SECURITY

Third-Party Risk Management Policy

Policy Owner: Paul Jones

Version: 2.0

Effective Date: 2021-07-06

Last Reviewed: 2026-02-24

1. Purpose

To ensure that third-party service providers who access, process, store, or transmit company or customer data maintain appropriate security controls consistent with Crystal Project Inc.'s risk profile.

2. Scope

This policy applies to:

- Vendors and service providers with access to production systems
- Vendors that process or store customer data
- Critical SaaS providers supporting business operations
- Subprocessors

3. Third-Party Risk Principles

Crystal Project Inc. applies a risk-based approach to third-party evaluation.

Vendors are assessed proportionate to:

- The sensitivity of data involved
- Level of system access
- Business criticality
- Regulatory exposure

Not all vendors require the same level of review.

4. Vendor Due Diligence

Before engaging a vendor that may access or process customer data:

- Security posture is evaluated.
- Relevant certifications (e.g., SOC 2) are reviewed where applicable.
- A written agreement or contract is executed.
- Data protection obligations are defined where required.

For critical infrastructure providers (e.g., cloud hosting), reliance may be placed on publicly available security documentation and independent audit reports.

5. Subprocessor Management

Vendors that process customer data on behalf of Crystal Project Inc. are designated as subprocessors where applicable.

Subprocessors are:

- Documented
- Contractually bound to appropriate data protection obligations
- Reviewed when material service changes occur

6. Ongoing Monitoring

Third-party services are reviewed periodically based on risk and criticality.

Monitoring may include:

- Reviewing updated audit reports
- Evaluating significant vendor changes
- Reviewing security incidents impacting the vendor
- Reassessing risk during contract renewal

Formal annual reassessments may not be required for low-risk vendors.

7. Vendor Security Expectations

Third-parties that process customer data are expected to maintain reasonable technical and organizational security controls, including where applicable:

- Access control mechanisms
- Secure system development practices
- Vulnerability management
- Logging and monitoring
- Incident response capabilities
- Business continuity measures

Crystal Project Inc. does not impose uniform control requirements but evaluates vendors proportionate to risk.

8. Termination of Services

Upon termination of a vendor relationship involving customer data:

- Access must be revoked.
- Data must be returned or securely destroyed in accordance with contractual terms.

9. Exceptions

Exceptions must be documented and approved by the Policy Owner.

10. Enforcement

Violations may result in corrective action or termination of vendor relationships where appropriate.

11. Review and Revision History

Version	Date	Description	Author
1.0	2021-07-06	Initial Version	Jona Morua
2.0	2026-02-24	Simplified and aligned to operational practice	Paul Jones