SECURITY

Data Management Policy

Policy Owner: Paul Jones

Version: 2.1

Last Reviewed: 2026-02-24

1. Purpose

To define how Crystal Project Inc. (“Crystal”) classifies, protects, retains, and securely disposes of information in accordance with business, contractual, and legal requirements.

2. Scope

This policy applies to:

- All data processed or stored by Crystal
- All information systems and infrastructure
- All personnel handling company or customer data

3. Data Classification

Crystal maintains three data classifications:

Confidential

Highly sensitive information requiring the highest level of protection.

Examples include:

- Customer data
- Personally identifiable information (PII)
- Authentication credentials and secrets
- Financial and payroll data
- Incident and vulnerability reports

- Source code
- Strategic plans

Restricted

Internal business information requiring protection but not classified as Confidential.

Examples include:

- Internal policies
- Contracts
- Internal reports
- Meeting materials
- Internal communications

Restricted is the default classification for company information unless otherwise specified.

Public

Information approved for public distribution.

Examples include:

- Marketing materials
- Public-facing policies
- Product documentation
- Press releases

4. Data Handling Requirements

Confidential Data

Confidential data must:

- Be accessible only to authorized personnel
- Be protected using role-based access controls

- Be encrypted in transit over public networks
- Be encrypted at rest where supported
- Be stored only in approved systems
- Be transferred externally only under appropriate contractual or legal safeguards

Production customer data is not used in non-production environments except where strictly necessary and appropriately safeguarded.

Restricted Data

Restricted data must:

- Be accessible on a need-to-know basis
- Not allow unauthenticated or anonymous access
- Be transferred externally only with appropriate authorization

Public Data

Public data may be freely distributed once formally approved.

5. Data Retention

Data is retained only as long as necessary to:

- Fulfill contractual obligations
- Meet legal or regulatory requirements
- Support legitimate business operations

Customer data is deleted in accordance with contractual terms, customer requests, and applicable agreements.

Legal hold requirements override standard retention timelines when applicable.

Retention practices are reviewed periodically.

6. Data Disposal

When Confidential or Restricted data is no longer required:

- It must be securely deleted or destroyed.
- Cloud-hosted data is deleted using platform-native secure deletion mechanisms.
- Devices returned to the company are wiped or reprovisioned prior to reassignment where applicable.

Third-party vendors must support secure deletion consistent with contractual obligations.

7. Backup and Replication

Production data may be replicated or backed up for resilience and disaster recovery purposes in accordance with the Business Continuity and Disaster Recovery Policy.

Backup and replicated data remain subject to the same classification and protection requirements as primary data.

8. Compliance and Review

Compliance with this policy may be verified through internal review processes and external audits where applicable.

This policy is reviewed at least annually.

9. Exceptions

Exceptions must be documented and approved by the Policy Owner.

10. Enforcement

Violations may result in corrective action, up to and including termination of employment or contract.

11. Review History

Version	Date	Description	Author
1.0	2021-07-19	Initial Version	Jona Morua
2.1	2026-02-24	Simplified and aligned to operational practice and DPA	Paul Jones