SECURITY

Human Resource Security Policy

Policy Owner: Kirsten Alexander

Version: 2.0

Effective Date: July 6, 2021

Last Reviewed: 2026-02-24

1. Purpose

To ensure that employees and contractors understand their information security responsibilities and are suitable for their assigned roles based on risk and access level.

2. Scope

This policy applies to:

- All employees of Crystal Project Inc. (Crystal Knows)
- Consultants and contractors
- Third-party personnel with access to Crystal production systems, networks, or sensitive information

3. Policy

3.1 Screening

Crystal Project performs background screening where appropriate and proportionate to:

- Role responsibilities
- Level of system or data access
- Sensitivity of information handled
- Identified organizational risk

Background screening may include:

- Reference checks

- Employment verification
- Criminal background checks where applicable and legally permissible

Third parties with privileged or administrative access to production systems may be subject to additional due diligence based on risk.

Screening practices are implemented in accordance with applicable laws and regulations.

3.2 Role Definition and Competence

Hiring managers define required qualifications and competencies in job descriptions.

Candidate evaluation may include:

- Interviews
- Technical assessments
- Reference checks
- Verification of education or certifications where relevant

Managers are responsible for ensuring personnel are capable of fulfilling their security responsibilities.

Performance and role effectiveness may be evaluated periodically at management's discretion.

3.3 Terms and Conditions of Engagement

At the time of hire or engagement:

- Information security responsibilities are communicated
- Relevant policies are made available
- Employees and applicable contractors sign confidentiality agreements

Contracts with third parties define security obligations where appropriate.

All personnel are required to comply with Crystal Project information security policies for the duration of their employment or engagement.

3.4 Management Responsibilities

Management is responsible for:

- Maintaining and reviewing information security policies at least annually
- Ensuring policies are accessible to relevant personnel
- Assigning and documenting security responsibilities
- Enforcing compliance with security requirements

Information security responsibilities are documented in job descriptions, policies, or related governance materials.

3.5 Security Awareness and Training

All employees and contractors with privileged or administrative access to production systems must:

- Complete security awareness training at onboarding
- Complete security awareness training periodically thereafter

Training completion is monitored by management.

All personnel are expected to remain aware of applicable information security policies and procedures.

3.6 Disciplinary Process

Violations of information security policies may result in:

- Suspension or removal of system access
- Investigation
- Disciplinary action
- Termination of employment or contract where appropriate

Disciplinary actions are proportionate to the nature and severity of the violation.

4. Exceptions

Exceptions to this policy must:

- Be documented

- Include justification
- Be approved by the Policy Owner or designated management authority
- Define compensating controls where applicable

5. Reporting and Enforcement

Suspected violations of this policy should be reported to management or Human Resources.

Confirmed violations may result in corrective action consistent with company policies and applicable law.

6. Review and Revision History

Version	Date	Description	Author
1.0	2021-07-19	Initial Version	Kirsten Alexander
2.0	2026-02-24	Updated to align with operational practice	Paul Jones