6. Screening Policy Details

6.1 Pre-Employment Screening

Before employment or engagement, the following checks must be conducted:

- **Identity verification** (government-issued ID, PAN, Aadhaar).
- **Employment and education verification** based on role sensitivity.
- **Reference checks** from previous employers.
- **Criminal background verification** for positions handling sensitive data or financial access.
- **NDA and confidentiality agreement** signed prior to onboarding.

No employee shall be provided access to information assets until screening and documentation are completed and verified by HR and the Information Security team.

6.2 Onboarding and Access Control

Upon completion of screening:

- HR shall notify IT and Security teams of the employee's joining details.
- Access to systems, applications, and data shall be granted strictly on a **role-based access control (RBAC)** principle.
- Temporary or contractor accounts must have defined validity periods.
- Employees shall be trained on:
    - Security awareness and acceptable use policies
    - Data handling procedures
    - Incident reporting mechanisms
- Employees must acknowledge the **Code of Conduct**, **Information Security Policy**, and **Acceptable Use Policy**.

6.3 During Employment (Monitoring and Control)

- Access rights must be **periodically reviewed** (at least quarterly or upon role change).
- HR and IT shall collaborate to update access privileges during:
    - Promotion, transfer, or departmental changes
    - Role modification or project reassignment
- All employees must undergo **annual security awareness training**.
- Any violation of information security policy will result in disciplinary action.

6.4 Off boarding and Access Revocation

When an employee resigns, is terminated, or completes a contract:

- HR must notify IT, Admin, and Security immediately.
- Access to all systems, applications, VPNs, and facilities must be **revoked on or before the last working day**.
- All company assets (laptops, mobile devices, access cards, SIMs, etc.) must be returned.
- Email forwarding or data transfer must be approved by the reporting manager.
- HR must ensure completion of:
    - Exit interview
    - Final settlement
    - Return of confidential materials
    - Deactivation confirmation from IT

Post-exit, the employee's data access must remain revoked and archived per retention policy.

6.5 Post-Employment Obligations

- The confidentiality agreement signed during onboarding remains enforceable after separation.
- Ex-employees must not disclose, share, or retain any company data, credentials, or intellectual property.
- Legal action may be taken for breach of confidentiality.