AIHR Information Security Statement

Owner: VP of Business Operations

Version 2.0

Last updated: 11 November 2024

1. **ISMS Implementation.** Information is a valuable asset that must be protected from unauthorized disclosure, modification, use, or destruction. Prudent steps must be taken to ensure that its confidentiality, integrity, and availability are not compromised. For this purpose, AIHR has implemented an Information Security Management System (ISMS) in accordance with the international standard ISO/IEC 27001. To drive continuous improvement, security goals are formulated, and AIHR has implemented a framework including procedures for internal auditing, third-party auditing, operational risk management, risk analysis, and management review to ensure the efficiency and effectiveness of the ISMS.

2. **Member Responsibility.** AIHR and the Client acknowledge that Member responsibility is critical to maintaining information security. AIHR provides Members with the necessary resources to perform their duties effectively in a secure electronic environment. Members must agree to the Member Terms when accessing their Account for the first time.

3. **Confidentiality.** Digital security obligations are explicitly incorporated into the AIHR employment contract. Employees shall maintain the confidentiality of information during their employment and after the termination of their employment.

4. **Security Roles.** AIHR ensures that appropriate responsibilities and authorities for security roles are clearly defined, assigned, and communicated within its organization to effectively govern, maintain, and continually improve the ISMS.

5. **Certification Reports.** Upon request, AIHR shall provide the Client with verifiable reports of its current certifications, including but not limited to its ISO 27001 certificate and statement of applicability.

6. **Awareness Training.** AIHR shall establish and maintain a security and privacy awareness program that provides training and education to all personnel. Training shall be conducted at the time of hire and, subsequently, at least annually throughout employment.

7. **Access Control.** AIHR employs processes to provision identities and access privileges based on the principle of least privilege. These processes include recurring reviews at appropriate intervals and the use of industry-standard authorization and authentication mechanisms. Password management shall comply with industry standards regarding complexity, lifecycle management, and protection. AIHR uses industry-standard encryption to secure Member personal data and Client data in transit over public networks and at rest.

8. **Event Logging.** AIHR shall maintain event logs recording user activities, exceptions, faults, and information security events. Modifications to access rights and successful or unsuccessful log-in attempts shall be logged. Logs shall be protected against unauthorized access, modification, deletion, or interruption and shall be regularly monitored.

9. **Backup Limitation.** AIHR has implemented backup procedures. However, Clients shall not be entitled to access these backups and cannot retrieve any data provided by Members or other data if a Member has accidentally removed such data.

10. **Vulnerability Management.** AIHR maintains a vulnerability management process to ensure the continuous and timely identification, analysis, and remediation of vulnerabilities. Controls for the detection, prevention, and recovery from malware are deployed to safeguard against all known types of malicious software.

11. **Secure Development.** AIHR employs secure development environments that span the entire system development lifecycle for system development and integration. Security functionality is tested during development, and Confidential Information shall not be used for testing purposes.

12. **Vendor Risk Management.** AIHR shall maintain a vendor risk management program to assess vendors that access, store, process, transmit, or otherwise impact the security or privacy of Client Data. Assessments shall evaluate vendors' security and privacy controls during the due diligence process and at regular intervals throughout the vendor relationship lifecycle.

13. **Incident Notification.** In the event of a significant IT Security Incident (*an event compromising the availability, integrity, or confidentiality of information, which has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned, or has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage*), AIHR shall notify the Client without undue delay. Notification shall be sent via email in English to the general contact person and include information available to AIHR regarding the IT Security Incident, including, to the best of AIHR's knowledge, (i) which systems, processes, or data are affected; (ii) the country where the IT Security Incident was noted and observed, along with contact information for the appropriate AIHR representative; and (iii) any measures or remedies that the Client may take in response to the threat.