WILEY

Technical and Organizational Measures

Cybersecurity and Privacy Strategy

Wiley protects its infrastructure and the personal data within it according to the information security principles of confidentiality, integrity, and availability. Our security program is based on the NIST Cybersecurity Framework (CSF), including but not limited to our policies, standard operating procedures, and technical controls. Our privacy program is based on the NIST Privacy Framework to complement and expand our security controls while meeting contractual and legal privacy requirements. Wiley's approach to security and personal data protection incorporates both technical controls and organizational processes.

Confidentiality

A mandatory security education and awareness program is in place to educate internal users on the importance of their obligation to protect the confidentiality of personal data. Employee background checks are performed before granting personnel any data access, and employees are required to acknowledge the commitment to confidentiality of any data they may access in the performance of their duties. Single sign-on (SSO), multi-factor authentication (MFA), and complex password requirements are in place to enforce secure authentication. Wiley follows the principle of least privilege by restricting data access to only individuals with a valid job-based reason to access production information.

Vendor contractual obligations are required for third-party sub-processors prior to any personal data access or transfer to require that the same level of protection be maintained throughout the duration of any vendor engagements, with stipulations covering security and confidentiality of personal data.

Wiley's information security policy requires all sensitive data to be encrypted both in transit and at rest. Endpoint protection is implemented to prevent and detect malware and other security threats. Firewalls and network anomaly detection systems are continuously monitored. The Wiley SOC monitors all system security alerts and investigates incidents which may impact the confidentiality, integrity, or availability of the environment or data within it.

Integrity

Wiley uses only hosted data center vendors with appropriate physical security and environmental controls which adhere to SOC 2 Type II as well as ISO 27001 certification standards. Production data is separated from development environments, and a formal change management process is in place to prevent unauthorized changes. To manage vulnerabilities, monthly scans are performed to confirm that the appropriate level of security patching and configuration is maintained. Secure audit logs are in place for nonrepudiation and traceability.

Availability and Resilience

Wiley uses industry-recognized hosted data center vendors with ISO 27001 and/or SOC 2 certifications to achieve high availability and resilience. Business continuity and disaster recovery plans are in place and tested periodically to confirm process effectiveness. Backups are taken and stored per data classification and retention requirements to enable restoration. Anti-DDoS protection is in place, and application security reviews are conducted on Wiley sites.

Risk Management

Wiley has implemented a data risk management strategy that considers the risks of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed. Wiley considers the likelihood and severity of the risks to individuals whose personal data Wiley may process in the performance of service contracts. Data protection is considered throughout the lifecycle of products and services, and technical personnel are trained in privacy by design and default.

Incident Response and Breach Notification

Wiley maintains a 24x7x365 Security Operations Center (SOC) that responds to and investigates system or security alerts as well as reported incidents. Wiley has implemented an Incident Response Plan (IRP) which prioritizes regulator and/or client breach notification requirements when they are applicable to a security or privacy incident. Where Wiley is engaged as a sub-processor on behalf of a client, Wiley will not notify individual data subjects affected by a breach directly and will instead notify the client of a data breach no later than the timeline specified in the agreement.