# Information Security Standard – Incident Response Plan

## Policy Statement

This Standard supports the Company Information Security & Privacy Policy and outlines the security incident response controls to be implemented across all of Company’s systems.

## Applicability

Compliance with the controls outlined in this document is mandatory for all Company employees, contractors, vendors, and guests.

## Non-compliance

Any instances of non-compliance with the controls outlined in this document should be reported following the procedures outlined in the Reporting Process.

## Scope

The requirements of this standard to all systems that store, process, or transmit Company information; or are used to connect to those systems that are used to store, process, or transmit Company’s information.

## Controls

Security Incident - Any unauthorized event or activity taken by internal or external entities that may adversely affect the confidentiality, integrity, or availability of the Company platform.

**IRP-1** Actions Required - All Employees

1. If you suspect a security incident is either in-process or has occurred, immediately submit a High Risk/High Impact ticket in JIRA.
2. Fully document all information in the JIRA ticket, including but not limited to:
   1. Description of the event
   2. Time of occurrence
   3. Affected system(s)
   4. Impact to customers/systems

**IRP-2** Actions Required - On-Call Engineering and Operations Staff

1. Notify the on-call security analyst via triggering the pagerduty ‘security’ incident
2. Prepare for forensics
   1. If a specific host is thought to be compromised, isolate it from the network by disabling the network interface and set it aside with the power cord still plugged in for the security team to perform forensic analysis. DO NOT TURN OFF THE MACHINE, and DO NOT CONTINUE TO WORK ON THE HOST.
   2. If the machine is a virtual machine or remote, set the firewall rules such that it can only be accessed via inbound SSH and has no outbound access and then take a snapshot of the running host. Download the snapshot for the security team to perform forensic analysis. DO NOT TURN OFF THE MACHINE, and DO NOT CONTINUE TO WORK ON THE HOST.
3. If an account is thought to be compromised, disable the account. If the account cannot be disabled without causing impact to the platform, such as a service account, immediately begin the procedures for a password reset.
4. Following standard engineering and operations processes, including creating a JIRA ticket for the incident if it does not exist and post-mortem document.
5. Document all activities taken, with timestamps for all actions.
6. Record all communications with internal and external parties relating to the incident, including HipChat logs, e-mails, and conversations
7. If incident is Sev-0 or Sev-1 in scale of impact to customers or operations, notify Engineering and Operations Management
8. Update support website using standard timelines
9. In conjunction with on-call security analyst, brief Engineering and Operations Management on issue

**IRP-3** Actions Required - On-Call Security Analyst

1. Review incident with on-call engineer
2. Review actions taken by engineering staff and recommend additional mitigations as necessary and appropriate to contain the incident.
3. In conjunction with on-call engineer, determine incident severity and brief engineering management
4. Notify customer/partner security teams.
5. Perform host and log analysis to determine root cause.

**IRP-4** Actions Required - Engineering and Operations Management

1. Determine if outage response meets necessary bar for activation of the ISCP.
2. Work with CS and Marketing to craft communications to customers
3. Provide guidance to On-Call staff as necessary.

## Appendices

### Document Management

|  |  |  |  |
| --- | --- | --- | --- |
| Author | Syltor Consulting | Version | 1.0 |
| Date Modified | 30 May 2019 | Approver |  |
| Last Reviewed |  | Reviewer(s) |  |
| Review Cycle | Annual | Next Review Date |  |