Computer Information Development, LLC

Backup and Data Retention Policy

Revision: 3.2

Classification: Operational

Contents

1. Overview

Any service-related configuration, code used for operations, and production data must be backed up consistently and often to ensure system recoverability in the event of disaster or media failure.

Additionally, this policy covers data destruction as the last part of a data retention methodology. Customer data is often destroyed as part of contractual agreements. Consumer-level data destruction is required for internal and external privacy policies, industry practices, and local, federal, and international regulations.

2. Scope

This policy applies to all data stored on company-owned, company-leased, and otherwise company-provided systems and media. This policy covers the types of data to be backed up, frequency of backups, storage and retention details, and backup restoration procedures.
Note: This policy may be superseded in part or whole by regulatory or contractual requirements.

3. Policy

3.1. Special Note Regarding Encrypted Data

In many cases, data inside encrypted databases will be migrated to new encrypted data stores over encrypted channels, facilitating secure transmission and secure backup. In cases where the data to be saved is offline, it will be important to assess future decryption capabilities and, if necessary, retain associated decryption keys for legacy data repositories.

3.2. Backup Frequency, Storage and Retrieval

3.2.1 — Backups shall be labeled descriptively and accurately.

3.2.2 — Backups shall happen routinely, based on business need, and alert on failure.

3.2.3 — Backups shall be stored in secure cloud storage under security controls consistent with the controls prior to backup.

3.2.4 — Backups shall be tested to ensure viability, and restoration procedures shall be documented.

3.2.5 — Backups of Confidential data must be protected by means of encryption adhering to CID's Encryption Policy.

3.2.6 — In instances of backup or general data storage on any Non-electronic or electronic media within CID's control outside of the cloud-based backup system, the media must be inventoried prior to being transported offsite.

The transport inventory must include at a minimum:

3.2.6.1 — who performed the inventory

3.2.6.2 — who the media was provided to

3.2.6.3 — the transport date

3.2.7 — Returned or retrieved media must be recorded on reception following the same inventory standards.

3.3. Backup and Retention Details by Data Definition

The following backup and retention guidelines apply based on definitions defined in CID's Data Classification policy:

3.3.1. Unrestricted Data

Unrestricted data will not be retained or backed up by policy.

3.3.2. Local User Data

In general, local (i.e. laptop) user data will not be retained. User workstations can be wiped by Infrastructure prior to device reassignment or at any other time required according to company needs or requirements.

3.3.2.1. Local User Data Retention Exceptions

Local user data may be retained in cases of incident, investigation, or archival importance.

3.3.3. Operational

Operational data should be backed up weekly on a secure cloud platform and shall be retained for 5 years.

3.3.4. Company Proprietary Data

Company proprietary data shall be retained for no less than 5 years and shall be retained until explicitly deemed fit for deletion by a Compliance Officer, who will assess the need for permanent retention of archive copies.

Company proprietary data shall be backed up on a secure cloud platform.

3.3.5. Transaction Audit Data

Transaction Audit Data shall be retained for 3 to 7 years, according to customer-specific industry standards and requirements (contractual, regulatory, or legal).

3.3.6. PII (Non-audit data)

Information related to individuals will be retained along with the associated transaction, except in cases where regulation or contractual obligations require special handling.

3.4. Off-boarding Employee Data Retention

The following data retention applies for voluntary and involuntary off-boarding CID employees.

3.4.1. Senior Management will contact appropriate system administrator to notify them of the termination, date and type (voluntary or involuntary).

3.4.1.1. Voluntary terminations — All data will be retained by Infrastructure on former employee's equipment for a total of thirty (30) days.

3.4.1.2. Involuntary terminations — All data for involuntary terminations will be retained by Infrastructure on former employee's equipment for a total of sixty (60) days.

3.4.1.2.1. Additional time and storage may be used in cases where there is a demonstrable legal need to have the data on hand in a read-only format.

3.5. Data Destruction

Data at the end of the applicable data retention period will be destroyed according to the applicable Data Classification, with the strictest level of destruction applied to sets of mixed data or potentially mixed data.

In cases where there is any uncertainty, follow the guidelines set forth in NIST 800-88 for secure erasure.

3.5.1. Internal Data Destruction Requirements

3.5.1.1. Data destruction on IT equipment and systems is only to be carried out internally by Infrastructure personnel.

3.5.1.2. Data destruction for Customer Data stored in production-level databases is only to be carried out by authorized Data Science personnel.

4. Policy Compliance

4.1. Compliance Measurement

Senior Management will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

4.2. Exceptions

Any exception to the policy must be approved by the Compliance and Infrastructure teams in advance.

4.3. Non-Compliance

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

6. Enforcement

This policy will be enforced by the Infrastructure team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment.
Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

7. Revision History

Version	Date	Description	Revisor
1.0	October 2011	Initial policy adoption	Compliance Department
2.0	October 2012	Grammar/spelling corrections only	Compliance Department
2.1	October 2013	Review only/No changes	Compliance Department
2.2	October 2014	Review only/No changes	Compliance Department
2.3	October 2015	Review only/No changes	Compliance Department
2.4	October 2016	Review only/No changes	Compliance Department
3.0	October 2017	Clause 3.4.1.2.1. added	Compliance Department
3.1	October 2018	Review only/No changes	Compliance Department
3.2	January 2019	Audit Updates Completed	Compliance Department
3.3	October 2019	Review only/No changes	Compliance Department