P2000 - Acceptable Use Policy

Contents

Purpose:..... 3
Scope:..... 3
Statement:..... 3
Policy Sections:..... 9
Section A: Roles and Responsibilities 9
..... 14
Policy References:..... 15
Related Procedure References:..... 15
Related Regulatory Information:..... 15

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 Integrity. Inappropriate use exposes Integrity to risks including virus attacks, compromise of network systems and services, and legal issues.

The intention behind Information Security's publication of an Acceptable Use Policy is not to impose restrictions that go against Integrity's established culture of openness, trust, and integrity. Instead, Information Security is committed to safeguarding Integrity's employees, partners, and the company from any illegal or damaging actions, whether intentional or unintentional, by individuals.

The Internet/Intranet/Extranet-related systems, comprising of computer equipment, software, operating systems, storage media, and network accounts for electronic mail, WWW browsing, and FTP, are owned by Integrity. These systems are designated for exclusive use in business-related activities that serve the best interests of the company, clients, and customers as a part of regular operations.

Security is a collective effort that requires the participation and support of all Integrity team members. It is the responsibility of every computer user to familiarize themselves with these guidelines and to align 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 and staffed contractors hold responsibility for the security and protection of electronic information resources that are under their control. These resources encompass, but are not limited to, networks, computers, software, and data. It is crucial to safeguard the physical and logical integrity of these resources from threats like unauthorized intrusions, malicious misuse, or inadvertent compromise.

Statement:

General Use and Ownership

Integrity proprietary information stored on electronic and computing devices whether owned or leased by Integrity, the employee, staffed contractor 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 staffed contractors have a responsibility to promptly report the theft, loss or unauthorized disclosure of Integrity proprietary information.

Integrity employees, and staffed 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 and staffed contractors 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

Integrity's information systems, devices, networks, applications, and communication tools are provided for business purposes. Incidental personal use is permitted only when it is minimal, infrequent, and does not interfere with job responsibilities, productivity, system performance, or security controls.

Such use must comply with all Company policies, legal and regulatory requirements, and must not result in additional cost, risk, or liability to the Company. All activity on Company resources is subject to monitoring, and users should have no expectation of privacy.

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. Integrity is not responsible for any loss of information, such as information stored in the wallet, or any consequential loss of personal property.

Personal Use refers to non-business-related, occasional, and brief use of Company resources, including activities such as:

- Checking personal email or messages
- Scheduling personal appointments
- Limited browsing for personal errands

Personal Use does not include:

- Operating a business or commercial activity
- Excessive or repeated non-work use
- Downloading/installing unauthorized software or applications
- Accessing, storing, or transmitting inappropriate, illegal, or high-risk content
- Any activity that compromises security, violates Company policy, or impacts system performance

Right to Monitor

The Information Technology Department will conduct monitoring of Internet usage from all computers and devices connected to the corporate network. The monitoring system will record the source IP address, date, time, protocol, and destination site or server for all traffic. Whenever feasible, the system should also capture the User ID of the individual or account responsible for initiating the traffic. This monitoring measure is in place to ensure compliance with company policies and to maintain the security and integrity of the corporate network.

Internet Use Filtering System

The Information Technology Department may block access to internet websites and protocols that are deemed inappropriate for Integrity's corporate environment. The following categories of websites are categories that may be blocked, including, without limitation:

- 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 Exceptions

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

Individuals may access blocked sites with proper permission if it is deemed necessary for legitimate business purposes. To request access to a blocked site that is appropriately categorized, individuals must submit a written or email request to their Human Resources representative. HR will then present all approved exception requests to Information Technology. Approved exceptions will be granted exclusively to the requesting associate, and Information Technology will keep a record of approved exceptions and provide reports upon request.

Security and Proprietary Information

System level and user level passwords must comply with the P2007 - Identity & Access Management Policy, and P2010 - Password Protection Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited

All computing devices must have a password-protected screensaver enabled, with the automatic activation feature set to 30 minutes or less. It is mandatory to lock the screen or log off when the device is unattended. This measure ensures that sensitive information is protected from unauthorized access and helps maintain security of the computing devices.

