TalentAxisPro Private Limited HR Security Policy

1. Overview

TalentAxisPro Private Limited has enforced an HR Security Policy since April 2024 to safeguard our talent pipeline, contractor ecosystem, and employee-related data while aligning with our Information Security Policy. This document outlines the protocols to protect sensitive personnel-related information, govern secure onboarding/offboarding, and uphold compliance across employment models.

2. Purpose

The HR Security Policy ensures secure management of human resources, including full-time employees, freelance evaluators, and third-party collaborators, particularly those with access to:

- Candidate assessments and reports
- Assessment videos and scoring tools
- Client-sensitive information
- Internal platforms and workflows

It supports risk mitigation, data confidentiality, ethical workforce conduct, and compliance with labor and data protection laws (e.g., GDPR, IT Act).

3. Scope

Applies to all:

- Full-time and part-time employees
- Contractual language assessors and AI trainers
- Interns, vendors, and freelancers onboarded for platform tasks
- HR, Admin, and IT personnel with access to people/process data

4. Data Covered Under HR Security

Data Type	Examples	Classification
Personal Information	Name, contact, bank details, ID proofs	Confidential
Work Assignments	Project briefs, candidate evaluation data, video access	Confidential
Employment Contracts	Offer letters, SoWs, NDAs, freelance agreements	Internal
Performance & Access Logs	Evaluation quality checks, user activity on platform	Internal

5. Acceptable Use & Code of Conduct

- TalentAxisPro Private Limited-issued platforms and credentials may only be used for assigned work.
- Sharing of credentials, candidate data, or scoring frameworks is strictly prohibited.
- Individuals must report any policy violations or suspicious activity within 24 hours.
- Any unauthorized data retention or reproduction is considered a **major security breach**

7. Training & Compliance

- **Security Orientation** is mandatory for all new personnel.
- Annual refresher training covers:
    - GDPR basics
    - Assessment confidentiality
    - Secure communication and data handling

8. Policy Violations & Disciplinary Action

Type of Violation	**Example**	**Consequence**
Minor Breach	Delay in data deletion confirmation	Warning + re-training
Moderate Breach	Accidental data sharing with unapproved users	Temporary access suspension
Severe Breach	Intentional sharing/download of candidate data	Contract termination + legal escalation