WILEY

Acceptable Use Policy

1. Introduction

1.1. Policy Purpose:

The primary purpose of this policy is to protect sensitive information including personal data stored as well as maintaining the confidentiality, integrity and availability of Wiley information and assets.

1.2. Policy Scope

This policy applies to all personnel (e.g., employees, contractors, consultants, suppliers, customers, government, academic agencies, and all personnel affiliated with third parties) worldwide who access and/or use Wiley devices and data.

2. Policy

2.1. Acceptable Use

1. It is acceptable to use Wiley computers for legitimate business purposes, if there is any uncertainty, employees should consult their supervisor or HR department.
2. Approval from management is required to use critical technologies.
3. Authorized users are individually responsible and accountable for any use of their account and password. These passwords should not be shared under any circumstances.
4. To determine the owner, contact information, and purpose of devices, asset tags shall be placed on each device accurately and readily.
5. Automatically disconnect remote access sessions after a period of inactivity.
6. Remote access systems for use by vendors and business partners must only be activated when needed by vendors and business partners, with deactivation after use.
7. Copying, moving, or storing of Cardholder Data onto local hard drives/removable media when accessing such data via remote access is prohibited.
8. Personnel shall report any suspected information security incident/non-compliance.

2.2. Unacceptable Use

1. Violations of the rights protected by copyright, trade secrets, patents or Intellectual Property or similar laws is strictly prohibited.
2. Revealing passwords, usernames or allowing use of your account by others is strictly prohibited.
3. Colleagues must not engage in activities that may harass, threaten, or abuse others.
4. Storage, distribution of music, video, or digital photograph files for personal use on Wiley equipment are prohibited, unless authorized.

5. Attempting obscure or concealed activities is strictly prohibited.
6. Personal hotspot for public access is not allowed.
7. Non mobile equipment must not be taken outside premises, without approval and classified data must not be shared without prior approval.
8. Storing any personal data onto Wiley assets is not allowed.
9. Engaging in activity that may: harass, threaten, or abuse others, degrade the performance of Wiley resources is not allowed.
10. Bypassing Wiley assets security controls or authentication procedures is strictly prohibited.

2.3. Remote Working Guidelines

When colleagues work remotely, adequate remote working security measures shall be established and implemented. At a minimum,

- establishing a secure communication channel between the remote workers and the network use of appropriate authentication mechanisms
- revocation of authority, access rights and return of equipment will be in place.

2.4. SAFEGUARDING SENSITIVE INFOMRATION AND OTHER NON-PUBLIC DATA

For sensitive and other non-public data:

- Access must be limited to only those who require it as part of their job function.
- No data shall be exported to any other non-Wiley system or shared otherwise without written approval of the data owner.
- Use of cloud or other non-Wiley mass storages prohibited.

3.0. Appendix A

Data Security - DOs and DON'Ts

DOs:	DON' Ts:
DO Lock your computer screen whenever it is unattended.	DON'T allow others to use your login ID or password.
DO Report suspicious or irregular computer behavior to Service Desk	DON'T allow vendors, contractors, or other third parties remote access to your PC.
DO Use care when entering passwords in front of others.	DON'T write down passwords anywhere.
DO Change your password immediately if you suspect it has been compromised	DON'T open electronic mail or its attachments if the sender is unknown or suspicious.
DO Dispose of confidential, restricted, and regulatory information (sensitive information including personal data), including faxes and other forms of hard copies by using on-site shredding boxes; hard drives and other electronic media must be degaussed and/or physically destroyed.	DON'T provide information such as login ID's, passwords, social security, etc. over the phone or electronic email requests with links. These are often fraudulent and are targeted to steal sensitive information or your identity.

4.0. Revision History:

Document Properties

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