P2011 - Physical Security Policy

Contents

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.

Statement:

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.

Any third-party request for a copy of the digital records must be approved by (a) the Chief Human Resources Officer or the Human Resources Business Partner Director and (b) any Assistant General Counsel or the Chief Legal Officer. In an emergency, the Chief Information Security Officer may also approve a request if an authorized representative from Human Resources and Legal are not available.

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 or contractor 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.

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.

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:

P2011 - Physical Security Policy		
Document Author	**Name:** **Title:** **Email:**	Matthew R Williams Senior Director, Cybersecurity & Cloud Engineering, CISO matthew.williams@integrity.com
Document Owner	**Name:** **Title:** **Email:** **Approved Date:**	Matthew R Williams Senior Director, Cybersecurity & Cloud Engineering, CISO matthew.williams@integrity.com 1/30/2025
Legal Management Approval	**Name:** **Title:** **Email:** **Approved Date:**	Duncan William McQueen Assistant General Counsel duncan.mcqueen@integrity.com 3/27/2025
Executive Management Approval	**Name:** **Title:** **Email:** **Approved Date:**	Harsh Singla Chief Technology Officer Harsh.Singla@integrity.com 4/8/2025

Last Published Date: 4/8/2025

Document Version Number 2.0