Security Incident Response Plan

Policy Statement

Security incidents pose a risk to Castle's business. Quick and effective handling of such incidents is an important factor in minimizing potential damage. This document describes Castle's process for handling security incidents.

Scope: This process applies to all Castle employees, and is part of the Castle corporate information security policy.

General Direction

A security incident is **any intended or unintended action which has a possible impact on the confidentiality, availability or integrity of sensitive information**. Examples are:

- A virus or other malware infection on a company laptop
- Theft of a laptop or mobile device which contains Castle sensitive information
- Accidental and unauthorized disclosure of Castle's strategic plan
- A hacking attempt, possibly detected by Castle's intrusion detection systems
- Detection of a (rogue) wireless access point within a sensitive data environment
- Castle systems being used in an unauthorized manner (e.g. bitcoin mining in AWS)
- Breach resulting in the loss of sensitive data (e.g. social security numbers, consumer PII, customer confidential or strategic information, HR or healthcare records, and so on)
- Unrecognized personnel working in Castle's offices without apparent justification
- Suspicion that an employee is stealing sensitive information to provide to a competitor
- An unknown email or phone call from a person claiming to be a Castle employee and asking for certain sensitive and confidential information (such as a password) without proper and verifiable identification (also known as "social engineering").

Whenever a security incident is detected, the employee detecting the incident must notify the information security department, who will classify the incident and take over the handling process. This can be achieved in one of two ways:

- Sending a notification email to security@castle.io; or
- Notifying a member of the security team in person.

If the incident demands immediate attention, or neither of the notification methods above are available, notification can further be made to the following company personnel:

- Sebastian Wallin
- Johan Brissmyr
- Filip Tepper
- Matthias Thinsz

In either case, notification must be positively acknowledged by the recipient before the hand-off may be considered complete.

Compliance with Regulations

In case of a security incident resulting in the compromise of information that is impacted by a state, federal or other regulation, all such regulations must be followed at all times. For example, a compromise of consumer personal information must be followed by the required notifications in CIPA (California Information Practices Act), civil code 1798, subsections .29 and .82 (aka SB1386) and similar state laws, the EU GDPR, the UK cookie law, etc. All inquiries from law enforcement must immediately be referred to the legal department. It is the expectation that the person managing the incident will follow these guidelines as part of the incident handling process. Further information is available later in this document.

Plan Testing

This plan must be tested at least once every 12 months, either by response to an actual incident or, if no such incident has occurred within the tested period, by emulating a “dummy incident”. Such testing will be coordinated with the information security department, and will involve at least the production environment and operations personnel. When relying on a “response to an actual incident”, evidence is required of an actual incident response process having been successfully initiated and properly followed to conclusion as part of normal operations.

Simulated testing will be communicated in advance to a small group of stakeholders from operations, legal, and public relations, but not otherwise, so as to maintain the integrity of the test.

Using the Plan and Training

All personnel listed in this handling process by name – collectively known as the incident response team (IRT) – must be properly trained in responding to security incidents.

Furthermore, members of the incident response group must continually strive to improve the response plan itself via post-incidents discussion. In particular, a focus should be placed on parts of the plan that did not work well. Improvements to the plan will be made to this document or any derivative process documentation.

Incident Report Documentation

Security incidents should be tracked in Castle's issue tracking platform (https://castleio.atlassian.net), and include enough information to support the handling process included below.

All incidents must be tracked to conclusion. The documentation, including any emails and other related evidence, must be maintained for at least 24 months in a central repository.

Incident Classification

As soon as feasible after initial identification, all incidents will be classified according to their severity. This helps ensure that the incident receives the appropriate attention. Such classification is generally left to the judgment of the incident manager. However, as a guideline and to assist in the classification process, see the following table. When classifying incidents, the most severe applicable classification applies:

Incident Criteria/Factors	Incident severity Characteristics Matrix		
	P2 (Low)	P1 (Medium)	P0 (High)
Application(s) Affected	Internal systems and/or applications	External (and possibly internal) systems or applications	Internal and external systems and applications
Infrastructure	None	Limited scope	Company wide impact
Impact to Users and/or Systems	Affects limited users or limited systems	Department wide impact	Company wide impact
Impact to Public	None	Potential impact	Definite impact
Countermeasures	Solutions are readily available	Weak countermeasures (potential solutions exist)	No countermeasures (no solutions exist)
Resolution Procedures	Available and well defined	Available but not well defined	Not available
Impact to Personal Identifiable Information (PII)	None	Possible	Definite

How to Handle an Incident – General Overview

Use the empty ***incident response form*** available within the security policy repository to track an incident.

Step 1 – Get the Facts and Don't Panic
Get a factual description of the incident as quickly as possible. Maintain objectivity, and do not make assumptions about culpability or accountability. Keep the description short and to the point.

