SECURITY

Asset Management Policy

Policy Owner: Paul Jones

Version: 2.1

Effective Date: 2021-07-06

Last Reviewed: 2026-02-24

1. Purpose

To ensure that organizational assets are identified, appropriately protected, and managed throughout their lifecycle.

2. Scope

This policy applies to:

- Information systems and infrastructure
- Cloud environments
- Source code repositories
- End-user computing devices
- SaaS platforms used to support business operations
- Data stored or processed by Crystal Project Inc

3. Definition of Assets

Assets include, but are not limited to:

- Production and development infrastructure
- Cloud accounts and services (e.g., AWS)
- Source code repositories
- SaaS applications
- Company-issued laptops and mobile devices

- Customer and internal data

4. Asset Inventory

Crystal Project maintains visibility into critical business and production assets through:

- Cloud provider account management (e.g., AWS)
- Centralized source code repositories
- Identity provider account listings
- A maintained inventory of company-issued devices
- Vendor and subprocessor documentation

Company-issued devices are tracked and periodically reviewed to ensure accountability.

The level of documentation and tracking is proportionate to organizational size and operational complexity.

5. Ownership of Assets

Each significant system or platform must have a designated responsible owner.

Owners are responsible for:

- Ensuring appropriate security controls are in place
- Reviewing access controls
- Coordinating remediation of security issues

Ownership may be assigned to an individual or a defined function.

6. Acceptable Use of Assets

All organizational assets must be used in accordance with:

- The Information Security Policy
- Employment agreements
- Applicable contractual obligations

Unauthorized use, removal, or modification of assets is prohibited.

7. Handling and Protection of Assets

Personnel issued company equipment must:

- Exercise reasonable care in protecting devices
- Prevent unauthorized access
- Secure devices when unattended
- Comply with endpoint security requirements

Mobile devices must comply with security standards defined in related policies.

8. Return or Disposition of Assets

Upon termination of employment or contract, company-issued assets must either:

- Be returned to Crystal Project, or
- Be formally transferred or disposed of with management approval.

Where devices are returned, appropriate steps must be taken to protect or remove company data prior to reuse or reassignment.

Access to digital systems must be removed in accordance with the Access Control Policy regardless of physical device disposition.

9. Exceptions

Exceptions must:

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

10. Violations and Enforcement

Violations may result in:

- Removal of system access
- 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	Kirsten Alexander
2.1	2026-02-24	Simplified and aligned to operational practice	Paul Jones