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 support@brytsoftware.com to notify the security team of issues. Be a good witness and include as many specific details as possible about what you have discovered.

Severity

Low and Medium Severity

Issues meeting this severity are simply suspicious or odd behaviors. They are not verified and require further investigation. There is no clear indicator that systems have tangible risks and do not require emergency response. This includes suspicious emails, outages, and 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 is likely to happen. This may include vulnerabilities with direct risk of exploitation, threats with risk or adversarial persistence on our systems (e.g. backdoors, malware), malicious access of business data (e.g. passwords, vulnerability data, payment information), or threats that put any individual at risk of physical harm.

High-severity issues should include an email to support@brytsoftware.com with "Urgent" in the subject line.

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 an email to bob@brytsoftware.com, brian@brytsoftware.com, and PR. Continue escalation until you receive an acknowledgment. The involvement of a crisis lead for public relations and notification to our consultant response partners are highly recommended.

Internal Issues

Issues where a malicious actor is an internal employee, contractor, vendor, or partner require sensitive handling. Please contact the CEO, bob@brytsoftware.com, and Brian, brian@brytsoftware.com, directly, and do not discuss this with other employees. These are critical issues and must be pushed to follow up.

Compromised Communications

If there are IT communication risks, the security response team will communicate this to managers with directions over cell phones. Communications may take place through a secured and encrypted communication channel such as Signal, Wickr, or Viber.

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 lessons learned from the 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)

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 related to the breach are discussed (communications, legal issues, social media responses, etc.) with leadership.

Response Team Members

Name	Cell Phones	Email	Secure Channel Com
Bob Schulte			
Brian Allen			
Tyler Crawford			