SECURITY

Risk Management Policy

Policy Owner: Paul Jones

Version: 2.1

Effective Date: 2021-07-06

Last Reviewed: 2026-02-24

1. Purpose

To ensure that information security and operational risks are identified, evaluated, and managed in a manner proportionate to the size and complexity of Crystal Project Inc.

2. Scope

This policy applies to:

- Information systems and infrastructure
- Customer data
- Business-critical processes
- Third-party vendors and service providers
- Software development and deployment practices

3. Risk Management Principles

Crystal Project applies a pragmatic, risk-based approach to security governance.

Risk management activities include:

- Identification of security and operational risks
- Evaluation of likelihood and impact
- Prioritization of remediation efforts
- Documentation of significant risks and treatment decisions

- Periodic review by leadership

Risk evaluation considers potential impact to:

- Confidentiality
- Integrity
- Availability
- Privacy
- Regulatory obligations
- Business continuity

4. Risk Identification Sources

Risks may be identified through:

- Annual third-party penetration testing
- Vulnerability scanning and monitoring tools
- Security incident postmortems
- Formal tabletop exercises conducted regularly (at least annually)
- Vendor risk reviews
- Software design and architecture reviews
- Operational experience and engineering judgment

Tabletop exercises are used to evaluate incident readiness, identify gaps, and improve response procedures.

5. Risk Evaluation

Identified risks are assessed based on:

- Likelihood of occurrence
- Potential operational or security impact
- Exploitability

- Exposure of customer or sensitive data
- Reputational or contractual implications

Risk scoring may be qualitative or quantitative depending on context.

Management retains discretion to adjust automated or third-party severity ratings based on contextual risk.

6. Risk Treatment

For each significant risk, one of the following responses may be selected:

- Mitigate
- Accept
- Transfer
- Avoid

Material risks and their treatment decisions are documented.

Risk remediation prioritization considers:

- Severity
- Resource availability
- Operational impact
- Customer commitments

7. Risk Review and Oversight

Risk posture is reviewed periodically by leadership.

Formal reviews may occur in conjunction with:

- Annual penetration testing
- Tabletop exercises
- Security reviews
- Audit preparation

- Strategic planning discussions

Significant risks are communicated to executive leadership as appropriate.

8. Continuous Improvement

Security incidents, tabletop exercises, and postmortems are used to:

- Identify systemic weaknesses
- Improve controls
- Update policies and procedures
- Reduce recurrence risk

Lessons learned are incorporated into operational practices.

9. Exceptions

Exceptions must:

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

10. Violations and Enforcement

Violations may result in:

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

11. Review and Revision History

Version	Date	Description	Author
1.0	2021-07-06	Initial Version	Jona Morua
2.1	2026-02-24	Simplified and aligned to operational practice	Paul Jones