PathwAI

HR Security Policy

Version 1 - Approved by Abdullah Adeeb

Contents

1. Objective

The objective of this policy is to establish a structured approach to managing information security requirements associated with human resources throughout recruitment, employment, changes in employment status, and termination. PathwAI Labs shall ensure that employees (both full-time and part-time) and external parties, including contractors and third-party staff, understand their roles and responsibilities concerning information security and comply with these requirements. Furthermore, PathwAI Labs shall safeguard the company's interests during employment transitions or termination.

2. Scope

This policy is applicable to all employees (full-time and part-time) and external parties, including contractors and third-party staff (such as housekeeping staff and security personnel), who have access to PathwAI Labs information systems.

3. Policy Statement

PathwAI Labs shall ensure that all employees (full-time and part-time) and external parties, including contractors and other third-party staff, are aware of and adhere to their responsibilities concerning information security. Additionally, PathwAI Labs will safeguard its interests during changes in employment or termination.

4. Human Resource Security Guidelines

4.1 Before Employment

- The competence of all job candidates shall be evaluated as part of the hiring process to ensure they meet job role expectations.
- Upon employment, PathwAI Labs employees and contractors shall sign employment terms and conditions that outline their information security responsibilities and related obligations, both during and post-employment.
- Background verification checks shall be conducted on prospective employees, where feasible:
    - The extent of these checks shall align with business needs, the classification of accessible information, and potential risks. This may include employment history verification, academic and professional qualification checks, identity validation, and criminal background checks for prospective PathwAI Labs employees.
    - In jurisdictions where background checks are restricted by law, reference checks may be performed based on the access level of the position.
    - Privacy and data protection laws, along with employment regulations, shall be observed. Contract partners will be assessed for their information security practices as part of Vendor Risk assessment. For additional details, refer to the Vendor Management Policy.

4.2 During Employment

- Information Security roles and responsibilities shall be clearly defined and documented for all applicable employees (full-time and part-time), contractors, and third-party staff.
- Relevant employees, contractors, and third-party staff shall receive training on organizational policies and procedures, including security requirements, legal obligations, and control measures, such as acceptable use of PathwAI Labs systems and the Code of Business Conduct.
- Awareness training on organizational policies shall be conducted upon onboarding and at least annually thereafter.
- Formal information security training shall be conducted during onboarding and at least once a year thereafter.
- The training materials and organizational policies shall be accessible to all employees via a public portal.
- The Information Security Officer is responsible for ensuring the implementation and compliance with information security controls by all employees.

4.3 Termination or Change in Employment

- On termination, employees shall return/hand over all organizational assets under their responsibility.
- Access rights and privileges to critical systems granted to employees or contractors shall be revoked in line with the access control policy.
- For changes in employment status, access rights and privileges to critical systems shall be reviewed and adjusted as needed.

5. Document Security Classification

Internal Use (please refer to the Data Classification policy for more details).

6. Non-Compliance

Verification of compliance with this policy shall include but is not limited to automated reporting, audits, and policy owner feedback. Any violation may result in disciplinary action, up to and including termination of employment or contractual agreements. The level of disciplinary action will reflect the severity, intent, and impact of the breach.

7. Responsibilities

The Information Security Officer is tasked with the approval and review of the policy and associated procedures. Supporting teams and staff members are responsible for implementing relevant sections of the policy within their scope of work.

8. Schedule

This policy shall undergo review annually and whenever significant organizational changes arise.

End of HR Security Policy. For version history, please see the next page.

Version History

	Version	Log	Date
1	Current	Policy version approved by Abdullah Adeeb	02 Dec, 2025
1		New policy version created	02 Dec, 2025