SECURITY

Cryptography Policy

Policy Owner: Security Team

Version: 2.0

Effective Date: 2021-07-06

Last Reviewed: 2026-02-24

1. Purpose

To ensure appropriate and effective use of cryptographic controls to protect the confidentiality, integrity, and authenticity of information processed by Crystal Project Inc.

This policy defines requirements for encryption, hashing, and cryptographic key management.

2. Scope

This policy applies to:

- All systems that store, process, or transmit Confidential or Customer data
- All production infrastructure
- All engineers and administrators managing cryptographic materials

3. Encryption Requirements

3.1 Data in Transit

All external network traffic transmitting Confidential or Customer data over public networks must use secure transport protocols.

- TLS 1.2 or higher is required
- TLS 1.3 is preferred where supported
- Weak or deprecated protocols (e.g., SSL, TLS 1.0/1.1) must not be enabled

Certificates must be issued by trusted certificate authorities and managed through approved infrastructure providers.

3.2 Data at Rest

Confidential and Customer data stored in production systems must be encrypted at rest using strong, industry-standard cryptography.

Where possible, encryption at rest is enforced through:

- Cloud provider managed encryption (e.g., AWS-managed encryption)
- Encrypted storage services (e.g., S3, RDS, EBS, etc.)
- Full disk encryption for employee laptops

3.3 Password and Credential Protection

User passwords must be stored using strong one-way hashing algorithms with salting and appropriate work factors.

Approved algorithms include:

- bcrypt
- scrypt
- PBKDF2
- Argon2 (where applicable)

Plaintext password storage is strictly prohibited.

4. Key and Secret Management

Cryptographic keys and application secrets must be:

- Access-controlled using role-based access controls
- Stored in approved secret management systems or secure environment configuration
- Not hard-coded into source code repositories
- Rotated when risk, exposure, or operational needs require it

Approved secrets management systems include AWS Secrets Manager, AWS KMS, and platform-managed secure environment configuration (e.g., Vercel environment variables). The appropriate system is selected based on secret type and sensitivity.

Access to cryptographic materials must be limited to authorized personnel only.

Where cloud-managed key services are used, provider controls are relied upon for key lifecycle management and audit logging.

5. Algorithm and Strength Standards

Crystal Project uses strong, industry-accepted cryptographic standards.

Examples include:

- AES-128 or AES-256 for symmetric encryption
- RSA-2048 or stronger for asymmetric encryption
- ECDHE for key exchange
- SHA-256 or stronger for hashing (where hashing is required)

Deprecated or insecure algorithms (e.g., MD5, SHA-1 for security-sensitive purposes, DES, RC4) must not be used.

6. Risk-Based Cryptographic Controls

Encryption and pseudonymization controls are implemented based on:

- The sensitivity of the data
- The risk to individuals and the organization

- Industry standards and regulatory requirements
- Cost and operational feasibility

Cryptographic implementations must align with current industry best practices.

7. Exceptions

Exceptions to this policy must:

- Be documented
- Include a risk assessment
- Be approved by the Policy Owner

8. Violations and Enforcement

Violations of this policy may result in:

- Removal of access
- Corrective action
- Disciplinary measures
- Termination of engagement where appropriate

9. Review and Revision History

Version	Date	Description	Author
1.0	2021-07-19	Initial Version	Jona Morua
2.0	2026-02-24	Modernized standards and cloud-aligned controls	Paul Jones