate entry points.

Should an employee voluntarily or involuntarily part with Integrity Marketing, all company property must be returned and access disabled. Company property includes but is not limited to badges, keys, alarm codes, and workstations.

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 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.

Risk Management Policy — Last Revised: 02/02/2022	
Document Author	**Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com
Document Current Owner	**Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com
Document Approvers	**Name:** Harsh Singla **Title:** Chief Technology Officer **Email:** harsh.singla@integritymarketing.com **Name:** Steve Lundstrom **Title:** Senior Director of Software and Data Engineering **Email:** steve.lundstrom@integritymarketing.com **Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com

Risk Management Policy

Purpose

The purpose of this policy is to help ensure Integrity Marketing Group ("Integrity") has a consistent basis for measuring, controlling, monitoring, and reporting risk across the organization. This policy is a formal acknowledgement of Integrity's commitment to Risk Management.

Scope

This policy applies to all processes, procedures, and technologies in Integrity's business environment, and all associated risks.

Definitions

Risk*: The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, given the potential impact of a threat and the likelihood of that threat occurring.

Risk Register: A comprehensive list of identified risks facing the organization, including suggestions for mitigation and all progress made towards remediation or mitigation.

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 assuming the role of Risk Manager and is responsible for collecting input from periodic risk assessments, the organization's threat and vulnerability activities, and other internal processes to identify all security risks facing the organization. Taking into account Integrity's business needs, the Integrity IT team must also collaborate with the Security Governance Committee to develop the company's organizational risk tolerance. In addition to identifying sources of security risk, Integrity IT must track previously identified risks in a risk register.

Business Unit IT: Business Unit IT Teams are responsible for conducting any security risk assessments delegated to them by the Information Security Governance Committee, the Chief Compliance Officer, or the Integrity IT team as necessary.

Policy Statement

Risk Management is an integral part of Integrity's decision-making process for all areas of information security and is incorporated within the strategic and operational planning processes at all levels across the organization.

Risk assessments must be conducted on all new projects, systems, and vendors to ensure that the resulting exposure to additional risk is acceptable and formally approved before onboarding. Risk assessments must also be performed periodically for existing technologies to confirm that the organization's entire threat landscape and risk profile are understood. All risk assessment responsibilities are delegated by the Integrity IT team.

The Integrity IT team is also responsible for collecting risk information from the company's broader security processes. This includes information provided by threat intelligence, vulnerability management activities, and lessons learned from past incidents or incident simulations.
Risk register items guide the Integrity IT team in advising the Information Security Governance Committee and help to provide a complete picture of the company's risk profile. Risk assessment results are also used to determine potential security improvements that align with Integrity's business needs and risk tolerance.

Each identified risk must be analyzed to understand its potential impact and provide input and guidance for deciding on the most appropriate form of remediation or mitigation. Upon completion of the analysis phase, the Security Team provides the Integrity IT team with recommended steps to remediate identified risks. In the event a decision is made to forgo remediation efforts, acceptance of an identified risk must be proposed by the Integrity IT team and approved by the Information Security Governance Committee.

The risk register will guide efforts to remediate or mitigate risks with the intent to reach acceptable levels of risk for any project, system, or vendor. Final decisions on risk mitigation plans or acceptance of residual risks must be made either by the Information Security Governance Committee or by the Integrity IT team, if delegated. These decisions are also tracked in the risk register.

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.

References

- Risk Management Policy
- Data Classification Policy
- Asset Management Standard

Secure System Development Policy — Last Revised: 02/02/2022	
Document Author	**Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com
Document Current Owner	**Name:** Matthew Williams **Title:** Senior Director of Cybersecurity &Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com
Document Approvers	**Name:** Harsh Singla **Title:** Chief Technology Officer **Email:** harsh.singla@integritymarketing.com **Name:** Steve Lundstrom **Title:** Senior Director of Software and Data Engineering **Email:** steve.lundstrom@integritymarketing.com **Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com

Secure System Development Policy

Purpose

The purpose of this policy is to standardize secure system development for all Integrity Marketing Group, Inc. ("Integrity") systems, applications, and services through the use of industry best practices. The policy describes the requirements for developing new systems, applications, and services at Integrity and to ensure that all development work is compliant as it relates to any and all regulatory, statutory, federal, and/or state guidelines.