Using an Integrity email address to make postings to media sources is strictly prohibited, unless such postings are directly related to official business duties and fully comply with all other Integrity policies on external communication,

including those outlined in the Employee Handbook. This policy is in place to maintain consistent and appropriate communication with media sources in alignment with Integrity's guidelines and procedures.

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

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.

Unacceptable Use

The following activities are generally prohibited, but individuals may be exempted from these restrictions if it is necessary to fulfill their legitimate job responsibilities. For example, systems administration staff may need to disable network access for a host that is disrupting production services. This exception is granted in order to ensure smooth functioning of business operations while maintaining appropriate security measures.

Under no circumstances is an employee or staffed contractor of Integrity authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Integrity-owned resources. Any use of Integrity's systems must comply with all applicable laws, including CAN SPAM, applicable CMS's marketing guidelines and all of Integrity's policies and procedures.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

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 individual's host, unless this activity is a part of the individual'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 individual'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 Integrity, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of Integrity ".

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. Individuals 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.
- Forwarding Integrity emails to non-Integrity managed 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.

Accessing an Integrity email account belonging to another individual requires authorization by Integrity Cybersecurity and Human Resources.

The use of a personal email for any Integrity business is prohibited. No emails should be forwarded to a non-Integrity managed email account unless an exception is granted by Integrity Cybersecurity.

Integrity may periodically provide phishing and related training and testing to all users of its email system. Completion of any training issued to users is a requirement for continued use of the Integrity IT systems.

Social Media

- The use of social media by employees is subject to the terms and restrictions included in the Employee handbook.
- Team members that are not Integrity employees shall not use Integrity resources or systems to use social media.

Generative AI tools usage

Employees may use Artificial Intelligence (AI) tools only for legitimate business purposes and only if the tool and its use case comply with the organization's P2016 - AI Governance and Responsible Use Policy. Unauthorized or unapproved AI tools or use cases are prohibited.

AI tools must not be used in ways that violate laws, regulations, contractual obligations, or Integrity's Core Values, including uses that could result in bias, unfair treatment, misleading content, or inappropriate automation of decision-making.

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 to address scenarios that cannot be effectively managed within the constraints of Integrity's security policies and standards. This exception process allows for effective management of such scenarios while aligning with Integrity's stated business outcomes. However, exceptions should be rare and carefully reviewed and approved by the appropriate parties to ensure that they do not compromise the overall security posture of the organization.

Any potential exceptions 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 this 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 this Policy must be submitted in writing to Information technology. Exceptions shall be permitted only upon receipt of written approval. Integrity Information Technology will retain documentation of currently permitted exceptions.

Non-Compliance

Violations of this Acceptable Use Policy may result in appropriate disciplinary measures in accordance with local, state, and federal laws.

All personnel covered by this Policy are obligated to report apparent violations of this program or its associated policies and standards.

Policy Sections:

Section A: Roles and Responsibilities

Section Name: Roles & Responsibilities

Statement:

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	• Overseeing the overall security risk management across Integrity and ensuring that the information security program is established and aligned with the mission and vision of Integrity and its Business Units. • Serving as the Information Security representative to the Executive Leadership team and interacting with Senior and Executive Leadership on information security matters. • Ensuring enforcement of Information Security policies at Integrity and its Business Units.

