WILEY

Vulnerability Management Policy

1. Introduction

1.1. Policy Purpose:

Vulnerability Management is the activity of remediating, mitigating, or developing compensating controls to address security vulnerabilities identified within Wiley network, systems, application, and other assets. The purpose of this policy is to establish rules and principles for managing and remediation of threats and vulnerabilities in Wiley owned network infrastructure, servers, operating systems on virtual machines, cloud-hosted server operating systems, database servers, databases, and applications.

2. Policy:

Vulnerability management is a never-ending process that requires Wiley to proactively manage vulnerabilities both in how its assets are configured and the level of currency in software patching. Therefore, Wiley a risk-based approach minimizes its attack surface through aggressive vulnerability management and patching operations.

2.1. Vulnerability Identification

Vulnerability identification involves the process of discovering vulnerabilities and adding identified vulnerabilities into an inventory within the target environment. To identify vulnerabilities, Wiley uses different sources such as vulnerability scanning, penetration testing, bug bounty sources etc.

2.2. Prioritization Based on the Severity Level

The Asset/Application Owner (respective vulnerability report recipients and accountable party to remediate the vulnerabilities) should prioritize the remediation efforts based on the severity level and the defined SLAs of the vulnerability. Severity for each vulnerability is determined based on the global accepted vulnerability management standards such as Common Vulnerability Scoring SystemV3 (CVSS V3), Open Web Application Security Project (OWASP)Risk Scoring, ISO 31000, etc.

2.3. Vulnerability Remediation/Risk Mitigation

2.3.1. Wiley Vulnerability Remediation Process

As vulnerabilities are identified the Asset/Application Owner should remediate all identified vulnerabilities based on the defined Service Level Agreement's (SLA's) or, in rare cases where remediation is not possible, respective owners are required to follow Wiley Information Security Exemption Process with clearly documented compensating controls to mitigate the risk.

2.3.2. Wiley Information Security Exemption Process

Exemption requests are reviewed to ensure it meets all the requirements to be considered for exemption and may require a review with appropriate application/infrastructure, etc. to ensure agreement that the exemption cannot be remediated. The exemption request & approval process requires, at a minimum,

- Clearly documented vulnerability & risk
- Valid business justification
- Clear implementation plan/corrective action plan with agreed specific agreed deadlines
- Valid mitigation and/or compensation controls and associate impact
- Formal business owner/s approval
- Security approval

3. Revision History:

Document Properties

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