P2017 - Backup and Restoration Policy

Contents

Purpose:

The purpose of this policy is to establish a framework for the systematic backup and restoration of Integrity, LLC ("Integrity") organizational data, ensuring data availability, integrity, and timely recovery in the event of data loss, system failures, or other unforeseen incidents.

Scope:

This policy applies to all electronic data generated, processed, or stored on Integrity's organizational systems, encompassing both on-premises and cloud-based data storage solutions.

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.

System Administrator: System Administrators must oversee both backup execution and regular validation to guarantee backup reliability. They must document procedures comprehensively, including recovery steps and escalation protocols. They shall collaborate with other stakeholders to establish and review backup and recovery objectives periodically to ensure alignment with business needs and technological advancements.

Application Owner: Application Owners shall collaborate closely with System Administrators to define data classification and backup requirements accurately. They shall actively participate in testing backup and recovery procedures for their applications to verify data integrity and application functionality after restoration. Application Owners shall also ensure that any changes or updates to the application are reflected in the backup and restoration processes promptly.

Hosting/cloud provider: Hosting/cloud provider shall be responsible for the backup strategies in their environment. They shall implement robust security measures to protect backup data from unauthorized access or tampering. They shall regularly audit backup systems for compliance with industry standards and regulations, such as SOC or ISO 27001, and provide transparent reports to customers regarding backup procedures and security measures.

Policy Statement

Regular Backups

All devices and applications having Integrity's data and information that cannot be easily reproduced shall be backed up regularly to mitigate the risk of data loss. Automation of backup processes shall be implemented wherever possible to minimize the risk of human error and ensure consistency and reliability in backup procedures.

Data Classification

Data shall be classified based on its sensitivity, confidentiality, integrity, and availability requirements, as well as its business criticality, to determine backup frequencies, retention periods, and security measures. Regular review and updates to the data classification scheme shall be conducted to accommodate changes in business priorities, technology, and regulatory landscape.

Retention Periods

Please refer to the Data Retention policy, which outlines the rules and regulations mandating the retention of specific documents for a designated period.

Data Integrity and Encryption

Regular integrity checks shall be performed on backup data to detect and mitigate any potential data corruption or tampering. When off-site storage is utilized, the hosting or cloud provider will be responsible for documenting integrity and availability processes.

Backup data shall be encrypted in transit as well as rest to protect it from unauthorized access or interception. Strong encryption algorithms shall be used to ensure confidentiality and integrity of data.

Offsite Storage and Geographic Redundancy

Approved cloud solutions for backups shall undergo thorough evaluation to ensure compliance with security standards and regulatory requirements. Encryption of backup data before transfer and storage in the cloud shall adhere to industry-standard encryption protocols and key management practices to maintain data confidentiality and integrity.

Regular audits and assessments shall be conducted to verify compliance with encryption and geographic redundancy requirements, with findings communicated to relevant stakeholders for remediation and improvement.

Restoration

Any data restore request shall be logged through the Integrity approved system (ticketing tool system). Users requesting a restores are required to provide all the details about the restore request, which shall include:

- The reason for the restore.
- The name of file/s and/or folder/s to be restored.
- Original location of file/s and/or folder/s.
- Date, day or time of deletion/corruption or nearest approximation.
- The last date, day, or time which the User recalls the data (files) being intact and accessed/used successfully.

All backup and recovery (restore) procedures must be documented by the System Administrator who will be responsible for conducting data (file) restores. Personnel accessing backup media for the purpose of a restore must ensure that any media used is returned to a secure location when no longer required (applies to media from both Integrity and remote storage locations). Users must request data (files) to be restored by contacting the System Administrator by raising restore request in Integrity approved system (ticketing system). Only files which the user is authorized to access will be provided from the restore. System Administrator will need to verify that the

User has permission and/or authorisation to view or obtain restored copies of file/s and/or folder/restores requested for information older than thirty (30) days will need to have further departmental approval before being undertaken. Backups are kept for a maximum of three (3) months after which no restores will be possible. Content will be restored to the same source folder, or the same area as mentioned in the ticket, so any requestor will need access to that folder/area to access the restored file. A log must be maintained to record the use of backup media whenever it has been requested and/or used from secure storage. The access to restored data shall be permitted to authorised owner of the data. The person appointed for User Acceptance Test of the restoration shall be appointed by the application owner. System Administrator or hosting/cloud provider shall give an estimation of how long a restore of a server/application will take. The restore time shall be approved by the IT Application Owner. The IT application owner shall be responsible for having the agreement about the restore time in place. The hosting/cloud provider is responsible that this restore time will be met.

Testing and Validation

Regular testing of the restoration process to confirm the viability and integrity of backup data shall be mandated. Backups shall be tested regularly to ensure data quality. A restore test shall be done at least annually to verify the restorability. In case of off-site storage, the hosting/cloud provider must have testing and verification strategies to ensure that the backups are possible to restore. Documentation of the testing result shall be maintained for audit purposes.

Documentation

Comprehensive documentation outlining backup procedures, schedules, incident response procedures, including escalation paths and communication channels and contact information for personnel responsible for backup management shall be maintained and made available to the application users.

Change Management

All changes to the backup schedule and configuration shall go through standard change management process (refer change management policy). Any change to the backup policy shall be approved by the Integrity management team and thorough impact analysis needs to be performed before approval.

Monitoring and Auditing

Real-time monitoring of backup systems shall be complemented by proactive alerting mechanisms to promptly identify and address any backup failures or anomalies. Incident response plans shall include predefined roles and responsibilities, escalation procedures, and communication channels to facilitate timely resolution of backup-related incidents and minimize their impact.

Disaster Recovery Plan Integration

Backup and restoration policies shall be fully integrated into the organization's disaster recovery plan, with regular exercises and simulations conducted to validate the effectiveness of recovery procedures. Integration efforts shall encompass not only data backup but also application recovery, infrastructure provisioning, and communication protocols to ensure comprehensive disaster recovery capabilities.

Vendor Support

Application owners shall establish clear expectations with vendors regarding backup processes, including compliance with business and regulatory requirements. Contracts with vendors shall include provisions for regular audits and assessments of backup processes to verify compliance and ensure alignment with organizational objectives.

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:

Related Procedure References:

Related Regulatory Information:

P2017 - Backup and Restoration Policy		
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 2.0