Human Resources Security Policy and Procedures

This policy defines the organization's Human Resources (HR) procedures related to managing personnel security throughout the employment lifecycle, ensuring alignment with security and operational objectives.

1. Governance and Review

1.1. Senior Management Approval

This Human Resources Security Policy, along with all associated procedures for recruiting, evaluating, counseling, and promoting personnel, is **formally approved by senior management** to ensure organizational support and mandatory compliance.

1.2. Annual Review

The entire Human Resources Security Policy document and its supporting processes are **reviewed on at least an annual basis** by HR, Legal, and the Security departments. This review ensures the policies remain current with relevant labor laws, industry standards, and the organization's security requirements.

2. Hiring, Evaluation, and Development Procedures

The HR policies include evaluating, counseling, and promoting actions, integrating security considerations into each stage of the employment lifecycle.

2.1. Recruitment and Hiring (Vetting)

1. **Security Screening:** Background checks appropriate to the role's security classification (e.g., access to sensitive data, administrative privileges) are conducted on all candidates prior to a final job offer. This includes verification of identity, employment history, and criminal records as permitted by law.
2. **Role Definition:** All job descriptions must explicitly state the security responsibilities, acceptable use requirements, and required technical proficiencies.

2.2. Performance Evaluation (Evaluating Actions)

1. **Security Compliance:** Annual and periodic performance reviews include a mandatory assessment of the employee's adherence to all security policies (e.g., password management, clean desk policy, incident reporting). Non-compliance is documented as a performance deficiency.
2. **Access Review Trigger:** Significant changes in job function or poor performance that results in a change of access or termination are immediately communicated to IT and Security to trigger a review or revocation of system access privileges.

2.3. Corrective Action (Counseling Actions)

1. **Disciplinary Process:** A structured disciplinary procedure is maintained to address policy violations, security breaches, or performance deficiencies. This process includes **counseling actions** such as verbal warnings, written warnings, suspension, and termination, depending on the severity and recurrence of the infraction.
2. **Security Violations:** Any severe security violation (e.g., intentional data disclosure, misuse of privileged access) is grounds for immediate counseling and may lead to termination. HR and Legal are involved in all disciplinary actions to ensure fair process and legal compliance.

2.4. Career Advancement (Promoting Actions)

1. **Security Clearance for Promotion:** Personnel being considered for **promoting actions** (e.g., promotions, transfers to roles with increased access or responsibility) must undergo a renewed security screening and mandatory review of their previous security compliance record before the promotion is finalized.
2. **Training Prerequisite:** Acceptance of a new role requiring elevated privileges (e.g., moving to an administrator role) requires the successful completion of mandatory, role-specific security training before the new access rights are granted.