Security Incident Response Policy

ACME Evil Anvil Corporation

March 2019

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC7.3, CC7.4, CC7.5

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

1 Purpose and Scope

a. This security incident response policy is intended to establish controls to ensure detection of security vulnerabilities and incidents, as well as quick reaction and response to security breaches.

b. This document also provides implementing instructions for security incident response, to include definitions, procedures, responsibilities, and performance measures (metrics and reporting mechanisms).

c. This policy applies to all users of information systems within the organization. This typically includes employees and contractors, as well as any external parties that come into contact with systems and information controlled by the organization (hereinafter referred to as "users"). This policy must be made readily available to all users.

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.

c. Within this document, the following definitions apply:

    i. *Information Security Vulnerability:* a vulnerability in an information system, information system security procedures, or administrative controls that could be exploited to gain unauthorized access to information or to disrupt critical processing.

ii. *Information Security Incident:* a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of information; interference with information technology operations; or significant violation of information security policy.

3 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 to with details of the incident.

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.

4 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 availability 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.

5 Procedure For Executing Incident Response

a. When an information security incident is identified or detected, users must notify their immediate manager within 24 hours. The manager must immediately notify the ISM on call for proper response. The following information must be included as part of the notification:

   i. Description of the incident

   ii. Date, time, and location of the incident

   iii. Person who discovered the incident

   iv. How the incident was discovered

   v. Known evidence of the incident

   vi. Affected system(s)

b. Within 48 hours of the incident being reported, the ISM shall conduct a preliminary investigation and risk assessment to review and confirm the details of the incident. If the incident is confirmed, the ISM must assess the impact to the organization and assign a severity level, which will determine the level of remediation effort required:

   i. High: the incident is potentially catastrophic to the organization and/or disrupts the organization's day-to-day operations; a violation of legal, regulatory or contractual requirements is likely.

   ii. Medium: the incident will cause harm to one or more business units within the organization and/or will cause delays to a business unit's activities.

   iii. Low: the incident is a clear violation of organizational security policy, but will not substantively impact the business.

c. The ISM, in consultation with management sponsors, shall determine appropriate incident response activities in order to contain and resolve incidents.

d. The ISM must take all necessary steps to preserve forensic evidence (e.g. log information, files, images) for further investigation to determine if any malicious activity has taken place. All such information must be preserved and provided to law enforcement if the incident is determined to be malicious.

e. If the incident is deemed as High or Medium, the ISM must work with the VP Brand/Creative, General Counsel, and HR Manager to create and execute a communications plan that communicates the incident to users, the public, and others affected.

f. The ISM must take all necessary steps to resolve the incident and recover information systems, data, and connectivity. All technical steps taken during an incident must be documented in the organization's incident log, and must contain the following:

    i. Description of the incident

    ii. Incident severity level

    iii. Root cause (e.g. source address, website malware, vulnerability)

    iv. Evidence

    v. Mitigations applied (e.g. patch, re-image)

    vi. Status (open, closed, archived)

    vii. Disclosures (parties to which the details of this incident were disclosed to, such as customers, vendors, law enforcement, etc.)

g. After an incident has been resolved, the ISM must conduct a post mortem that includes root cause analysis and documentation any lessons learned.

h. Depending on the severity of the incident, the Chief Executive Officer (CEO) may elect to contact external authorities, including but not limited to law enforcement, private investigation firms, and government organizations as part of the response to the incident.

i. The ISM must notify all users of the incident, conduct additional training if necessary, and present any lessons learned to prevent future occurrences. Where necessary, the HR Manager must take disciplinary action if a user's activity is deemed as malicious.