Incident Response Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

This Policy governs ABC Company’s detection, response, documentation, and reporting of Incidents affecting Information Resources. Incidents include, but are not limited to, unauthorized access, theft, intrusion, misuse of data, other activities contrary to ABC Company’s Acceptable Use Policy, denial of service, corruption of software, computer, and electronic communication-based events.

# II. Purpose

This policy is established to protect the integrity, availability and confidentiality of information, prevent loss of service, and comply with legal requirements. This policy establishes an incident Response Team and the process for identifying and reporting an incident, initial investigation, risk classification, documentation and communication of Incidents, responder procedures, incident reporting, and training.

# III. Scope

This policy applies to the Risk Management Officer, Chief Security Officer, Executive Management, Director of IT, and Security Staff.

# IV. Policy

The Chief Security Officer (CSO) shall ensure:

* The Risk Management Officer (RMO) is aware of risks related to Information Resources and any changes to Information Resources are communicated to the RMO so that appropriate risk analysis and risk treatment controls can be implemented.
* Procedures and processes identify and respond to suspected or known incidents, mitigate them to the extent practicable, measure harmful effects of known incidents, document incidents and their outcomes, collect evidence, and provide appropriate reporting to ABC Company management.
* Incident response procedures list examples of security incidents and the appropriate responses for each.
* An Incident Response Team has been assembled to receive notice of Incidents and manage the process of investigating, responding to, and reporting of the incident.

A. Establishment of an Incident Response Team

The CSO is responsible for incident detection and remediation of Information Resources. The CSO will consult key representatives of ABC Company’s IT, Human Resources, Legal, Internal Audit, or other departments as warranted to establish an Incident Response Team appropriate to respond to a specific Incident.

As necessary, the CSO and Incident Response Team shall assign Staff to manage specific security incidents:

* Plan. An Incident Response Plan (Plan) shall be developed. The Plan shall be reviewed and approved by the Executive Management or a committee that reports to Executive Management. The Plan shall document applicable state and federal laws, regulations, and standards to ensure response procedures meet appropriate requirements. The Plan shall identify third-party contact information that can assist with the incident and appropriate reporting. The Plan shall be tested at least annually to ensure it is sufficient and effective. The Plan shall be updated as a result of such tests.
* Initial Investigations. The Plan shall provide a quick and orderly response to incidents. The Plan shall identify steps to be followed for the initial reporting of events and subsequent investigations. Where appropriate, Staff shall be on call to handle incidents reported outside of standard business hours.
* Risk Classification. Initial investigations shall identify the incident severity level and classify the risk to the organization according to the guidelines contained in the Risk Assessment Classification section of this policy.
* Documentation and Communications. The initial investigations staff shall inform the CSO of the Incident and the preliminary risk classification. The CSO shall follow the guidelines identified in the Documentation and Communication of Incidents section of this policy.
* Responder Procedures. The CSO shall identify the appropriate procedures and Staff to address the specific incident. Responders will attempt to identify as much information about the event so as to limit additional adverse effects. Responders and appropriate Staff will evaluate and recommend to the CSO appropriate actions to be taken.
* Special Situations/Exceptions. The CSO shall identify and document procedures that address special situations and exceptions.
* Incident Reporting. The CSO shall keep Executive Management informed on the status of current incidents. A post incident report shall be created.
* Training and Testing. The CSO shall ensure Staff have the proper training to fulfill their incident response roles and responsibilities.

B. Identifying and Reporting Incidents

The Incident Response Team shall work with ABC Company departments to establish proactive monitoring systems that can identify potential incidents. Examples of incidents include, but are not limited to, ransomware, malware, data breach, Denial of Service (DoS), insider attacks, etc. In addition, any ABC Company Staff may refer an activity or concern to IT Operations.

Once an incident has been reported, the Incident Response Team will log and track incidents and, working with others as appropriate, take steps to investigate, escalate, remediate, refer to others, or otherwise address as outlined in the remainder of this policy.

In addition to reporting incidents, Staff shall report to the appropriate management any weaknesses or deficiencies in Information Resources.

C. Risk Assessment Classification

The CSO will establish an internal risk assessment classification to focus the response to each incident, and to establish the appropriate team participants to respond. This classification matrix shall correspond to an “escalation” of contacts and indicate personnel at ABC Company to be involved and procedures applicable for each class of incident.

