SECURITY

Operations Security Policy

Policy Owner: Paul Jones

Version: 2.0

Effective Date: 2021-07-06

Last Reviewed: 2026-02-24

1. Purpose

To ensure the secure and reliable operation of production systems and supporting infrastructure used by Crystal Project Inc.

2. Scope

This policy applies to:

- Production systems and infrastructure
- Cloud environments
- Business-critical systems
- Logging, monitoring, and backup processes

3. Operational Change Management

Production changes must be implemented through approved CI/CD pipelines and version-controlled processes as defined in the Secure Development Policy.

Operational controls include:

- Automated testing prior to deployment
- Pipeline-controlled production releases
- Audit logging of changes
- Restricted direct access to production environments

Emergency changes may be implemented when necessary to restore service or mitigate risk and must be reviewed retrospectively.

4. Environment Controls

Crystal Project Inc. maintains logical separation between:

- Local development environments
- Preview or testing environments
- Production systems

Production access is restricted to authorized personnel and protected by role-based access controls and MFA.

5. Logging and Monitoring

Production systems are configured to generate logs appropriate to their function.

Logging and monitoring practices include:

- Centralized log aggregation across production systems
- Recording user and administrative activities
- Monitoring for suspicious activity
- Alerting on high-risk security events
- Protecting logs from unauthorized modification

Logs are retained for a minimum of 90 days in active storage and 12 months in archive. Retention periods may exceed these minimums based on contractual or regulatory requirements.

6. Backup and Recovery

Critical systems and production data are backed up using cloud-native backup mechanisms.

Backups:

- Run automatically on a scheduled basis

- Are protected from unauthorized access
- Are periodically validated for restore capability

User endpoint devices are not centrally backed up. Personnel are responsible for storing critical business documents in approved cloud storage systems.

7. Vulnerability Management

Technical vulnerabilities are identified through:

- Independent third-party penetration testing performed annually
- Automated dependency vulnerability scanning (continuous)
- Cloud-native monitoring tools
- External reporting (e.g., responsible disclosure)

Vulnerabilities are evaluated based on severity, exploitability, and business impact and remediated according to the following targets:

Severity	Remediation Target
Critical	72 hours
High	14 days
Medium	30 days
Low	90 days

Remediation progress against these targets is tracked by engineering leadership and reviewed as part of the security governance process.

8. Malware and Threat Protection

Company-issued devices must use operating systems with built-in security protections enabled.

Threat detection and filtering mechanisms are utilized for email and production systems where supported by platform providers.

Personnel must not disable security protections without authorization.

9. Infrastructure Hardening

Production infrastructure is configured in accordance with cloud provider best practices, including:

- Restricted network exposure
- Role-based access control
- Encrypted communications
- Minimal open ports and services
- Removal of unused accounts and permissions

Infrastructure configurations are maintained through code where feasible.

10. Audit and Review

Operational controls may be reviewed through:

- Internal review processes
- Tabletop exercises
- Post-incident reviews
- External audits where applicable

11. Exceptions

Exceptions must be documented and approved by the Policy Owner.

12. Enforcement

Violations may result in:

- Removal of system access
- Corrective action
- Disciplinary measures
- Termination of engagement where appropriate

13. Review and Revision History

Version	Date	Description	Author
1.0	2021-07-06	Initial Version	Kirsten Alexander
2.0	2026-02-24	Rewritten for CI/CD and cloud-native operations	Paul Jones