WILEY

Access Control Policy

1. Introduction

1.1. Introduction

This document is the Security Technical Implementation Guide (STIG) for Access Controls. This is a supplemental guide that should be viewed in corroboration with the Wiley Information Security Program (WISP).

1.2. Objective

The purpose of this policy is to establish a standard process for granting, modifying, and revoking access to information processing facilities at Wiley for its employees, contractors and third parties. Wiley has taken measures to implement access control across its networks, IT systems and services to provide authorized and appropriate user access, and to ensure appropriate preservation of data confidentiality, integrity, and availability. Access credentials are an important aspect of information security. They are the front line of protection for information.

1.3. Scope

The policy applies to information processing facilities including information systems, applications and network devices included in the Information Security Management System scope and boundaries at Wiley and applicable to all employees of Wiley, as well as all third-party contractors and agents of Wiley, government, academic agencies that have access to Wiley information, Wiley business Systems and applications owned or leased by Wiley.

2. Policy

2.1. Compliance

2.1.1. Compliance Measurement

The IT GRC (IT Governance Risk and Compliance) 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.

2.1.2. Exemptions

While every exception to a standard potentially weakens protection mechanisms for Wiley systems and underlying data, occasionally exceptions will be required. When requesting an exception, users are required to submit a business justification for deviation from the standard. All exemptions must be reviewed and signed-off and will be tracked.

2.2. 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.

2.3. User Access Management

The allocation of access rights to information systems and services shall be done in accordance with this policy which encompasses all stages in the life cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention shall be given, where required, to controlling the allocation of privileged access rights, which could allow users to override the system controls. Access should be granted on a business "need to know" basis.

Assign all users a unique ID before allowing them to access system components by ensuring each user is uniquely identified instead of using one ID for several employees. Authentication mechanisms are assigned to an individual account and should not be shared among multiple accounts.
Manage IDs used by third parties to access, support, or maintain system components via remote access, enabling only during the time period needed and disabling when not in use.

2.4. Major components in consideration:

- Access is defined based on "Least privilege" principles Access will be revoked in a timely manner.
- Accounts and access privileges should be reviewed periodically.
- All vendor-supplied default accounts must be disabled, or default passwords changed.

2.5. Revision History:

Document Properties

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