P2002 - Asset Management

Contents

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.

Statement:

Roles & Responsibilities

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

Integrity IT: The Integrity IT Team is responsible for 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

Asset Identification and Inventory

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 shall be protected against theft, mishandling, and accidental damage. Information about all IT assets shall be maintained in a single asset inventory, in which asset information is tracked, managed, and audited throughout their lifecycle.

IT assets shall be uniquely identified and inventoried upon acquisition or deployment. The Integrity IT Support Services Team shall maintain an accurate inventory of all assets, including their location, configuration, and ownership information in an IT Asset Inventory. IT Asset Inventory shall be maintained in an automated tool to ensure up-to-date, complete, accurate, and unique inventory of assets.

The IT Asset Inventory shall include the following standardized data fields as per applicability:

- Enterprise asset identifier
- Date of purchase

- Purchase price
- Item description
- Manufacturer
- Model number
- Serial number
- Name of the enterprise asset owner (e.g., administrator, user), role, or business unit, where applicable.
- Physical location of enterprise asset, where applicable
- Physical (Media Access Control (MAC)) address
- Internet Protocol (IP) address
- Warranty expiration date
- Any relevant licensing information

Asset inventory records shall be regularly updated to reflect changes in asset status, such as acquisitions, disposals, transfers, or decommissioning. All assets shall be tracked and linked back to the asset inventory to provide visibility into asset location, type, classification, and owner. This inventory shall be utilized for operational and security related tasks, such as auditing, protection, responding to incidents, and risk management. Periodic audits shall be conducted to validate the accuracy of asset inventory records. Regular audits help identify discrepancies, update asset statuses, and maintain data integrity.

Tracking of assets shall be done via asset tagging or the use of another unique identifier for efficient asset tracking. This enables easy identification and location of assets, especially in large-scale environments.

During asset onboarding, all asset information shall 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 shall also be reflected in the asset inventory.

Decisions about acquisition, maintenance, and disposal of assets shall 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.

Asset Acquisition and Deployment

All acquisitions of IT assets shall be authorized by the appropriate departmental authority and documented accordingly. IT assets shall only be deployed in accordance with approved configurations and usage policies. Proper documentation of asset acquisitions, including purchase orders, invoices, and license agreements, shall be retained for audit purposes.

Asset Monitoring and Maintenance

IT assets shall be monitored regularly to detect and prevent unauthorized activities, security breaches, or performance issues. Regular maintenance and updates shall be performed to ensure the security and functionality of IT assets.

All Integrity system assets shall 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 shall 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.

Asset Disposal and Decommissioning

IT assets shall be disposed of or decommissioned in accordance with established procedures and regulatory requirements. Data sanitization procedures shall be applied to remove sensitive or confidential information from decommissioned assets before disposal or repurposing. Integrity shall maintain a process for the off-boarding of assets which includes the use of approved vendors. All disposal and destruction of assets shall be performed in compliance with the organization's legal and regulatory environment. Proper documentation of asset disposal, including disposal certificates and asset retirement records, shall be maintained for audit purposes.

Asset Auditing and Compliance

Regular audits of IT assets and related processes shall be conducted to ensure compliance with this policy and applicable regulations. Audit trails and logs must be maintained to track changes to IT assets, user activities, and security events. Any non-compliance with this policy or identified deficiencies must be promptly addressed and remediated.

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

Policy Sections:

Policy Compliance

Section Name: Policy Compliance

Statement:

Compliance Measurement

The Integrity Security Governance Committee will verify compliance with this policy through various methods, including but not limited to, periodic walk-throughs, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Integrity Security Governance Committee in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A contractor found to have violated this policy may be subject to an immediate termination of the right to access Integrity's systems and may also include the termination of Integrity's engagement with the contractor's employer.

Policy References:

Policy Status	Document Name	Category	Document Author	Document Owner	Document Version Number	Last Published Date
✔ Active	P2012 - Risk Management Policy	2000 - Information Technology	Matthew Williams	Matthew Williams	2.0	4/8/2025
✔ Active	P2015 - Threat and Vulnerability Management Policy	2000 - Information Technology	Matthew Williams	Matthew Williams	2.0	4/8/2025
✔ Active	P2004 - Data Classification Policy	2000 - Information Technology	Matthew Williams	Matthew Williams	2.0	4/8/2025

Related Procedure References:

Related Regulatory Information:

P2002 - Asset Management		
Document Author	**Name:** **Title:** **Email:**	Jeremy Hart Asureti - Manager jeremy.hart@asureti.com
Document Owner	**Name:** **Title:** **Email:** **Approved Date:**	Matthew Williams Senior Director Cybersecurity & Cloud Engineering CISO matthew.williams@integrity.com 10/21/2025
Legal Management Approval	**Name:** **Title:** **Email:** **Approved Date:**	Duncan McQueen Assistant General Counsel duncan.mcqueen@integrity.com 1/16/2026
Executive Management Approval	**Name:** **Title:** **Email:** **Approved Date:**	Harsh Singla Chief Product and Technology Officer Harsh.Singla@integrity.com 1/21/2026

Last Published Date: 1/21/2026

Document Version Number 3.0