SandBox Union

Incident Management Policy

Table of Contents

1. Introduction

This Incident Management policy outlines various incidents that may affect the security and integrity of SandBox Union's information systems and how to respond in the event an incident would occur.

2. Purpose

The purpose of this Incident Management policy is to establish a policy for identifying, containing, mitigating, and reporting security incidents with respect to electronic Protected Identifiable Information.

3. Scope

This Incident Management policy and related policies, standards, and procedures apply to all SandBox Union full-time, part-time, temporary, and intern employees, contractors, sub-contractors, consultants, affiliates, and any individuals or companies utilizing SandBox Union-provided IT equipment, computers, and/or networks or have access to the data environment, including any third-party contracted by SandBox Union to handle, process, transmit, store, or dispose of SandBox Union's data. This includes external partners or suppliers who have access to or are responsible for SandBox Union's information, regardless of its form or medium.

4. Policy Sections

4.1 Disciplinary Process

Sanctions for violations of SandBox Union's security policies shall not commence without prior verification of a breach. The formal disciplinary process shall ensure that correct and fair treatment for employees who are suspected of committing breaches of security and that a graduated response that takes into consideration factors (impact, number of offenses, training, regulatory requirements, and contractual obligations). And for each incident, SandBox Union shall document the personnel involved in the disciplinary process, the steps taken and the timeline associated with those steps, the steps taken for notification, the rationale for the discipline, whether the discipline was due to a compliance failure, and the final outcome.

SandBox Union shall maintain a list of employees involved in security incident investigations and the resulting outcome.

SandBox Union shall ensure individuals are held accountable and responsible for actions initiated under their electronic signatures to help deter record and signature falsification.

4.2 Prevention of Misuse of Information Assets

Management shall approve the use of information assets. If any unauthorized activity is identified by monitoring or other means, this activity will be brought to the attention of

the individual manager concerned for consideration of appropriate disciplinary and/or legal action.

4.3 Reporting Information Security Events

Formal information security event reporting procedures to support the corporate direction (policy) shall be established, together with an incident response and escalation procedure, setting out the action to be taken on receipt of a report of an information security event, treating the breach as discovered, and the timeliness of reporting and response. Organization-wide standards shall be specified for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that is included in the incident notification. This reporting will also include notifying internal and external stakeholders, the appropriate Community Emergency Response Team, and law enforcement agencies in accordance with all legal or regulatory requirements for involving that organization in computer incidents. With the importance of Information Security Incident Handling, a policy shall be established to set the direction of management. Employees and other workforce members, including third parties, shall be able to freely report security weaknesses (real and perceived) without fear of repercussion.

A point of contact shall be established for the reporting of information security events. It will be ensured that this point of contact is known throughout the organization, is always available and is able to provide adequate and timely response. The organization shall also maintain a list of third-party contact information (e.g., the email addresses of their information security officers), which can be used to report a security incident.

SandBox Union implements an insider threat program that includes a cross-discipline insider threat incident handling team.

SandBox Union shall ensure that workforce members do not interfere with federal or state investigations or disciplinary proceedings through willful misrepresentation or omission of facts or using threats or harassment against any person.

SandBox Union shall ensure that violations of these requirements are incorporated into disciplinary procedures.

4.4 Responsibilities and Procedures

SandBox Union shall implement a formal incident response program, which includes the definition of specific phases for incident response. A program of business processes and technical measures will be established to triage security-related events and handle different types of information security incidents, including system failure or loss of service, malicious code, denial of service, errors, unauthorized disclosures of covered information, system misuse, unauthorized wireless access points, and identity theft. In addition to normal contingency plans, the program shall also cover analysis and identification of the cause of the incident, containment, increased monitoring of system use, and planning and implementation of corrective action to prevent recurrence.

SandBox Union shall assign a single point of contact for the organization responsible for sharing information and coordinating responses and has the authority to direct actions required in all phases of the incident response process.

SandBox Union shall test and/or exercise its incident response capability regularly.

4.5 Learning from Information Security Incidents

The information gained from the evaluation of information security incidents shall be used to identify recurring or high-impact incidents and update the incident response and recovery strategy.

7. Revision History

Version	Date	Approved By	Change Description
1.0	04/14/2021	Joseph Organisciak	Initial Creation