VerbiQ

Access Revocation Policy

TalentAxisPro Private Ltd
16A, 2nd Floor, Cityvista Downtown, Kharadi, Pune – 411014

1. Purpose

The purpose of this policy is to define the process for revoking access to Talent AxisPro Private Ltd's internal systems, tools, and client platforms when an employee, contractor, or third-party associate exits the organization or no longer requires access due to role changes or project completion. This is critical to ensuring data security, client confidentiality, and compliance with global standards.

2. Scope

This policy applies to:
- All full-time and part-time employees
- Contractual staff, freelancers, and interns
- Any third-party vendors or consultants with system access

3. Policy Statement

Talent AxisPro mandates that all access credentials—both internal and client-related—must be revoked within 24 hours of the individual's disassociation from the company or their reassignment to a non-relevant role.

Failure to comply may result in a security breach and impact our relationship with clients and regulatory bodies.

4. Types of Access Covered

The policy applies to access rights across:
- Company email accounts (e.g., Gmail, Outlook)
- Cloud storage (e.g., Google Drive, Dropbox, OneDrive)
- Project management tools (e.g., Trello, Notion, Asana, Jira)
- Communication platforms (e.g., Slack, Microsoft Teams, WhatsApp Groups)
- Client platforms (e.g., LMS, CRM, proprietary portals)
- Internal HR/finance/admin systems
- Physical access (office entry cards, biometric access)

5. Roles & Responsibilities

Role	Responsibility
Reporting Manager	Inform HR/Admin of any exit, termination, or role change
HR Department	Initiate the revocation process; maintain records

IT/Admin Team	Revoke access to systems, collect and store proof of revocation
Employee/Associate	Return all physical access tools and confirm disconnection from work systems

6. Access Revocation Procedure

• Trigger Event: Employee exit (voluntary/involuntary), Project completion, Internal transfer/role change

• Notification: Reporting Manager notifies HR and Admin team immediately via email

• Access Review and Form Completion: HR fills out an Access Revocation Checklist, listing all access points

• Execution: IT/Admin revokes access across systems within 24 hours

• Proof of Action: Screenshots or logs are saved in a centralized folder

• Tracker Update: HR logs revocation date, time, responsible team member, and confirmation of completion

7. Record Retention

All revocation records must be stored securely for at least 2 years and be made available for audit purposes upon request by clients or regulatory authorities.

8. Exceptions

Any exception to this policy must be approved by the HR Head and IT Admin in writing and recorded with justification.

9. Review and Updates

This policy will be reviewed annually by the HR and IT teams and updated based on changes in legal, regulatory, or client requirements.

Signatures

Sheetal Ramkumar
CEO & Founder

Ramkumar Kayarat
CHRO & Founder