WILEY

Security Awareness, Training and Education Policy

1. Introduction

1.1. Policy Purpose

The purpose of the Security Awareness & Training (SAT) guideline is to develop a security-minded workforce. This guideline document specifies the Wiley internal information Security Awareness and Education (SAE) program to inform and assess all staff regarding their information security obligations.

1.2. Policy Scope

This document applies throughout Wiley as part of the corporate governance framework. It applies regardless of whether the staff members use computer systems and networks, since all staff are expected to protect all forms of information assets including computer data, written materials / paperwork, and intangible forms of knowledge and experience. This program also applies to third party contingent workers working for the organization whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g., by generally held standards of ethics and acceptable behavior) to comply with our information security policies.

1. Policy

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

1.3. SECURITY-MINDED WORKFORCE

Information security workforce development and improvement programs are complementary to organizational security awareness and training programs. Information security workforce development and improvement programs focus on developing and institutionalizing core cybersecurity capabilities of selected personnel needed to protect organizational operations, assets, and individuals.

Initial orientation and ongoing security training should include the following topics:

- Information security basics
- Cybersecurity policies and best practices
- Email policy
- Acceptable usage policy
- Data classification & handling
- Malicious software & spam
- Offsite security / security at home
- Wireless security
- Third party security (outsourced vendors)
- Visitor security procedures
- Incident response procedures
- Business continuity roles and procedures

- Password Management
- Change and access Management.
- Information security compliance and standards

1.4. SECURITY AWARENESS

Organizations generally determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the systems to which personnel have authorized access. The content includes a basic understanding of the need for cybersecurity and user actions to maintain security and to respond to suspected security incidents.

1.5. SECURITY TRAINING

Methods can vary depending on the role of the personnel and their level of access to sensitive data. Colleagues should complete training courses upon hire and at least annually thereafter. The security awareness and training program should include, at a minimum, the following components:

- Training goals.
- Target audience(s).
- Learning objectives.
- Deployment methods.
- Evaluation method to determine training effectiveness.
- Frequency.
- Duration.
- Deliverables or handouts; and
- Attendance tracking.

2. Revision History:

Document Properties

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