	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.	• Establishing processes to measure Information Security risk and periodically reporting risk to the Information Security Governance Committee. • Leading the overall strategic planning and decision management processes related to Information Security Policy Development. • Conducting site visits as a risk manager, analyzing risks, and updating and maintaining the risk register to continuously improve processes. • Leading the incident response program, including reviewing and updating the incident response plan and leading the Incident Response Team in incident response scenarios
Vice President Enterprise Risk Management	Manage the implementation of, and compliance with, Integrity Marketing Group's Privacy Policies and Procedures across the Integrity enterprise, in coordination with each Business Units' compliance teams (see below) that provide guidance for the protection and safeguarding of all data classified as Regulated in the organization's Data Classification and Retention Policy.	• Managing the implementation of, and compliance with, Integrity's Privacy Policies and Procedures that provide guidance for the protection and safeguarding of all data classified as Regulated in Integrity's Data Classification and Retention Policy. • Overseeing the development, implementation, and

		oversight of privacy and compliance related programs. • Serving as the compliance and privacy representative to the Executive Leadership team and interacting with Senior and Executive Leadership on compliance and privacy matters. • Receiving, documenting, and responding to requests, complaints, and reports of alleged violations related to privacy. • Providing guidance and information about privacy-related matters to employees and stakeholders.
Information Security Governance Committee	1. Facilitate making organization-wide, datadriven 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.	• Executing the information security program, including authorization of decisions regarding access, usage and risk levels associated with data across Integrity. • Developing and providing a framework that allows all key security decisions to be reviewed by key stakeholders. • Developing a security improvement roadmap based on inputs from more focused security teams.
Compliance Deputies or Compliance Officers at each Business Unit	Responsible for updating and coordinating privacy compliance at each of Integrity's Business	• Assuming the role of Compliance Officer delegate in day-to-day

	Units.	operations of managing privacy and compliance programs at a Business Unit. • Contributing to the oversight of privacy related policies and procedures at the applicable Business Unit. • Receiving, documenting, and responding to requests, complaints, and reports of alleged violations related to privacy at the Business Unit. • Providing guidance and information about privacy-related matters to employees and stakeholders at the Business Unit. • Coordinating with the Compliance Officer to maintain Integrity's overall compliance.
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 References:

Policy Status	Document Name	Category	Document Author	Document Owner	Document Version Number	Last Published Date
Active	P2016 - AI Governance and Responsible Use Policy	2000 - Information Technology	Sumit Dhawan	Matt Williams	5.0	3/30/2026
Active	P2010 - Password Protection Policy	2000 - Information Technology	Jeremy Hart	Matt Williams	3.0	1/21/2026
Awaiting Document Owner Approval	P2004 - Data Classification Policy	2000 - Information Technology	Matt Williams	Matt Williams	2.0	4/8/2025
Active	P2007 - Identity & Access Management Policy	2000 - Information Technology	Jeremy Hart	Matt Williams	3.0	1/21/2026
Awaiting Document Owner Approval	P2009 - Network Policy	2000 - Information Technology	Matt Williams	Matt Williams	2.0	4/8/2025
Pre-Published	P2001 - International IT Resource Policy	2000 - Information Technology	Sumit Dhawan	Matt Williams	2.0	5/21/2026
Awaiting Document Owner Approval	P2021 - Email Policy	2000 - Information Technology	Sumit Dhawan	Matt Williams	1.0	4/8/2025
Active	P2024 - Chat Platform Usage Policy	2000 - Information Technology	Sumit Dhawan	Matt Williams	1.0	11/26/2025

Related Procedure References:

Related Regulatory Information:

P2000 - Acceptable Use Policy		
Document Author	**Name:** **Title:** **Email:**	Sumit Dhawan Manager Cybersecurity Compliance Sumit.Dhawan@integrity.com
Document Owner	**Name:** **Title:** **Email:** **Approved Date:**	Matt Williams Senior Director Cybersecurity & Cloud Engineering CISO matthew.williams@integrity.com 5/20/2026
Legal Management Approval	**Name:** **Title:** **Email:** **Approved Date:**	Vernie Hsu Deputy General Counsel Integrity/General Counsel Integrity Wealth vernie.hsu@integrity.com 5/20/2026
Executive Management Approval	**Name:** **Title:** **Email:** **Approved Date:**	Harsh Singla Chief Product and Technology Officer Harsh.Singla@integrity.com 5/21/2026

Last Published Date: 5/21/2026

Document Version Number 3.0