Step 2 – Establish the Source of Notification
Obtain an understanding of the initial incident discovery, specifically who identified the incident, when it was identified, and who was initially contacted.

Step 3 – Understand what Happened
Interview the reporter of the incident and the immediate escalation point. Obtain a description of what steps were taken initially to identify the incident, why and how it was escalated. Understand how the incident was identified, and whether it was triggered by a system alert or log, and obtain a copy of such alerts or logs. Attempt to determine where the incident originated (e.g. office, AWS Network, etc), when it started, and what was compromised, as well as the scope of compromise. **Classify the incident impact and severity once the relevant information .**

Step 4 – Validate the Incident
Describe the steps taken to verify the incident. Ascertain that it qualifies as a security incident, and that it is not a false alarm. Get a copy of all the outputs leading to the conclusion that an incident has happened.

Step 5 – Contain and Correct the Problem
Describe the steps taken to contain the problem. Get copies of containment configurations (e.g. firewall rules), as well as logs and system messages showing progress of successful containment. Ensure proper handling of information as potential legal evidence. Determine if a backup was performed, including whether (1) forensic copies of affected systems had been created for further analysis; (2) a log of commands and other documentation since incident identification has been maintained; (3) a log of all actions taken are retained; and (4) forensic copies are stored in a secure location.

Step 6 – Eradicate the Threat and Restore Operational Status
Describe the steps taken to eradicate the threat and restore systems to operational status. Get pre/post-incident configurations, logs, and system messages. Ensure that systems restored to production are protected against the identified threat. Verify the scope of damages. Assess how long and for what the restored systems will be monitored, and determine if there are any prior benchmarks that could be used as a baseline to compare against monitoring results of the restored systems.

Step 7 – Investigate
Describe the investigation steps taken in order to identify the responsible party and manage the evidence. Make notes of technical steps as well as events, people and times involved. List the evidence collected during the process. In case of non-electronic evidence, seal them in a clearly marked envelope.

Step 8 – Plan for the Future (“Lessons Learned”)
Write down the steps that will be taken in the future in order to eliminate further threat from similar incidents. Include technical and non-technical items. Describe the root-cause analysis and recommended changes to configurations, products and processes.

Legal Compliance

Notice Requirements

Consistent with Castle's corporate security policy, and other applicable laws and regulations, the company may be required to notify regulatory and law enforcement agencies, as well as its customers, of incidents involving unauthorized access to or use of customer or employee information, etc. Castle shall comply with all notice requirements under the security guidelines. The legal department will consult with other representatives, as necessary, to determine whether, and which agencies must receive notice, as well as the manner, content and timing of delivery of such notices, based on certain standards. To the extent necessary, Castle may elect to consult with internal and external counsel.

The requirement should include but are not limited to the following parties (if applicable):

Regulatory Agencies
Law Enforcement
Federal Bureau of Investigation
Local Police Department
Customers
Depending on the nature of the threat and assessed risk, "Standards" for providing notice(s) as a whole or just to those impacted may be used (limited notices)
Service Providers or Third Parties (if any)
Credit Bureaus
Banks and Credit Card Associations (for fraud)

Manner of Delivery of the Notice(s)

Castle will deliver required customer/employee notices in a manner designed to ensure that customers/employees can reasonably be expected to receive them. For example, based on the facts and circumstances, the company may choose to contact all customers/employees affected by phone, mail, or email for those customers/employees whom it has a valid email address and who have agreed to receive communications electronically.

Notice Provisions of State Law

The laws of California and other states require Castle to disclose incidents involving specific events or unauthorized access to or use of customer and employee information. It is the policy of Castle to comply with all such applicable requirements. Upon becoming aware of an incident involving unauthorized access to or use of such information, the legal department will coordinate internal or external counsel where appropriate to direct a review of the relevant state laws to determine whether the breach gives rise to any additional notice requirements.

Notice to Service Providers

Corporate information security guidelines require Castle to be able to address security breaches to customer and employee information hosted on systems maintained by its domestic and foreign service

providers. Accordingly, Castle's relevant service provider contracts will require the service provider to take appropriate actions to address incidents of unauthorized access to the company's customer and employee Information, including investigation and remediation of breach incidents as well as notification to the company as soon as possible of any such incident. This will enable Castle to expeditiously implement its incident response program. In addition, where appropriate, Castle's relevant contracts may contain a clause giving the company the right, through internal and/or external auditors, to conduct due diligence reviews to monitor and ensure the service provider remains in compliance with federal and state laws and regulations as well as company policies.

Incident Response Team (IRT)

- Sebastian Wallin
- Johan Brissmyr
- Filip Tepper
- Matthias Thinsz