Scope

This policy applies to all Integrity employees and third party vendors/contractors involved in development or modification of Integrity systems, applications, and services.

Definitions

System Development Life Cycle*: The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal.

Configuration Management*: Collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.

Interface*: Common boundary between independent systems or modules where interactions take place.

Roles & Responsibilities

Integrity Security Governance Committee: The Integrity Security Governance Committee is responsible for the development, implementation, maintenance, and enforcement of this policy. The Security Governance Committee is responsible for periodically auditing and testing IT teams' SDLC practices to assess their security posture and conformance to this policy.

Integrity IT: Integrity IT Team is responsible for performing risk assessments on acquired entities' System Development Life Cycle and providing guidance to help Business Unit IT Teams securely develop and implement systems, applications, and services.

Business Unit IT: Business Unit IT Teams are responsible for addressing, implementing and documenting secure practices for systems, applications, and services development for all new and

* - Definition taken from the Computer Security Resource Center Glossary: https://csrc.nist.gov/Glossary

existing Integrity systems. In addition Business Unit IT Teams are responsible for reporting and tracking deficiencies in SDLC systems under their purview

Policy Statement

Integrity Marketing Group must implement processes and controls for the secure development of enterprise software in accordance with the security best practices below.

Software Development Environments: Development, testing, and operational environments must be separated to reduce the risks of unauthorized access or changes to the operational environment. "Regulated" and "Confidential" data, as defined in the Data Classification policy, must not be used in the development or test environments.

Requirements Documentation: Information security requirements must be included in the requested requirements for new systems or enhancements to existing systems. Data owners, along with system administrators, are required to document key system security information, including external interfaces and types of information processed, stored, or transmitted.

System Development Life Cycle (SDLC): For all significant development or acquisitions, Data Owners, in collaboration with Data Custodians, are required to manage systems using a secure System Development Life Cycle model. For any SDLC model that is used, information security should be integrated into the SDLC model to ensure appropriate protection for the information the system will transmit, process, and store.

Development Rules: Rules for the development of software and systems must be established and applied to all system development efforts within the organization. Data owners, along with developers, must utilize industry-recognized best practices to build secure applications. Testing of security functionality should be carried out during development.

Configuration Management (CM): Configuration management and control activities should be conducted to document any proposed or actual changes in the security plan of a given information system. Business Units should strive for consistency in CM practices across the business but may need to develop or tailor CM strategies.

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.

Third-Party Risk Management Policy — Last Revised: 02/02/2022	
Document Author	**Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com
Document Current Owner	**Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com
Document Approvers	**Name:** Harsh Singla **Title:** Chief Technology Officer **Email:** harsh.singla@integritymarketing.com **Name:** Steve Lundstrom **Title:** Senior Director of Software and Data Engineering **Email:** steve.lundstrom@integritymarketing.com **Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com

Third-Party Risk Management Policy

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.

Definitions

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.

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.

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 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.

References

- Asset Management Policy
- Risk Management Policy

Threat and Vulnerability Management Policy — Last Revised: 02/02/2022	
Document Author	**Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com
Document Current Owner	**Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com
Document Approvers	**Name:** Harsh Singla **Title:** Chief Technology Officer **Email:** harsh.singla@integritymarketing.com **Name:** Steve Lundstrom **Title:** Senior Director of Software and Data Engineering **Email:** steve.lundstrom@integritymarketing.com **Name:** Matthew Williams **Title:** Senior Director of Cybersecurity & Cloud Engineering | CISO **Email:** matthew.williams@integritymarketing.com

Threat and Vulnerability Management Policy

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.

Definitions

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.

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	9.0-10.0	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.

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.