Incident Response Policy

CONTENTS

EXECUTIVE SUMMARY

An effective Incident Response Program enables Holmes Murphy and Associates to follow best practices for identifying, investigating and responding to a security incident, respond to a security incident in a fast, effective and consistent manner, and protect Holmes Murphy and Associates' organization from the consequences of a breach of its responsibilities.

REFERENCES

NIST800-53r5

1.0 - PURPOSE

The purpose of the Incident Response Policy is to clearly define IT roles and responsibilities for the investigation and response of computer security incidents and Data Breaches.

2.0 - SCOPE

The policy covers aspects of the systems that involve the overall security of Holmes Murphy and relates to all services and departments. This policy will be reviewed after any intrusions and all security incidents but more frequently if appropriate.

This policy also attributes to any device that is connected to the network or that holds and stores any company data.

3.0 - POLICY

3.1 – Holmes Murphy and Associates provide incident response training to information system users consistent with assigned roles and responsibilities:

- Provide training before assuming an incident response role or responsibility, when required by information system changes, and annually thereafter.
- Provide additional or supplemental IR training when information system changes occur.
- Provide ongoing refresher training on an annual basis.

3.2 - All personnel are required to report suspected security events to Information Security personnel immediately after the event is discovered.

3.3 - The Incident Response Team (IRT) detects and investigates security events to determine whether an incident has occurred, and the extent, cause and damage of incidents. The IRT coordinates with key internal stakeholders as necessary to complete the information gathering and analytics necessary.

3.4 - The IRT directs the recovery, containment and remediation of security incidents and may authorize and expedite changes to information systems necessary to do so. The IRT coordinates response with external parties when existing agreements place responsibility for incident investigations on the external party.

3.5 - During the conduct of security incident investigations, the IRT is authorized to monitor relevant IT resources and retrieve communications and other relevant records of specific users of IT resources, including login session data and the content of individual communications without notice or further approval and in compliance with the Monitoring of IT Resources Policy.

3.6 - Any external disclosure of information regarding information security incidents must be reviewed and approved by the Information Security Officer, Legal, and other stakeholders as appropriate. The information will be sanitized to prevent the disclosure of confidential and/or Personally Identifiable Information.

3.7 - The IRT coordinates with law enforcement, government agencies, peer IRTs and relevant Information Sharing and Analysis Centers (ISACs) in the identification and investigation of security incidents. The IRT is authorized to share external threat and incident information with these organizations.
3.8 – Holmes Murphy and Associate must retain all documents and data related to an incident according to the data retention schedule.

3.9 – Incident Response Plan
Holmes Murphy maintains a formal Incident Response Plan that:

- Provides the organization with a roadmap for implementing its incident response capability.
- Describes the structure and organization of the incident response capability.
- Provides a high-level approach for how the incident response capability fits into the Holmes Murphy processes.
- Meets the unique requirements of the Holmes Murphy, which relate to mission, size, structure, and functions.
- Defines reportable incidents.
- Provides metrics for measuring the incident response capability within the Company.
- Defines the resources and management support needed to effectively maintain and mature an incident response capability.

3.10 – Information Security coordinates at least annual testing and recertification of the Incident Response Plan.

4.0 – COMPLIANCE & AUDITING

4.1 Policy Enforcement

Any violations of this policy may result in disciplinary action up to and including termination of employment.

4.2 Policy Validation Activities

Auditing will occur to document workstations not seen on the network for a specified time and will be reported in the Information Security monthly report.

The Technology Operations department will ensure perpetual updates are made to the asset management system.

4.3 Policy Exceptions

Any exception to this policy will be documented and approved by executive leadership.

5.0 – RELATED POLICIES & STANDARDS

Incident Response Standards and Procedures
Incident Check List
Security Monthly Report
Acceptable Use Policy

6.0 - RESPONSIBILITIES

Incident Response Team

The Incident Response Team (IRT) detects and investigates security events.

Information Security

Information Security assess security events and coordinates IRT as appropriate.

7.0 – DEFINITIONS

Incident Response Team: A function of the Information Security Office responsible for receiving, reviewing, and coordinating the response to Monthly Security reports and activity involving Data and/or Information Systems.

Data Breach: Unauthorized access, acquisition, use or disclosure of Restricted Data. Data breach notifications are subject to regulatory requirements following a privacy investigation and risk assessment.

Incident: An event, whether electronic, physical or social that adversely impacts the confidentiality, integrity or availability of data or information systems; or a real or suspected action, inconsistent with Acceptable Use policies.

Information System: An individual or collection of computing and networking equipment and software used to perform a discrete business function.

APPROVAL AND OWNERSHIP

Approved By	Title	Date
André Carroll	Analyst	May 2022
Bryan Thompson	Information Security	August 2023