SECURITY

Information Security Policy

Policy Owner: Paul Jones

Version: 2.0

Effective Date: 2024-09-12

Last Reviewed: 2026-02-24

1. Purpose

This policy defines Crystal Project Inc's overall approach to information security governance and establishes the framework under which specific security policies and controls operate.

The objective is to protect the confidentiality, integrity, availability, and privacy of customer data, company information, and supporting systems.

2. Scope

This policy applies to:

- All employees and contractors
- All information systems and infrastructure
- All company-controlled and customer data
- All devices used to access company systems

3. Security Governance Principles

Crystal Project maintains a pragmatic, risk-based security program appropriate to its size and operational complexity.

Security governance includes:

- Executive oversight of security risk
- Role-based access control and least privilege

- Multi-factor authentication (MFA) required for all workforce identities
- Secure software development practices
- Encryption of data in transit and at rest
- Independent third-party penetration testing performed annually
- Periodic access reviews
- Incident response readiness and tabletop exercises
- Vendor risk management
- Continuous improvement through postmortems and review

Security is a shared responsibility across the organization.

4. Responsibilities

Policy Owner

The Policy Owner is responsible for:

- Maintaining the security program
- Reviewing policies at least annually
- Approving exceptions
- Coordinating incident response
- Communicating material risks to executive leadership

Employees and Contractors

All personnel must:

- Follow applicable security policies
- Protect company and customer information
- Report suspected security events promptly
- Use company systems responsibly and in accordance with business purposes

5. Policy Framework

This Information Security Policy is supported by the following policies and plans:

- Access Control Policy
- Asset Management Policy
- Risk Management Policy
- Incident Response Policy
- Secure Development Policy
- Cryptography Policy
- Business Continuity and Disaster Recovery Plan
- Third-Party Risk Management Policy
- Human Resource Security Policy

These policies define specific operational requirements.

6. Monitoring and Compliance

Crystal Project may monitor systems, networks, and logs as necessary to:

- Maintain operational security
- Detect misuse or unauthorized access
- Ensure compliance with company policies

Compliance may be evaluated through internal review processes and external audits where applicable.

7. Exceptions

Exceptions to this policy must:

- Be documented
- Include justification
- Be approved by the Policy Owner

8. Enforcement

Violations of this policy may result in:

- Removal of system 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
1.2	2024-09-12	Updated for policy migration	Paul Jones
2.0	2026-02-24	Simplified and aligned to operational practice	Paul Jones