P2004 - Data Classification Policy

Contents

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.

Statement:

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.

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.

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.

Policy Sections:

Policy Compliance

Section Name: Policy Compliance

Statement:

Compliance Measurement

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

Exceptions

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

Non-Compliance

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

Policy References:

Document Name	Category	Document Author	Document Owner
P2005 - Data Protection and Lifecycle Policy	2000 - Information Technology	Matthew R Williams	Matthew R Williams

P2004 - Data Classification Policy		
Document Author	**Name:** **Title:** **Email:**	Matthew R Williams Senior Director, Cybersecurity & Cloud Engineering, CISO matthew.williams@integrity.com
Document Owner	**Name:** **Title:** **Email:** **Approved Date:**	Matthew R Williams Senior Director, Cybersecurity & Cloud Engineering, CISO matthew.williams@integrity.com 1/30/2025
Legal Management Approval	**Name:** **Title:** **Email:** **Approved Date:**	Duncan William McQueen Assistant General Counsel duncan.mcqueen@integrity.com 2/17/2025
Executive Management Approval	**Name:** **Title:** **Email:** **Approved Date:**	Harsh Singla Chief Technology Officer Harsh.Singla@integrity.com 4/8/2025

Last Published Date: 4/8/2025

Document Version Number 2.0