Incident Response Plan

This incident management plan outlines actions and procedures to respond to events that could impact critical business activities at Inteum Company or a compromise of availability, integrity, or confidentiality of Inteum Company data or systems.

This document offers guidance for employees or incident responders who believe they have discovered or are responding to a security incident. This document will be reviewed at least annually and will be updated as needed.

Preparation

Escalation

Email to support@inteum.com should be used to notify the security team of any potential security issues. Include specific details about the potential security incident.

The following individuals are members of the Inteum Company Incident Response Team.

Response Team Members

Name	Role	Phone	Email
Tim Hollobon	Vice President & Chief Technology Officer	425-823-1780	timh@inteum.com
Rob Sloman	President & Chief Executive Officer	425-820-8415	robs@inteum.com
Matt Campbell	IT & Security manager	425-814-8212	mcampbell@inteum.com

Incident Response War Room

CEO office room at the Inteum Company office located at 9720 NE 120th Place, Suite 101, Kirkland, WA 98034 will serve as the incident response war room where the Incident Response Team will manage the communications with Inteum Company management and any external parties as needed.

Communication with External Parties

A single member of the Management Team (and a backup) will be designated to communicate with clients, supply chain stakeholders and public entities (e.g. the media, law enforcement) on behalf of Inteum Company as necessary. This individual is responsible for determining how public communications/inquiries will be handled during a security incident.

Identification

Incident Severities

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 may be likely to happen. This may include vulnerabilities with direct risk of exploitation, threats with risk or adversarial persistence on systems (e.g. backdoors, malware), malicious access of business data (e.g., passwords, vulnerability data, payments information, sensitive client data), or threats that put any individual at risk of physical harm.

High severity issues should include an email to support@inteum.com with "Urgent" in the subject line to alert incident responders.

Example as part of test runs of the IRP:

High severity

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 message to support@inteum.com as well as messages to the CEO and CTO. 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 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 Incident Response team will announce an out of band solution within the office, and will communicate this to managers with directions over cell phones.

Containment

For critical issues, the response team will follow an iterative response process designed to investigate, contain exploitation, remediate the 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. The Incident Response Team will convene in the central "War Room."
3. The following meeting will occur at regular intervals until the incident is resolved:

Incident Response Meeting—Agenda

- Update Incident Timeline

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

Document in detail the *Breach Timeline* with all known temporal data related to the incident. All *Indicators of Compromise* will be updated and shared among incident 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 incident *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 incident are discussed (communications, legal issues, blog posts, etc.) with leadership.

Perform Backups

As appropriate and possible, the response team will perform a full block-level backup (full forensic disk image) of every system impacted by the security incident. Once backups are completed, the backup will be stored on an unaffected offsite location, for example AWS. The response team member who performed the backup will notify the CEO and CTO of its location.

Gather Evidence

The evidence gathered will primarily be used in the Eradication phase to determine the cause of the incident, but it may also be needed for legal purposes. In the case the incident has legal ramifications, all evidence must be gathered in such a way that it will be admissible in potential legal proceedings. Therefore, detailed notes must be kept on how evidence was gathered, preserved, stored, and transferred between individuals. The following information should be collected regarding evidence collected during a security incident:

- Identifying information (e.g., the location, serial number, model number, hostname, media access control (MAC) addresses, and IP addresses of all impacted systems)
- Name, title, and phone number of each individual who collected or handled the evidence during the investigation which will be used to establish the chain of custody for the evidence
- Time and date (including time zone) of each occurrence of evidence handling
- Evidence storage locations and who has access to the evidence

It is important to note that some data is volatile (e.g. memory, running processes, open network connections, etc.), so care must be taken to capture this data before it is no longer available.

Eradication

Examine all evidence available (e.g., audit logs, forensic data) gathered during the Containment phase to determine how the incident occurred. Once the incident response team determines the cause and scope of the incident, controls to prevent further compromise may need to be improved or implemented altogether. For example, unnecessary ports may need to be closed, or unnecessary services disabled, firewall rules updated, deleting malware, removing or disabling breached accounts, etc.). Depending on the extent of the incident, the impacted system will either be rebuilt or repaired.

Remediation timelines

Below table summarizes the remediation timelines based on the risk levels

Risk Levels	Remediation
Critical	1 day
High	3 days
Medium	5 days
Low	7 days

Recovery

If the decision is to repair the system, the incident response team must ensure that all changed files, applications, etc. are returned to their valid secure state. Any malicious code must be removed. Each repair action must be documented.

If the decision is to rebuild the impacted system, the response team will use only verified and trusted means to rebuild the system (e.g. validated images, vendor software, and validated data). Because of the technologies available, it is often easier and faster to rebuild a system vice repairing it. All the latest patches for the operating system and applications should be installed on the rebuilt host.

Once the system is rebuilt or repaired, the incident response team will verify the method of compromise is not resident on the system. Once the system is verified to be clean, services will be restored and clients will be

notified, as applicable. Incident response team members will monitor the systems and associated logs to ensure the system is not compromised again and is fully supporting business functions.

Lessons Learned

The incident response team lead will facilitate a lessons-learned meeting no later than one week of the end of the recovery phase for the incident. Each Inteum Company employee that participated in the incident response will provide feedback on the Inteum Company incident response team's ability to respond to the incident. Minutes will be kept for the meeting. All identified improvements will be incorporated into this plan. All documentation relating to the incident will be kept for a minimum of three years to support any potential legal proceedings or additional analysis by the incident response team.

Example IRP scenario

Incident Response Stage	Summary of Incident Response Activities
Identification	Employee makes IT group aware of laptop issue with slowness and unexpected popups, when compared to the other comparable laptop which aren't experiencing this behavior. Based on known factors issue seems like a high risk for Malicious virus /malware potentially installed on employee's laptop. Determine with user when exactly the issue started and what was the user doing and where was the user at (office network/off site/home?)
Containment	IT group will isolate this infected laptop by disconnecting their Ethernet cable or wireless access in order to not have the issue spread to the other network resources.
Eradication	Step1: Determine current state of the anti-virus software installed (up to date/latest definition?) on the machine by running a full scan to see if it can clean the system. Step2: If current anti-virus cannot detect the virus then install additional anti-virus/anti adware tools to see if they can identify and clean what is causing the issue.

Incident Response Stage	Summary of Incident Response Activities
	Step3: Once laptop has been cleaned, confirm no traces of virus after reboot and sub sequential scans.
Recovery	Determine how/when the system was comprised and the intent of the virus was and if it has any long term consequences. Next step is to return clean laptop back to the employee and make sure they are aware of IT security policies and procedures. And also the IT group will take necessary steps to prevent similar events occurring in future.

Revision History

The following table maintains the history of changes to this policy.

Rev	Date	Author	Description
1.0	1/8/18	Preet Mood	Initial version
1.1	1/31/18	Preet Mood	Example IRP scenario section added
1.2	1/22/18	Preet Mood	Reviewed the document and added Remediation timelines section.
1.3	3/14/19	Preet Mood	Reviewed document and No changes are needed
1.4	1/12/2021	Preet Mood	Reviewed document and No changes are needed
1.5	1/5/2022	Preet Mood	Reviewed document and No changes are needed
1.6	1/23/2023	Preet Mood	Reviewed document and no changes are needed
1.7	1/16/2024	Preet Mood	Reviewed document and no changes are needed
1.8	6/12/2024	Yavuz Alparslan	Remove version number from file name and added 'supply chain notification' under Communication per control IR-6(3).
1.9	6/13/2024	Preet Mood	Reviewed and Approved
1.9	3/4/2025	Yavuz Alparslan	Reviewed document and no changes are needed