WILEY

Information Security Policy

1. Introduction

1.1. Policy Purpose:

The purpose of the Wiley Information Security Program (WISP) is to prescribe a comprehensive framework for:

- Creating a leading practice-based Information Security Management System (ISMS) that is structured on leading frameworks such the NIST Cybersecurity Framework (CSF) and Payment Card Industry Data Security Standard (PCI-DSS)
- Protecting the confidentiality, integrity, and availability of Wiley data and systems.
- Protecting Wiley, its employees, and its clients from illicit use of Wiley systems and data.
- Ensuring the effectiveness of security controls over data and systems that support Wiley's operations.
- Recognizing the highly networked nature of the current computing environment and provide effective company-wide management and oversight of those related cybersecurity risks; and
- Providing development, review, and maintenance of minimum-security controls required to protect Wiley's data and systems.

2. Policy:

These policies, standards and guidelines apply to all Wiley data, systems, activities, and assets owned, leased, controlled, or used by Wiley, its agents, contractors, or other business partners on behalf of Wiley. These policies, standards and guidelines apply to all Wiley employees, contractors, sub-contractors, and their respective facilities supporting Wiley business operations, wherever Wiley data is stored or processed, including any third-party contracted by Wiley to handle, process, transmit, store, or dispose of Wiley data.

These policies do not supersede any other applicable law or higher-level company directive or existing labor management agreement in effect as of the effective date of this policy.

Wiley reserves the right to revoke, change, or supplement these policies, standards, and guidelines at any time without prior notice. Such changes shall be effective immediately upon approval by management unless otherwise stated.

2.1. Policy Information:

This document is the official Wiley Information Security Program and is authorized by the Executive Leadership Team. It is the responsibility of every Wiley personnel to follow the Wiley Information Security Policy for the overall security environment to operate effectively.

Formal security awareness programs are implemented to ensure all colleagues are aware of their roles and responsibilities pertaining to security. The security awareness program provides multiple methods of communicating awareness and educating personnel. This may include posters, newsletters, emails, PowerPoint presentations, web-based training, meetings, and promotions.

2.2. Wiley Information Security Program Overview

2.2.1. Introduction

The Wiley Information Security Program provides information on the prescribed measures used to establish and enforce the cybersecurity program at John Wiley and Sons, Inc. (Wiley).

Wiley is committed to protecting its employees, partners, clients, and Wiley from damaging acts that are intentional or unintentional. Effective cybersecurity is a team effort involving the participation and support of every Wiley user who interacts with data and systems. Therefore, it is the responsibility of every user to know these policies and to conduct their activities accordingly.

Protecting company data and the systems that collect, process, and maintain this information is of critical importance. Consequently, the security of systems must include controls and safeguards to offset possible threats, as well as controls to ensure availability, integrity, confidentiality, and safety.

Commensurate with risk, security measures must be implemented to guard against unauthorized access to, alteration, disclosure or destruction of data and systems. This also includes protection against accidental loss or destruction.

2.2.2. Wiley's Global Security Organization

The Wiley Global Security Organization pursues the following key objectives:

• Safeguard Wiley's employees and assets through the execution of an effective, employee centered strategy, supporting continuous and sustainable internal business execution.

• Protect persons, property, goodwill, and buildings from the external forces of nature, accidental damage-causing events, and intentional actions that disrupt operations or cause damage.

• Define and deploy Wiley's product security strategy across all development units, product security research, security enablement, validation and code analysis, product security response, and product security communication.

• Secure reliable IT services across Wiley by providing strategic directions for IT security & risk. Define the cloud security strategy at Wiley leveraging a multi-dimensional security and compliance approach as well as addressing data protection to establish and maintain a state- of-the-art security architecture including cyber security.

3. Revision History:

Document Properties

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