Incident Response Program

VERSION:	**2022-1**
AUTHOR:	**Technology Operating Committee**
RELEASE DATE:	**October 2022**

Purpose

The purpose of the Incident Response Program (IRP) is to define how Gravyty (hereafter referred to as "the Company") will respond to suspected or actual information security, privacy and unauthorized fund transfer incidents (collectively, hereafter referred to as "incidents" unless noted otherwise). This will identify who is responsible for incident response, what constitutes an incident, how the Company will handle incidents, and communication and reporting requirements.

Scope

This program applies to suspected or actual information security, privacy and unauthorized fund transfer incidents. The definitions for these incident types are as follows:

- **Information Security Incident** – Violation or threat to the Company's information security environment or established information security practices. The following are examples of this incident type:
  - *Suspected virus or malware infection*
  - *Vendor reporting a cyber-attack on their web-based application*
  - *Observed sharing of personal network/application accounts*
  - *Inappropriate usage of the Company's information technology assets*
  - *Stolen or lost Company-issued laptop*
  - *Unauthorized changes to the network, applications and/or databases without the Company's knowledge, etc.*

- **Privacy Incident** – Disclosure of sensitive customer information whether by human error or malicious activity. The following are examples of this incident type:
  - *Customer receives another customer's information*
  - *Customer data being misplaced or stolen*

Roles and Responsibilities

The following are the roles and responsibilities regarding the Incident Response Program:

Individual / Group / Department	Responsibilities
Chief Executive Officer	● Responsible for deciding on the course of action that the IRT will take based on all provided information.
Technology Operating Committee	● Responsible for managing the overall response and recovery activities for all incidents and determining the severity of each incident. ○ Co-Responsible for reviewing incident notifications sent by employees (via email, forms, or other communication). ● Responsible for directing the Information Technology department in incident response efforts. ● Responsible for completing, reviewing and submitting Suspicious Activity Reports for unauthorized fund transfer incidents. ● Responsible for securing the physical crime scene, beginning a chain of custody when necessary. ● Responsible for coordinating and maintaining relationships with local, state, and federal law enforcement. ● Responsible for assessing physical damage to the property.
Director of Marketing	● Responsible for directing communication with media outlets regarding incidents and response efforts.
VP of Engineering	● Responsible for coordinating and reporting on information security, privacy and unauthorized fund transfer incidents and response activities. ● Responsible for completing, reviewing and submitting Suspicious Activity Reports for information security incidents. ○ Co-Responsible for reviewing incident notifications sent by employees (via email, forms, or other communication). ● Responsible for assisting the Incident Response Team on incidents relating to the logical crime scene and preserving information that may assist in an ensuing digital investigation.

Human Resources	● Responsible for researching and responding to reported privacy incidents and coordinating privacy identification, handling, notification, and resolution. ● Responsible for completing, reviewing and submitting. ● Responsible for advising the Chief Technology Officer on incidents involving employees.
Employees	● Responsible for reporting any suspected or actual incidents to the Chief Technology Officer.
Network Security Vendor	● Responsible for providing reactive and proactive services for all network activity that may adversely affect the perimeter network and notifying the Company regarding suspected and actual incidents.
Forensic Services Vendor	● Responsible for providing reactive services for incidents requiring digital investigations or computer forensics.

Incident Response Team

The Incident Response Team helps the Company respond to incidents systematically and effectively, recover from incidents, minimize loss or theft of information and disruption of services, notify required customers and personnel, and deal with any related legal issues. The team members are not static and may include individuals from various departments throughout the Company or vendors based on the incident.

Incident Classification

The Incident Response Program classifies an incident based on the risk they present to the Company, specifically regarding the scope of impact, criticality of system/service, sensitivity of information and probability of exposure.

