Security Incident Response Policy

Double Good Technologies, LP

March 2024

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC7.3 - Incident Detection and Response, CC7.4 - Incident Reporting and Response, CC7.5 - Security Incident Review and Analysis

Table 2: Document history

Date	Comment
Mar 13 2023	Revision for SOC 2 Alignment

1 Purpose and Scope

a. This Security Incident Response Policy (SIRP) establishes controls to ensure:

- Detection of security vulnerabilities and incidents
- Prompt response and containment of security breaches

b. This document provides procedures for security incident response, including:

- Definitions
- Procedures
- Responsibilities
- Performance measures (metrics and reporting mechanisms)

c. This policy applies to all users of information systems within the organization, including:

- Employees
- Contractors
- Third-party vendors with access to organizational systems

2 Background

a. A key objective of the organization's Information Security Program is to focus on detecting information security weaknesses and vulnerabilities so that incidents and breaches can be prevented wherever possible. The organization is committed to protecting its employees, customers, and partners from illegal or damaging actions taken by others, either knowingly or unknowingly. Despite this, incidents and data breaches are likely to happen; when they do, the organization is committed to rapidly responding to them, which may include identifying, containing, investigating, resolving , and communicating information related to the breach.

b. This policy requires that all users report any perceived or actual information security vulnerability or incident as soon as possible using the contact mechanisms prescribed in this document. In addition, the organization must employ automated scanning and reporting mechanisms that can be used to identify possible information security vulnerabilities and incidents. If a vulnerability is identified, it must be resolved within a set period of time based on its severity. If an incident is identified, it must be investigated within a set period of time based on its severity. If an incident is confirmed as a breach, a set procedure must be followed to contain, investigate, resolve, and communicate information to employees, customers, partners and other stakeholders.

3 Definitions

a. **Information Security Vulnerability:** A weakness in an information system, procedures, or controls that could be exploited for unauthorized access or disruption (TSC CC7.3).
b. **Information Security Incident:** A suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, disruption, modification, or destruction of information; or a violation of security policy (TSC CC7.3).
c. **Data Breach:** The unauthorized access or disclosure of sensitive data, as defined by applicable regulations (New definition for SOC 2).

4 Policy

a. All users must report any system vulnerability , incident, or event pointing to a possible incident to the Information Security Manager (ISM) as quickly as possible but no later than 24 hours. Incidents must be reported by sending an email message and slack channel to the Information Security Manager (ISM) as quickly as possible.

b. Users must be trained on the procedures for reporting information security incidents or discovered vulnerabilities, and their responsibilities to report such incidents. Failure to report information security incidents shall be considered to be a security violation and will be reported to the Human Resources (HR) Manager for disciplinary action.

c. Information and artifacts associated with security incidents (including but not limited to files, logs, and screen captures) must be preserved in the event that they need to be used as evidence of a crime.

d. All information security incidents must be responded to through the incident management procedures defined below.

e. In order to appropriately plan and prepare for incidents, the organization must review incident response procedures at least once per year for currency, and update as required.

f. The incident response procedure must be tested on at least twice per year

g. The incident response logs must be reviewed once per month to assess response effectiveness.

5 Procedure For Establishing Incident Response System

a. Define on-call schedule and assign an Information Security Manager (ISM) responsible for managing incident response procedure during each avail-

ability window.

b. Define notification channel to alert the on-call ISM of a potential security incident. Establish company resource that includes up to date contact information for on-call ISM.

c. Assign management sponsors from the Engineering, Legal, HR, Marketing, and C-Suite teams.

d. Distribute Procedure For Execute Incident Response to all staff and ensure up-to-date versions are accessible in a dedicated company resource.

e. Require all staff to complete training for Procedure For Executing Incident Response at least twice per year.

