### JD Software LLC

**Incident Response Plan**

This document offers guidance for employees or incident responders who believe they have discovered or are responding to a security incident.

**Escalation**

Email to [panic@jdsoftwarellc.com](mailto:panic@jdsoftwarellc.com). Be a good witness. Behave as if you were reporting a crime and include lots of specific details about what you have discovered.

**Severity**

**Low and Medium Severity**

Issues meeting this severity are simply suspicions or odd behaviors. They are not verified and require further investigation. There is no clear indicator that systems have tangible risk and do not require emergency response. This includes suspicious emails, outages, strange activity on a laptop.

**High Severity**

High severity issues relate to problems where an adversary or active exploitation hasn’t been proven yet, and may not have happened, but likely to happen. This may include vulnerabilities with direct risk of exploitation, threats with risk or adversarial persistence on our systems (eg: backdoors, malware), malicious access of business data (eg: passwords, vulnerability data, payments information), or threats that put any individual at risk of physical harm.

High severity issues should include an email to [panic@jdsoftwarell.com](mailto:panic@jdsoftwarell.com) with “Urgent” in the subject line, or a message to #security with “@channel incident” in the message to alert incident responders.

**Critical Severity**

Critical issues relate to actively exploited risks and involve a malicious actor. Identification of active exploitation is critical to this severity category.

Critical severity issues should involve a message to “@channel” in #security as well as messages to the CEO and CTO, COO, and PR. Continue escalation until you receive acknowledgement. Involvement of a crisis lead for public relations, a lawyer familiar with breach notification, and a “heads up” to our consultant response partners are highly recommended.

**Internal Issues**

Issues where the malicious actor is an internal employee, contractor, vendor, or partner requires sensitive handling. Please contact the CEO and CTO directly and do not discuss with other employees. These are critical issues and must be pushed to follow up.

**Compromised Communications**

If there are IT communication risks, the Aurora team will announce an out of band solution within the office, and will communicate this to managers with directions over cell phones.

**Response Steps**

For critical issues, the response team will follow an iterative response process designed to investigate, contain exploitation, remediate our vulnerability, and document a post-mortem with the lessons of an incident.

1. CTO or CEO will determine if a lawyer be included and attorney client privilege between responders will begin.
2. A central “War Room” will be designated.
3. The following meeting will occur at regular intervals until the incident is resolved:

**Breach Response Meeting — Agenda**

* Update Breach Timeline
* New Indicators of Compromise
* Investigative Q&A
* Emergency Mitigations
* Long Term Mitigations (including Root Cause Analysis)
* Everything Else

We will *Update a Breach Timeline* with all known temporal data related to the incident. All *Indicators of Compromise* will be updated and shared among breach responders. The group will add new knowns and unknowns to the *Investigative Q&A*. A list of tactical *Emergency Mitigations* will be updated. A list of long term, post breach *Long Term Mitigations* will be updated. Once items related to response are covered, technical responders may leave the meeting and meta-topics (*Everything Else*) related to the breach are discussed (communications, legal issues, blog posts, etc) with leadership.

**Response Team Members**

| **Name** | **Cell Phones** | **email** | **position(s)** |
| --- | --- | --- | --- |
| Jimmy | 503-929-6466 | [jimmy@jdsoftwarellc.com](mailto:jimmy@jdsoftwarellc.com) | CEO/CTO/HR/Dev |

**Runbooks**

**DoS Attack**

Change Cloud Flare's setting to "under attack"

**Data leak**

Azure, remove all public access to database and take a snap shot of the database. Disable all services and allow apps to run in offline mode, until patched.