WILEY

Data Classification & Handling Policy

1. Introduction

1.1. Purpose

Wiley's Data Classification and Labelling Policy establishes a framework for classifying data based on its level of sensitivity, value, and criticality to Wiley. In accordance with all applicable legal requirements, Wiley shall protect data in both hardcopy and digital form by limiting access to authorized users and utilizing methods of sanitizing or destroying media so that data recovery is technically infeasible. Data Classification will aid in determining the baseline security and privacy controls required to protect Wiley data.

1.2. Scope

The purpose of the Data Classification and Labelling Policy is to ensure that technology assets are properly classified, and measures are implemented to protect Wiley's information and third parties entrusted by Wiley to manage information from unauthorized disclosure, regardless of it is being transmitted or stored. Applicable statutory, regulatory, and contractual compliance obligations dictate the safeguards that must be in place to protect the confidentiality, integrity, and availability of data.

2. Policy

2.1. Compliance

Compliance Measurement: The IT Governance, Risk and Compliance (IT GRC) team will monitor and verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Non-Compliance: An employee found to have violated or failure to comply to this policy may be subject to disciplinary action, up to and including termination of employment, termination of contract, and penalties or criminal sanctions, depending on the circumstances. All suspected or known violations of the Data Classification Policy or any other Wiley Information Security Policy must be reported to the Security and Compliance team.

2.2. Data Classification Management

Wiley Process/Business/Data owners are responsible for identifying and classifying the data that resides within their applications or that are stored within their organizations data storage sites (i.e., SharePoint/Team Drive, File shares, etc.), under clearly defined authorization boundaries. Classification

should be based on the requirements for confidentiality, integrity, and availability of the data, as well as the potential impact of data loss.

Assets must be classified in terms of system criticality and data sensitivity. Asset custodians and Process/Business/Data owners are required to:

a. Categorize the information system and data; and

b. Where applicable, document the security categorization results (including supporting rationale) for the information system.

2.3. Data Classification Levels (DCLs)

- **DCL Level 1: Public**

This classification applies to information which has been explicitly approved by Wiley Process/Business/Data owners for release to the public.

- **DCL Level 2: Internal**

This classification applies to information that is specifically meant for employees (and/or contingent workers-contractors where applicable) of Wiley.

- **DCL Level 3: Restricted and Regulatory**

This classification applies to any sensitive or critical business information which is intended for use within Wiley and should be limited to a need-to-know basis. Its unauthorized disclosure, alteration or destruction of the data could adversely impact Wiley and/or its stakeholders leading to legal and financial repercussions and adverse public opinion.

3. Revision History:

Document Properties

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