6 Procedure For Executing Incident Response

a. Incident Identification and Reporting

- Users who identify a security incident or vulnerability must notify their immediate manager within 24 hours (TSC CC7.3).
- The manager must immediately notify the on-call ISM for proper response (TSC CC7.4).
- Required notification details include:
  - Description of the incident
  - Date, time, and location
  - Person who discovered the incident
  - How the incident was discovered
  - Known evidence
  - Affected system(s)

b. Initial Investigation and Risk Assessment (within 48 hours)

- The ISM will conduct a preliminary investigation and risk assessment to confirm details (TSC CC7.4).
- If confirmed, the ISM will assess the impact and assign a severity level:
- High: Potentially catastrophic or disrupts daily operations; likely legal/regulatory violation (TSC CC7.4).
- Medium: Harms one or more business units or delays activities (TSC CC7.4).
- Low: Clear policy violation but minimal business impact (TSC CC7.4).

c. Incident Response Activities (based on severity)

- The ISM, in consultation with management sponsors, will determine appropriate response actions to contain and resolve the incident (TSC CC7.4).

d. Evidence Preservation

- The ISM must take all necessary steps to preserve forensic evidence (logs, files) for further investigation and potential law enforcement involvement (TSC CC7.5).

e. Data Breach Communication (High/Medium Severity)

- For High or Medium severity incidents involving a data breach, the ISM will work with designated teams (Brand/Creative, Legal, HR) to create a communication plan for users, the public, and other affected parties (New section for SOC 2).

f. Incident Resolution and Recovery

- The ISM must take all necessary steps to resolve the incident and recover systems, data, and connectivity (TSC CC7.4).
- All technical steps taken during the incident must be documented in the organization's incident log, including:
  - Description of the incident
  - Severity level
  - Root cause (source, malware, vulnerability)
  - Evidence
  - Mitigations applied (patch, re-image)
  - Status (open, closed, archived)
  - Disclosures (parties notified)

g. Post-Incident Activities

- After resolution, the ISM will conduct a post-mortem analysis, including:
- Root cause analysis (TSC CC7.5)
- Documentation of lessons learned (TSC CC7.5)
- The CEO may elect to contact external authorities (law enforcement, investigators) depending on the incident severity (TSC CC7.4).
- The ISM will notify all users of the incident and conduct additional training if necessary (TSC CC7.4).
- HR will take disciplinary action for malicious user activity (TSC CC7.4).

7 Business Continuity and Disaster Recovery (BC/DR)

This organization maintains a separate Business Continuity and Disaster Recovery (BC/DR) plan. Our incident response procedures focus on immediate actions to identify, contain, and resolve security incidents. The BC/DR plan complements these procedures by outlining strategies for long-term operational continuity in the event of a large-scale disruption. These two plans work together to ensure a comprehensive response to security threats.

Here's how these plans work in conjunction:

- During incident response, the focus is on identifying and isolating the threat, minimizing damage.
- Once the immediate threat is contained, the BC/DR plan can be activated to restore critical systems and business functions.
- Lessons learned from incident response investigations can be incorporated into the BC/DR plan to improve future preparedness.

8 Reporting to External Authorities

The organization is committed to cooperating with law enforcement and other relevant authorities in the event of a security incident. The timeframe for reporting incidents to external authorities will depend on the specific nature of the incident and the requirements of any applicable laws or regulations. However, we generally aim to report confirmed data breaches to law enforcement within 72 hours of confirmation.

Here are some factors that may influence the reporting timeframe:

Severity of the incident: High-severity incidents with potential legal ramifications will be reported more promptly. Need for further investigation: Additional investigation may be necessary before a complete report can be made to authorities. Regulatory requirements: Industry regulations or data breach notification laws may dictate specific reporting timeframes. The Information Security Manager (ISM) will work with the Legal department to determine the appropriate timeframe for reporting each incident to external authorities. The organization will strive to balance the need for timely notification with the need for thorough investigation.

9 Review and revision:

This policy will be reviewed and revised periodically to ensure it remains relevant and effective.