SECURITY EXHIBIT

Last updated: 23 February 2026

In order to protect the confidentiality, integrity, and availability of its internal and Customer data, Pendo has implemented an information security program that includes the following technical, administrative/organizational, and physical controls:

Governance and organizational controls.

Reporting relationships, organizational structures, and proper assignment of responsibilities for system controls, including the appointment of the executive-level Chief Information Security Officer (CISO) with responsibility for oversight of service organization controls for security, availability, processing integrity, confidentiality, and privacy of Customer applications/information, are documented and communicated.

Pendo has established a risk assessment framework used to evaluate risks throughout the company on an ongoing basis. The risk management process incorporates management's risk tolerance, and evaluations of new or evolving risks.

Personnel security:

a. Job requirements are documented in job postings and candidates' abilities to meet these requirements are evaluated as part of the hiring process.
b. Members of the Pendo workforce that have access to Customer data are required to undergo background checks.
c. Pendo employees receive training in data privacy concepts and responsibilities, as well as Pendo commitments on privacy, upon their hire and refresher training on an annual basis.
d. Pendo personnel are required to read and accept the Pendo's Code of Conduct and the statement of confidentiality and privacy practices upon their hire and to formally reaffirm them annually thereafter.

Third party management:

a. Pendo monitors performance of services housed at third-party locations for adequate performance per service level agreements.
b. Confidential information is disclosed only to third parties who have agreements with Pendo to protect personal information in a manner consistent with the relevant aspects of Pendo's privacy policies or other specific instructions or requirements.
c. Pendo evaluates the ability of third parties to meet the contractual security requirements. For those storing or processing Pendo's confidential information, the third party is required to hold an audited third party security attestation (e.g. SOC 2 Type II, ISO 27001)
d. Non-Disclosures agreements are in place with third parties governing authorized access to confidential information

Incident management:

a. Policies and procedures for operational and incident response management require incidents to be logged and reviewed with appropriate action (e.g. system changes) taken if necessary.
b. A formal incident response plan and standard incident reporting form are documented to guide employees in the procedures to report security failures and incidents.
c. The incident response plan enforces a process of resolving and escalating reported events. Its provisions include consideration of needs to inform internal and external users of incidents and advising of corrective actions to be taken on their part as well as a "post mortem" review requirement.

Change management:

a. Pendo application system changes include documentation of authorization, design, implementation, configuration, testing, modification, approval commensurate with risk level.
b. Pendo's change management policy and procedures require review and authorization by appropriate business and technical management before system changes are implemented into the production environment.
c. Changes are tested in a separate test environment prior to moving them to the production environment.
d. The change management process includes identification of changes that require communication to internal or external users. System and organizational changes are communicated to internal and external users through Pendo’s application.

Identity and access management:

a. Pendo personnel are assigned unique usernames and are required to use strong passwords for access to Pendo’s systems. Shared accounts are not allowed unless required for specific use cases that have been authorized by the CISO.
b. Wherever technically feasible, two-factor authentication is used to access Pendo’s system and applications.
c. System access rights are granted or modified on a business-need basis depending on the user's job role and/or specific management request.
d. Pendo performs reviews of privileged and regular user access to production critical systems on a quarterly basis to determine access appropriateness.
e. Access controls are in place to restrict access to modify production data, other than routine transaction processing.

Vulnerability management:

a. On at least an annual basis, penetration testing is performed on Pendo’s application and infrastructure.
b. On at least a weekly basis, Pendo executes vulnerability scans to detect vulnerabilities in Pendo’s application.
c. For penetration tests and vulnerability scans, Management addresses all vulnerabilities identified in the scans within defined timeframes based on severity level.

Logical security controls:

a. External points of network connectivity are protected by firewalls.
b. Anti-virus/malware and endpoint detection and response software is in place on all computers and updated regularly to protect computers (e.g. laptops) used by Pendo personnel.
c. Pendo's application includes code validation checks for inputs outside of acceptable value ranges, which triggers alerts that are addressed.
d. Sensitive data is stored on secure cloud services and is protected and encrypted when in transit and at rest. TLS, HTTPS, SSH, SFTP, or other encryption technologies are used to protect data in transit. AES-256 or other appropriate industry standard standards are used to protect data at rest.
e. Pendo's policies restrict the use of confidential or private data in a non-production or test environment.
f. Pendo's policies enforce user responsibility for securely encrypting data in any rare and exceptional circumstances where it may be necessary to write confidential data on removable USB drives.

Asset management:

a. All applications, databases, software, systems, and services that contain Customer data or are production-critical to providing services are inventoried and assigned a management-level Business Owner. The Business Owner is required to authorize system changes and approve user access.

Physical access management:

a. Access to Pendo's office location is monitored by a receptionist during business hours. Doors are locked outside business hours and when a receptionist is not present.
b. Visitors to Pendo's office location are required to sign in and are provided a temporary identification badge.
c. Physical keys and card access to areas where critical equipment is located is restricted to authorized individuals. Pendo management reviews holders of keys and access cards annually.

Performance management, data processing integrity, backups, and disposal:

a. Pendo utilizes tools that measure processing queues to verify the timeliness of processing incoming data while monitoring real-time results.
b. Data lost during processing is detected, and automatically creates an alert to the Engineering team. Alerts are addressed by the Engineering team
c. Upon occurrence of processing errors within Pendo's application, the change management process is followed with a change ticket initiated and the error investigated and resolved.
d. Pendo periodically performs a secure disposal of Customer data that is older than its default retention period, or outside of alternative retention periods specified by Customers. The disposal process also supports removal of personal information related to individual data subjects.