P2003 - Business Continuity and Disaster Recovery Policy

Contents

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.

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 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.

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

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
P2002 - Asset Management	2000 - Information Technology	Jeremy Hart	Matthew R Williams

P2003 - Business Continuity and Disaster Recovery 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