Incident Risk	Low	Moderate	High
Reputational Risk	● Negative media coverage at a town/city level ● Minor impact to the company brand	● Negative media coverage at a regional, state or county level ● Moderate impact to the company brand	● Negative media coverage at a national/global level ● Significant impact to the company brand
Financial Risk	● Minor monetary losses or fines to the Company and/or customer	● Moderate monetary losses or fines to the Company and/or customer	● Significant monetary losses or fines to the Company and/or customer

Scope of Impact	● Impacts a small portion of the Company's systems and employees ● Impacts a small number of customers	● Impacts a moderate portion of the Company's systems and employees ● Impacts a moderate number of customers	● Impacts the entire Company ● Impacts a significant number of customers
Criticality of System/Service	● Impacts non-critical systems or vendor services		● Directly or indirectly impacts mission-critical systems ● Prevents customers from being able to use services
Sensitivity of Information	● Involves public information	● Involves confidential or internal use only information	● Involves regularly restricted information or sensitive customer information
Probability of Exposure	● Little to no risk of propagation to other systems causing damage or disruption	● Moderate probability of propagating to other systems causing damage or disruption	● High probability of propagating to other systems causing significant damage or disruption

Incident Response Process

The Company uses the following approach when responding to incidents covered within the scope of the Incident Response Program.

Detection & Reporting

The Company requires that employees report suspected or actual incidents to the Incident Response Team by emailing any member of the incident response team. Once such communication is completed and sent by the employee, the Technology Operating Committee and/or VP of Engineering will perform an initial analysis of the incident to help determine its validity and severity.

Containment

The Incident Response Team will determine the appropriate containment strategy based on the incident, such as:

- Does application access need to be restricted until the threat has been appropriately mitigated or removed?
- Is there a potential for damage and theft of Company-owned assets?
- Can the severity of the incident grow larger if not addressed immediately?
- Does evidence need to be preserved for legal purposes?

The Incident Response Team will perform the initial analysis of the incident; however, the Company may also bring in a Forensic Services Vendor to assist in the collection and preservation of electronic information.

Protecting Evidence

In the event that evidence needs to be maintained after being contained, the Incident Response Team will follow general guidelines to protect the evidence, such as:

- If the incident involves a system that is not powered, the power will not be turned back on; however, the power cord and connected devices will be removed.
- If the incident involves a system that is powered, the power will not be turned off.
- If the incident involves a destructive process, the power cord will be removed along with the network cables and connected devices.

The Incident Response Team will perform the initial analysis of the incident; however, the Company may also bring in a Forensic Services Vendor to assist in the collection and preservation of electronic information. Additionally, the Information Technology department may perform preliminary evidence collection by following the procedures provided by the Forensic Services Vendor.

Remediation & Recovery

The Incident Response Team, along with Information Technology and/or Compliance, will determine the appropriate remediation efforts, which may include restoring systems, rebuilding systems, changing passwords, modifying configurations, patching/upgrading systems, etc. Additionally, the remediation efforts will include a review of existing controls that may need to be modified or new controls that need to be implemented to help prevent the incident from reoccurring.

Notification

The Incident Response Team will follow the notification procedure outlined in the Data Security Policy.

Incident Tracking

Incidents reported to the Incident Response Team will be entered into an Incident Tracking Log maintained by the Technology Operating Committee. The purpose of the Incident Tracking Log is to help ensure that the incidents are resolved in a timely manner, root cause analysis is performed, and control gaps are adequately addressed.

Oversight

The Incident Response Team will provide Executive Management with a status of actual incidents and the response efforts. Additionally, the Chief Executive Officer and VP of Engineering will provide a brief overview of reported incidents to the Board of Directors (as needed) to help ensure they are kept aware of incidents impacting the Company.

Resources

The following are contact information and resources to help ensure a successful Incident Response Program:

Individuals & Agencies	
Attorney General – Consumer Protection Department	Seattle Business Regulations: 206-386-1267 Seattle Attorney General: 206-684-8200
Federal Bureau of Investigation (FBI)	FBI – Seattle, WA: 206-622-0460
Law Enforcement	Seattle, WA Police Department: 206-625-5011

Approved by TOC October 2022