**Security Monitoring & Compliance Audit Logs**

**Objective:** To uphold data integrity, ensure regulatory compliance, and provide ongoing protection against cyber threats.

**Detailed Components:**

* **24/7 Security Event Monitoring**
  + Cloud-based SIEM (Security Information and Event Management) system
  + Alert thresholds for suspicious logins, mass data exports, unauthorized access
* **Access Control and Audit Trail Logs**
  + Role-based login histories with timestamps and session durations
  + Data editing logs showing who changed what, when, and why
* **Penetration Testing Reports**
  + Quarterly ethical hacking summaries
  + Lists of vulnerabilities found, prioritized mitigation steps taken
* **Encryption Protocols Assessment**
  + Confirmation of AES-256 encryption for stored data
  + HTTPS and SSL/TLS for all data in transit
* **Compliance Documentation**
  + Adherence reports for GDPR, African Union Data Policy, and UNDP digital guidelines
  + Data Subject Rights: consent tracking, deletion requests
* **Security Breach Response Plan**
  + Incident Response SOP with contacts, communication plan, and resolution workflows
* **Automated Compliance Audit Tools**
  + Regular scans for misconfigurations or expired certificates
  + Reports generated monthly and shared with governance boards