Incident Management Program Policy

Purpose

AllCode's Incident Management Program Policy defines the responsibilities of AllCode's teams when responding to or reporting security incidents. It delineates roles within AllCode and their clients to outline who should be involved in different types of security incidents.

Definitions

- "Customer" means a third party that has entered into a binding, written agreement with AllCode for the provision of Services.
- "Company" means AllCode.

Initial Notification of Security Incident

AllCode shall notify the Customer's Security Operation Center immediately of any security incidents via Customer's appropriate channel. AllCode will have an information security on-call technician summoned within one (1) hour of AllCode becoming aware of occurrence of a Security Incident. Additionally, within twenty-four (24) hours of Company's becoming aware of occurrence of a Security Incident, Company shall also notify Customer in writing and by email to the address and email specified by the Customer.

Subsequent Reports and Notifications

After the initial notification, Company shall subsequently update the Customer's Security team of security incidents, as required below via dedicated teleconference bridge-line established for the event.

Additionally, as required below, Company shall notify Customer via email of all Security Incidents and shall provide all written reports to Customer.

Security Incident Resolution Times

In the event of a Security Incident, Company shall use continuous efforts to correct the Security Incident immediately and notify Customer upon resolution.

Interim Status Reports

Company shall provide Customer with an interim written status report of each Security Incident within 4 hours, and at agreed upon intervals thereafter, based on the agreed upon severity of the incident and such report shall include:

- Date of Security Incident
- Brief description of Security Incident including known or suspected cause

- Company Incident Coordinator
- Customer's Incident Coordinator they are working with
- Impact of the Security Incident to Company
- Company's Response Plan to the incident
    - What has been done so far
    - What needs to be done/action items
- Current Status
- Expected timeframe for full-service restoration or resolution

Final Report

Company shall provide Customer with a final written report of each Security Incident within three (3) business days of resolution or a determination that the problem cannot be satisfactorily resolved within such time period (in which case, an estimated date for final resolution will be proposed) and such report shall include:

- Company's Name
- Company's Incident Coordinator and contact info
- Customer's Incident Coordinator
- Date Incident Occurred
- Length of Outage
- Incident Executive Overview
- Incident Details:
    - List of individuals and 3rd parties that were involved
    - How/when the incident was initially detected
    - When/how the incident was reported to Customer
    - Description of what resources/services were impacted
    - Description of impact of Security Incident to Customer
    - Containment – How was the incident contained
    - Root Cause – What was the cause for disruption
    - Corrective Action During Incident
    - Permanent Corrective Action/preventative measures
- Conclusion

Post Mortem Reviews

Company shall coordinate the scheduling of a Post Mortem Review with the Customer's Incident Coordinator. This review should be scheduled within seven (7) business days of the resolution of the incident or determination that the problem cannot be satisfactorily resolved within such time period.

Right to Security Assessment

In the event of a Security Incident, Customer shall have the right to conduct a Security Assessment to validate that all necessary and timely remedial actions have been taken by the Company to correct the Security Incident.

Incident Severity Levels

Incident response will be addressed based on the severity of the incident. Incident severity takes several factors into account: sensitivity of the data involved, number of end users impacted, and its overall impact on the ability of the Customer's solution to work. Incident severity also will be used to determine who manages an incident, who is informed about an incident, and the extent and immediacy of the response to the incident.

High

A security incident will be considered "high" if any of the following characteristics are present:

Threatens to impact (or does impact) systems critical to the Customer's ability to function normally. Poses a serious threat of financial risk or legal liability. Threatens to expose (or does expose) personal privacy data. Threatens to propagate to or attack other networks, or organizations internal or external to the Customer. Terroristic threats or other threats to human life or property.

Medium

A security incident will be considered "medium" if any of the following characteristics are present:

Threatens to impact (or does impact) a significant number of systems or people. The Customer's software can still function, but a group or section of the software may be unable to perform its mission. Impacts a non-critical system or service.

Low

Low severity incidents have no characteristics from the "medium" or "high" categories and may include the following:

Only a small number of systems are impacted. Little to no risk of the incident spreading or impacting other organizations or networks

Incident Response Summary Table

The following table summarizes how IT security incidents will be handled based on severity. It includes response times for each severity level.

Incident Severity	Response Time
High	Within twenty-four (24) hours of critical vendor patch release announcement, notification from Customer, or discovered security breach, whichever is earlier
Medium	Within forty-eight (48) hours of vendor patch release, or discovered security breach, which is earlier
Low	Within seven (7) calendar days of occurrence.