SECURITY

Information Security Roles and Responsibilities

Policy Owner: Paul Jones

Version: 2.0

Last Reviewed: 2026-02-24

1. Purpose

This policy defines information security roles and responsibilities within Crystal Project Inc. (“Crystal”) to ensure accountability, clarity, and effective governance of the security program.

2. Scope

This policy applies to:

- All employees
- Contractors
- Executive leadership
- Individuals with access to company systems or data

3. Security Governance Structure

Crystal maintains a lean, engineering-led security governance model appropriate to its size and operational complexity.

Security responsibilities are distributed across leadership and operational roles as defined below.

4. Roles and Responsibilities

Policy Owner (Chief Technology Officer)

The Policy Owner is responsible for:

- Overall security program oversight

- Maintaining and reviewing security policies
- Coordinating risk management activities
- Overseeing incident response
- Approving policy exceptions
- Reporting material security risks to executive leadership
- Ensuring alignment between security posture and business objectives

Executive Leadership

Executive leadership:

- Provides oversight of enterprise risk, including cybersecurity risk
- Participates in material incident and breach decisions
- Supports resource allocation for security initiatives

Engineering

Engineering is responsible for:

- Secure software development practices
- Infrastructure security and hardening
- CI/CD security controls
- Implementation of vulnerability remediation
- Operational logging and monitoring
- Supporting disaster recovery and resilience testing

Engineering leadership works with the Policy Owner to ensure security controls are embedded in development and operations.

Human Resources (or Designated Leadership)

Responsible for:

- Ensuring personnel are informed of company policies

- Coordinating onboarding and offboarding processes
- Supporting background checks where applicable
- Ensuring personnel complete required security awareness training

System Owners (Where Applicable)

Individuals responsible for specific systems must:

- Ensure appropriate access controls are applied
- Support risk identification and remediation
- Approve non-standard access requests where appropriate

All Personnel

All employees and contractors are responsible for:

- Adhering to company security policies
- Protecting company and customer information
- Reporting suspected incidents or vulnerabilities
- Minimizing risk exposure through responsible system use

5. Policy Compliance

Compliance with this policy may be evaluated through:

- Internal review processes
- External audits where applicable
- Risk management activities

Non-compliance may result in corrective action up to and including termination.

6. Exceptions

Exceptions must be documented and approved by the Policy Owner.

7. Review History

Version	Date	Description	Author
1.0	2021-07-19	Initial Version	Jona Morua
2.0	2026-02-24	Updated to reflect current organizational structure	Paul Jones