In general, incidents are assigned to one of the following classifications:

* Unauthorized access – a person, process, or program is granted unauthorized physical or logical access to Information Resources. This classification includes a breach of sensitive data and should be reported to CSO as soon as the incident is detected.
* Denial of service (DoS) – an attack that overloads an Information Resource to prevent it from performing its normal function. Distributed Denial of Service (DDoS) attacks are large-scale attacks from multiple sources.
* Malicious software (malware) – infects an operating system or application and prevents the software from performing its intended operation. In addition, the malware may delete software and data, compromise the integrity of information, and disclose sensitive information to unauthorized personnel.
* Improper use – a person, process, or program that violates acceptable use policies. Examples include a disgruntled Staff member who ignores policies and procedures, a network administrator who circumvents log files, and a Staff member who extracts customer lists.
* Scans/probes/attempted access – an unauthorized person, process, or program that attempts to identify vulnerabilities through the use of vulnerability scanning, network mapping, and penetration testing tools.
* Other – this classification includes other types of incidents not described above. For example, unconfirmed incidents, potentially malicious events, or other activity that warrants additional review.

The CSO, working with appropriate ABC Company Staff, shall estimate the financial cost to respond to an incident for each of the above classifications. For example, the cost to respond to unauthorized access to personally identifiable or other Sensitive Information. Such information shall be conveyed to the ABC Company Executive Management or a committee that reports to Executive Management.

D. Documentation and Communication of Incidents

The CSO shall ensure that incidents are appropriately logged and archived. Any incidents involving sensitive information shall be identified so the appropriate security procedures can be followed. The CSO shall provide current status and reports to ABC Company Executive Management.

Wherever possible, documentation of such incidents shall cross-reference other event databases such as IT ticket and network monitoring systems. Any incidents involving systems that are tracked in the inventory database shall be cross referenced in that database with the CSO incident tracking log.

The CSO or Incident Response Team representatives are responsible for communicating the incident to appropriate personnel and maintaining contact, for the purpose of update and instruction, for the duration of the incident.

E. Responder Procedures

The CSO shall maintain standard responder procedures for the response and investigation of each incident, as well as securing the custody of any evidence obtained in the investigation. The application of these procedures shall be governed by the classification described above as well as the Incident Response Plan. Staff shall refer to the Incident Response Plan for specific information on how to manage and respond to incidents. The procedures will specify the location, method of custody for each incident, and if custody of evidence is required.

F. Special Situations/Exceptions

Any personally owned devices, such as phones, wireless devices or other electronic transmitters which have been used to store sensitive information and are determined to contribute to an incident, may be subject to seizure and retention by ABC Company Staff. By using personally owned devices within the ABC Company network for business purposes, Staff are subject to ABC Company policies restricting their use.

Proper forensic procedures, including chain of custody, shall be required for collection, retention, and presentation of evidence to support potential legal action. For more information about retention guidelines, see the Data Retention Policy.

Cloud computing controls shall be in place to ensure privacy and formal notification of a compromise of a Tenant's system(s).

G. Incident Reporting

The CSO shall provide appropriate reporting to ABC Company Executive Management. Such reporting to include, but is not limited to, updates to inform management of relevant details, risks, current status and progress, tasks to be completed, and expected outcomes and dates. Post incident reporting shall include appropriate details, mitigation actions, timeframes, and lessons learned.

In addition to reporting of specific incidents, the CSO shall provide annual reporting to Executive Management that summarizing incidents reported and actions taken. The annual report shall identify numbers and types of incidents, impact, costs incurred, lessons learned, and other relevant factors.

Incident reports and supporting documents shall be retained in accordance with ABC Company’s Data Retention Policy.

On an on-going basis, the RMO shall identify data breach notification requirements. In the event of a data breach, the RMO shall notify ABC Company Executive Management of relevant requirements so that appropriate action can be taken.

H. Training

The CSO shall be responsible for ensuring that incident response team members and related Staff have the proper training. Information shall be published for all Staff regarding the reporting of computer anomalies and incidents. Such information should be included in routine employee awareness activities.

Staff shall acknowledge their duties and responsibilities and agree to adhere to appropriate incident response policies, procedures, plans and related documents. No less than annually, awareness and refresher training shall be provided to maintain incident response readiness and competency. The CSO may also arrange incident response exercises to test and evaluate Staff, related procedures, and assess the ability to respond to incidents in a timely and effective manner.

# V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to the Risk Management Officer, Chief Security Officer, Executive Management, Director of IT, and Security Staff.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT EDM01.01, APO12.02, APO12.07, APO13.07, DSS03.02, DSS05.02, MEA03.01

GDPR Article 33, 34

HIPAA 164.308(a)(6)(ii), 164.314(a)(2)(i), ARRA 13402

ISO 27001:2013 A.16

NIST SP 800-37 3.5, 3.7

NIST SP 800-53 AU-4, AU-6, AU-10(3), AU-11, CA-7, IR-4, IR-6, IR-8, SI-2, SI-4

NIST Cybersecurity Framework DE.AE-2-4, DE.CM-1-6, DE.DP-2, RS.MI-2, RC.RP-1

PCI 11.1.2, 11.5.3, 12.8.3, 12.10