

TalentAxisPro Private Limited Information Security Policy

1. Overview

TalentAxisPro Private Limited has maintained a structured Information Security Policy since Q2 2024, reflecting our responsibility to protect sensitive digital assets entrusted to us by clients, candidates, and internal stakeholders. This policy outlines the measures we’ve implemented to secure:

- Candidate data
- Assessment videos and reports
- Client-provided information
- Contractual and operational documents
- Proprietary assessment and process frameworks

2. Purpose

The policy ensures that TalentAxisPro Private Limited’s information—especially identity-sensitive and proprietary material—is protected from loss, unauthorized access, misuse, and disclosure. It supports compliance with industry and regulatory expectations, including GDPR and IT Act guidelines.

3. Scope

Applies to:

- All TalentAxisPro Private Limited employees, freelance evaluators, AI trainers, contractors, and platform contributors
- All cloud services, endpoints, assessment tools, and internal documentation platforms (e.g., Drive, Notion, Jira, AWS, GitHub)
- All data classified as confidential, internal, or restricted under TalentAxisPro Private Limited's governance standards

4. Data Categories Managed by TalentAxisPro Private Limited

DATA TYPE	DESCRIPTION	CLASSIFICATION
CANDIDATE DATA	Names, contact details, performance reports, assessment videos	Confidential
ASSESSMENT REPORTS	AI + human-generated reports and scores	Confidential
ASSESSMENT VIDEOS	Recorded video/audio responses of candidates	Confidential

CONTRACTS	NDAs, SoWs, client and vendor agreements	Internal
CLIENT INFORMATION	Point of contact, hiring requirements, communication records	Confidential
PROCESS DOCUMENTS	Test templates, rubrics, evaluation workflows	Internal

5. Access Management

- All sensitive data is stored in access-controlled environments (Google Workspace, AWS S3, Notion Enterprise, etc.)
- Access is **role-based** and provisioned on a **need-to-know** basis
- Access audits are conducted **monthly** and adjusted immediately when roles change or contracts end
- MFA (multi-factor authentication) is enforced for all privileged accounts

6. Data Security Measures

- **Video Storage:** Assessment videos are stored in encrypted cloud environments with expiring access links
- **Contract Safeguards:** All external evaluators and data handlers are bound by NDAs and secure platform guidelines

7. Platform & Process Security

- All assessments are hosted in secure, GDPR-compliant environments
- Candidate responses are anonymized before use in model training
- Source documents and scoring rubrics are shared via secure, time-restricted channels
- TalentAxisPro Private Limited's proprietary evaluation framework is monitored for unauthorized access or sharing

8. Incident Response

- All users are required to report suspected breaches within 2 hours of identification
- Incidents are logged, triaged, and addressed within 2 hours depending on severity
- Any client-related data breach is disclosed within **2 hours**, with a root cause and mitigation report

9. Training & Awareness

- All employees and freelancers complete security onboarding training
- Annual refresher training includes secure handling of candidate data and process documents
- Contractors are given task-specific data handling guidelines prior to platform access

10. Compliance & Review

- TalentAxisPro Private Limited aligns with GDPR, IT Act, and ISO/IEC 27001 principles
- All freelance evaluators and AI contributors must sign the SOW Contract that outlines confidentiality and proprietary standards.
- Policy reviews occur annually or upon any material change in data handling, platform upgrades, or legal guidance

11. Policy Enforcement

Non-compliance may result in:

- Suspension or termination of access privileges
- Contract cancellation (in case of third parties)
- Disciplinary action as per TalentAxisPro Private Limited's internal code of conduct