AIHR Information Security Statement

Owner: VP of Business Operations

Version 3.0

Last updated; 23 October 2026

1 Purpose and scope

This statement describes AIHR's approach to protecting information supporting its learning platform and related client services. Client Data means information processed by AIHR on behalf of a client in delivering those services. Member means an individual authorised to use the platform. This statement is to be read alongside the applicable service agreement, Data Processing Agreement (DPA) and Member Terms. Any conflict must be resolved under the applicable contractual order of precedence.

2 Information security management

AIHR maintains a risk-based Information Security Management System (ISMS) aligned with ISO/IEC 27001:2022. Security objectives, risk assessments, internal audits and management reviews support continual improvement. AIHR seeks to keep its risk assessments and security controls up to date, taking account of changes in its services, operating environment and relevant threats.

3 Governance and responsibilities

Management is accountable for information security and the resources needed to support it. The Information Security Officer (ISO) coordinates ISMS maintenance and improvement. Designated business and system owners implement and operate controls within their areas of responsibility.

4 Personnel security and awareness

Employees and contractors with access to confidential information are subject to appropriate confidentiality obligations, including after their engagement ends. AIHR promotes security and privacy awareness through onboarding, training and guidance suited to individuals' roles and relevant threats. Awareness materials are kept up to date as needs evolve.

5 Member responsibilities

Members must protect their accounts, keep authentication credentials confidential, comply with the applicable Member Terms and promptly report suspected account misuse or security incidents through AIHR's designated support channel. Clients are responsible for their own user administration where this is within their control.

6 Identity and access management

Access is approved according to business need and the principle of least privilege. Access management takes account of role changes and departure, with the aim of keeping access rights appropriate. Privileged access receives additional protection. Authentication measures, including multi-factor authentication where appropriate, are selected according to system capabilities and risk. Password protection follows applicable internal security standards.

7 Data protection and encryption

AIHR applies encryption to Client Data and Member personal data in transit over public networks. Cryptographic measures and key access are managed in line with the sensitivity of the information and relevant security requirements. Personal data processing, retention and deletion are governed by applicable agreements, privacy information and retention requirements. Removal from backups follows the documented backup lifecycle.

Security operations and assurance

8 Logging and monitoring

Relevant authentication, privileged access, access changes and security events are logged for systems supporting the services. Logging and monitoring arrangements are designed to support incident detection and investigation, with protection and retention appropriate to the systems, risks and applicable requirements.

9 Backup and recovery

Backup and recovery arrangements support restoration of critical services and data following disruption. Recovery arrangements are maintained with regard to service needs and relevant risks, with validation and testing as appropriate. Backups are intended for operational recovery; direct client access and restoration of individual deleted records are subject to supported technical capabilities and agreed service terms. No individual-record recovery guarantee is implied.

10 Vulnerability and malware management

AIHR uses preventive, detective and recovery measures to reduce malware risk. Vulnerability management takes account of relevant alerts and identified weaknesses. The approach to remediation reflects severity, exposure and business impact.

11 Secure development and change management

AIHR takes security into account in development and change processes, using review, testing and management of software dependencies as appropriate to the nature and risk of the change. Development, testing and production access are separated as appropriate. Synthetic or appropriately anonymised data is used for testing; use of confidential or personal data requires explicit approval, an appropriate legal basis where required, and safeguards consistent with its sensitivity.

12 Supplier security

Suppliers that process Client Data or materially support service delivery are assessed according to their risk and criticality. Relevant security, confidentiality and data protection requirements are included in agreements. AIHR seeks to keep supplier assurance information up to date, taking account of supplier risk, material changes and relevant arrangements for service termination and data return or deletion.

13 Incident response and notification

Where AIHR acts as a processor, it notifies the affected client without undue delay after becoming aware of a personal data breach involving personal data processed on that client's behalf, in accordance with applicable law and the Data Processing Agreement (DPA). Notification of other relevant security incidents follows the applicable client agreement. AIHR shares available information to support the client's response, with further information provided as appropriate.

14 Business continuity

AIHR maintains continuity and recovery arrangements for critical services, taking account of key supplier dependencies. AIHR seeks to keep these arrangements appropriate to its services, dependencies and relevant risks, supported by review and exercises where appropriate. Any contractual availability commitments or recovery targets are set out in the applicable service agreement.

15 Responsible use of artificial intelligence

AIHR takes a risk-based approach to the use of AI in service delivery and supporting business processes. Tool selection and use take account of confidentiality, privacy and information accuracy. Human oversight is applied according to the sensitivity and impact of the use,

including security assurances, client registrations and material business decisions. Applicable restrictions on the use of confidential information and personal data remain in force.

16 Assurance and review

Information about AIHR's certification status, scope and validity is available on request. Supporting assurance information, including relevant Statement of Applicability information, is shared subject to confidentiality and appropriate disclosure controls. AIHR keeps this statement up to date to reflect relevant changes in its services, security approach and applicable requirements. Questions and incident reports can be raised through AIHR's designated client support or security contact.