elevaite365

TECH THAT MATTERS

Elevaite365

HR Security Policy

Version 1.0

PURPOSE

The Human Resource Security Policy aims to ensure that all Elevaite365 (hereby referred to as organization) employees, contractors, and third parties are qualified, informed, and well-equipped to perform their duties responsibly. It also ensures that access rights to the organization's assets and data are removed or adjusted upon termination or role changes, reducing the risk of unauthorized access or misuse of information.

SCOPE

The policies outlined herein apply to all resources at all sensitivity levels, including full-time, part-time, and temporary staff employed by, working for, or on behalf of the organization; contractors and consultants engaged with or working on behalf of the organization; and any individuals or groups who have been granted access to organization's IT systems and information.

DEFINITIONS

1. Confidentiality: The principle of safeguarding sensitive information from unauthorized access, use, or disclosure, ensuring that personal, financial, and organizational data is protected by company policies and legal requirements.

2. Employee Access Control: A system of policies and procedures designed to regulate and monitor employee access to sensitive information, systems, and physical spaces within the organization, ensuring that individuals can only access what is necessary for their job function.

3. Incident Response: The structured approach to addressing and managing security breaches or threats, including steps to detect, respond to, and recover from security incidents that may impact HR systems, employee data, or overall organizational security.

4. Background Checks: Reviewing an individual's criminal, financial, and employment history before hiring or promoting within an organization to ensure a secure and trustworthy workforce.

RESPONSIBILITY

HR Head

1. Primary responsibility for implementing this policy.

2. Coordinates with the ISG (Information Security Group) and department heads to ensure consistency and compliance.

Department Heads

Provide oversight for their teams, ensure job descriptions include any necessary security responsibilities, and work with HR to enforce policy requirements.

ISG (Information Security Group)

Guides policy content, assists with security training and ensures alignment with broader information security objectives.

POLICY

Job Descriptions - Roles and responsibilities

1. Documentation: Each role within the organization must have a job description clearly stating roles, responsibilities, and security-specific duties.

2. Security-Related Tasks: Where relevant, job descriptions must explicitly mention responsibilities for implementing or maintaining organizational security.

Background Checks

1. Purpose: To validate the credentials and reliability of new hires, contractors, or third-party personnel who will have access to organizational resources.

2. Timing: Background verification typically occurs before joining or within 30 working days from the date of joining.

3. Scope of Checks (based on client/organizational mandates):

Character references

Verification of academic qualifications

Relieving letter from previous employer (as applicable)

Identity checks (e.g., passport, driver's license, bank account proof)

Criminal background checks (where permissible by law)

4. Third Parties: Depending on business or client requirements, similar checks apply to contractors and consultants.

5. Signing Offer: All offered candidates must sign the offer of appointment. The letter must outline security responsibilities for both the organization and the employee.

Management Responsibilities

1. Supervisor/Manager Awareness: Supervisors should remain alert to any changes in an employee's circumstances or behavior that could indicate a potential security risk.

2. Monitoring Conduct: Line managers are expected to observe staff performance and attitude and intervene early if they detect signs of stress, conflict, or other factors that may lead to security incidents.

Confidentiality Agreements

1. Employees: All employees must sign a confidentiality or non-disclosure agreement (NDA) as part of their employment terms.

2. Third Parties: Contractors, consultants, or other third parties must also sign NDAs that align with client or organizational mandates.

3. Role Changes: When an employee is promoted or transferred, the confidentiality agreement may be re-reviewed to reflect updated responsibilities or access levels.

Information Security and Data Protection Training and Awareness

1. Mandatory Training: All employees, contractors, and third parties must undergo information security and data protection awareness sessions.

2. New Hires: Orientation includes introducing security policies, guidelines, and best practices.

3. Periodic Updates: Regular reminders (via login popups, emails, posters) to keep security top-of-mind.

4. Records: Attendance and completion records of such programs are maintained by HR and/or ISG.

Disciplinary Process

1. Policy Violation: Any employee, contractor, or third-party user who violates organizational security policies and procedures may face disciplinary action.

2. Fair Treatment: Ensures correct and equitable handling of suspected breaches, consistent with the Disciplinary Policy.

3. Escalation: Depending on severity, actions may include written warnings, final warnings, or termination of employment/contract.

Employees, Contractors, and Third-Party Termination of Employment

1. Orderly Exit: Termination must follow the organization's standard separation policy or the contractual terms.

2. Role Changes/Transfers: When a user is transferred or assigned a new responsibility, user access is reassessed to ensure it aligns with the new duties and doesn't compromise security.

Return of Assets

1. Organization Property: Upon termination (or at the end of the contract), employees and third parties must return all organizational assets (e.g., laptops, access cards, tokens, documents).

2. Verification: Department heads or HR confirm the return of assets before processing final clearances.

Removal of Access Rights

1. Timely Removal: HR, IT, and relevant department heads coordinate to remove or adjust system access upon an individual's departure or role change.

2. Documentation: Ensure all relevant directories, systems, and applications (e.g., email, VPN, cloud platforms) are updated to revoke access.

Non-Compliance

1. Breach Consequences: If a breach or policy violation occurs, management will initiate corrective measures, which may include:

1.1 Restricting user access to systems or services.

1.2 Initiating disciplinary action (up to and including termination).

1.3 Terminating contracts or agreements with contractors or third parties, if applicable.

2. Legal Action: Where warranted by severity or legal requirements, the organization may pursue legal recourse against the violators.

Version Details

Version	Version Date	Description of changes	Created By	Approved By	Published By
Version 1.0	-	Initial Release	Borhan	-	-