SECURITY

Acceptable Use Policy

Policy Owner: Paul Jones

Version: 1.0

Effective Date: 2026-07-28

Last Reviewed: 2026-07-28

1. Purpose

To set expectations for the acceptable use of Crystal Project Inc systems, accounts, and data, so that company and customer information stays secure.

2. Scope

This policy applies to:

- All employees and contractors
- Company systems, accounts, and SaaS applications
- Company and customer data in any form

3. General Principles

Crystal Project maintains a pragmatic, risk-based approach to acceptable use, proportionate to its size and operational complexity.

Personnel are expected to:

- Use company systems and accounts for legitimate business purposes
- Protect the confidentiality, integrity, and availability of company and customer data
- Follow the Information Security Policy, Data Management Policy, and Access Control Policy
- Report suspected security incidents or policy violations promptly

Reasonable personal use of company systems (e.g., checking personal email) is fine, provided it doesn't interfere with work or create security or legal risk.

4. Acceptable Use

Personnel should:

- Access only the data and systems needed for their role
- Keep credentials confidential and use MFA where required
- Use approved channels (per the Data Management Policy) when sharing confidential or customer data
- Use good judgment with unsolicited attachments, links, or requests for credentials (phishing)
- Get authorization before connecting new SaaS applications or integrations that touch company or customer data

Unauthorized use, disclosure, or removal of company or customer data is prohibited.

5. Software and Devices

Personnel are trusted to use good judgment on the devices they use for work, consistent with the Asset Management Policy. Only software needed for business purposes, obtained through reasonably trustworthy sources, should be used to access company or customer data.

6. Exceptions

Exceptions must:

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

7. Violations and Enforcement

Violations may result in:

- Removal of system access

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

8. Review and Revision History

Version	Date	Description	Author
1.0	2026-07-28	Initial version	Paul Jones