WILEY

Incident Response Policy

1. Introduction

1.1. Purpose:

The purpose of the Incident Response (IRO) policy is to establish and maintain a capability to guide Wiley's response when security-related incidents occur.

2. Policy:

Wiley shall maintain a cybersecurity incident handling capability that includes adequate preparation, detection, analysis, containment, recovery, and reporting activities.

This policy is supported by the following control objectives, standards, and guidelines.

IRO-1: Incidents Response Operations

Wiley is required to document enterprise-wide incident response controls that, at a minimum, include:

(a) A formal, documented Incident Response Plan (IRP); and
(b) Processes to facilitate the implementation of the incident response processes and associated controls.

The objective is to ensure a consistent and effective approach to the management of cybersecurity incidents, including communication on security events and weaknesses.

IRO-2: Incident Handling

Wiley management and IT staff are required to:

(a) Investigate notifications from detection systems.
(b) Identify and assess the severity and classification of incidents.
(c) Define appropriate actions to take in response to the incident; and
(d) Respond with appropriate actions to minimize impact and ensure the continuation of business functions.

Organizations recognize that incident response capability is dependent on the capabilities of organizational systems and the mission/business processes being supported by those systems. Therefore, organizations consider incident response as part of the definition, design, and development of mission/business processes and systems. Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function).

IRO-3: Incident Response Plan (IRP)

Wiley management and IT staff are required to establish processes and technical measures to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.

It is important that organizations develop and implement a coordinated approach to incident response. Organizational missions, business functions, strategies, goals, and objectives for incident response help determine the structure of incident response capabilities. As part of a comprehensive incident response capability, organizations consider the coordination and sharing of information with external organizations, including, for example, external service providers and organizations involved in the supply chain for organizational systems.

IRO-4: Incident Monitoring

Mechanisms should be put in place to monitor for cybersecurity incidents.

Documenting system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

IRO-5: Incident Reporting

For actual or suspected cybersecurity incidents:

(a) Users are responsible for reporting system weaknesses, deficiencies, and/or vulnerabilities through appropriate management channels as quickly as possible.
(b) Information security events should be reported through appropriate management channels as quickly as possible; and
(c) If a breach occurs, breach notification procedures must occur without unreasonable delay, except:
    1. When a law enforcement agency has determined that notification will impede a criminal investigation; or
    2. To discover the complete scope of the breach and restore the integrity of the system.

The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for regulatory agencies. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable laws, policies, regulations, standards, and guidance.

IRO-6: Root Cause Analysis (RCA) & Lessons Learned

Incident response personnel are required to:

(a) Perform a Root Cause Analysis (RCA) following events that trigger usage of the Integrated Security Incident Response Team (ISIRT); and
(b) Incorporate lessons learned in updates to Incident Response Plans (IRPs).

3. Revision History:

Document Properties

Policy	Incident Response Policy
Last Review Date	21st June 2024
Approved by	Robyn Wright – CISO & DPO
Classification	**Public (Can be externally shared)**