SECURITY

Incident Response Policy

Policy Owner: Paul Jones

Version: 2.1

Effective Date: 2021-07-06

Last Reviewed: 2026-02-24

1. Purpose

To define how Crystal Project Inc identifies, responds to, and resolves security incidents affecting systems, infrastructure, or data.

2. Scope

This policy applies to security events or incidents involving:

- Customer data
- Production systems
- Infrastructure
- Internal systems
- Confidential information

3. Definitions

Security Event

An observable occurrence related to system or data security.

Security Incident

A confirmed event resulting in unauthorized access, disruption, data exposure, or compromise.

4. Reporting

All personnel must promptly report suspected security events.

Reports may be made through internal communication channels (e.g., Slack) or directly to engineering leadership.

Customers may report issues through official support channels.

5. Severity Classification

Incidents are classified based on impact:

- **Critical** – Active compromise, confirmed malicious activity, or material customer impact.
- **High** – Significant vulnerability or elevated operational risk.
- **Medium / Low** – Limited impact or suspicious activity requiring investigation.

Severity determines escalation urgency and communication cadence.

6. Response Process

When a significant incident occurs:

1. A dedicated Slack channel is created.
2. Engineering leadership coordinates response.
3. Investigation and containment actions begin immediately.
4. Systems are restored or mitigations are applied.
5. Communication is provided to leadership and, if required, customers.

A real-time huddle may be used during active incidents.

7. Roles and Responsibilities

Policy Owner (Incident Lead)

- Coordinates response efforts
- Determines severity
- Assigns remediation tasks
- Determines incident resolution

- Evaluates notification requirements

Engineering Team

- Investigates root cause
- Implements containment and remediation
- Restores services
- Documents findings

Executive Leadership

- Informed of material incidents
- Participates in external communication decisions when required

8. Breach Determination and Notification

If an incident involves potential unauthorized access to customer data or regulatory impact:

- The Policy Owner, in consultation with executive leadership, determines whether notification obligations apply.
- Notifications are made in accordance with contractual and legal requirements.

9. Documentation

All confirmed incidents are documented.

Documentation includes:

- Timeline of events
- Impact assessment
- Root cause analysis (for significant incidents)
- Corrective actions

Postmortems are maintained in internal systems (e.g., Notion).

10. Post-Incident Improvement

Significant incidents are reviewed to:

- Identify systemic weaknesses
- Improve controls and detection
- Prevent recurrence

Lessons learned are incorporated into engineering and operational practices.

11. Testing and Readiness

Incident response readiness is evaluated through periodic tabletop exercises (conducted at least annually and often more frequently).

Tabletops may be combined with broader risk discussions.

12. Exceptions

Exceptions must be documented and approved by the Policy Owner.

13. 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