**Security Architecture Design**

**Objective:**

Design a defense-in-depth security framework that protects sensitive HR data, ensures authorized access only, and supports compliance with international privacy and data protection regulations (e.g., GDPR, UN Data Protection Policies).

**Core Layers:**

**A. Data Protection:**

* **Encryption at Rest**: AES-256 on databases and file systems (e.g., HR attachments like contracts).
* **Encryption in Transit**: TLS 1.3 over HTTPS + SSL pinning in mobile apps.

**B. Authentication:**

* Email + Password with strong password policy (min length, expiry, lockouts).
* **MFA**: SMS/Authenticator App-based MFA for all HR/Admin users.
* **OAuth 2.0 / OpenID Connect**: For integration with donor or UN SSO identity providers.

**C. Authorization (RBAC):**

* Fine-grained role matrix controlling:
  + Module access (e.g., only HR can approve leave).
  + Field-level access (e.g., payroll visibility restricted).
  + Action-level access (e.g., only Line Managers can rate performance).
* Admin dashboard to assign and revoke roles securely.

**D. Monitoring & Logging:**

* **Audit Logs**:
  + Downloadable reports of user activity (login, changes, approvals).
  + Immutable logs stored in WORM (Write Once, Read Many) format.
* **Threat Detection**:
  + IP blacklisting and geo-fencing.
  + Alerts for login anomalies or multiple failed attempts.

Integration with SIEM (Security Information and Event Management) tools like Splunk/Graylog