Data Archival Policy for In-House Developed Software at PSeGS and DGRPG

Department of Governance Reforms & Public Grievances (DGRPG) and its implementation agency i.e. Punjab State e Governance Society (PSeGS) being the IT organization of State of Punjab are handling many software projects like eSewa, mSewa, Admission Portal, Comprehensive Agriculture Portal etc. Considering that the size of production data increases in very large numbers, so it is difficult to manage and handle data in the live environment, it also affects the performance of portals, so proper archival mechanisms are to be implemented to avoid these problems. This policy serves as a guideline for the systematic archival of data in PSeGS and DGRPG. Adhering to this policy will help ensure that data is managed effectively, securely, and in compliance with legal and regulatory requirements.

1. Purpose

This policy outlines the guidelines and procedures for the archival of data generated by in house developed software(s) at Punjab State e-Governance Society (PSeGS) and Department of Governance Reforms and Public Grievances (DGRPG). The aim is to ensure data integrity, security, and availability for future reference, compliance, and decision making.

2. Scope

This policy applies to all data generated, processed, and stored by in-house developed software(s) at PSeGS and DGRPG. It includes, but is not limited to, user data, transaction logs, audit trails, and system backups.

3. Definitions

- **Archival Data:** Data that is no longer actively used but must be retained for long term storage for legal, regulatory, or historical purposes.
- **Active Data**: Data that is frequently accessed and used for day-to-day operations.
- **Retention Period:** The duration for which data must be retained before it can be archived or disposed of.

4. Responsibilities

- **Software Cell:** Responsible for implementing and managing the data archival process, ensuring compliance with this policy, and maintaining archival infrastructure.
- **Data Owners:** Responsible for determining the retention period of data and ensuring that data is archived in accordance with this policy.

- **Compliance Officer:** Ensures that data archival practices comply with relevant legal and regulatory requirements.

5. **Data Retention and Archival Criteria**
    - **Retention Period:** Data should be retained based on its classification:
        - **Services Data:** The services data including supporting documents of all in house applications/software(s) on which no action has been taken within last 45 days and is at approved/rejected state shall be archived.
        - **Reporting Data:** 1 or 2 Years
        - **Audit Logs:** 2 years
    - **Archival Trigger:** Data that has exceeded its retention period should be identified and archived.
6. **Archival Process**
    - **Identification:** Data that has reached the end of its retention period should be identified automatically or manually.
    - **Migration:** Identified data should be migrated to a secure archival storage system.
    - **Verification:** The data integrity shall be ensured by verifying checksums or hashes before and after migration.
    - **Indexing:** Archived data should be indexed to facilitate easy retrieval.
    - **Access Control:** Access to archived data should be restricted to authorized personnel only. The District GR branches or PSeGS/DGRPG HQ teams may be provided user IDs to access and retrieve the archived data either in the concerned portal itself or in a secure format. Such an access should have search functionality for easy searching of data as per requirement.
    - **Monitoring:** Regularly monitor the archival system to ensure data integrity and accessibility.
7. **Data Retrieval & Re-Archival**
    - **Request Process:** Authorized personnel can request access to archived data through a formal request process. All data archival requests from District GR Branches or PSeGS/DGRPG HQ teams shall be submitted through effice.
    - **Approval:** All requests for archived data must be redirected through the data owner or Project Manager of concerned portal/software/department/project.

- **Restoration:** Once request for restoration is received, data should be restored from the archival storage to an active system or provided in a secure format within 12 hours by the Software team.
- **Re-Archival:** If the data is restored in the portal/application/software it self, then it shall be archived again as per timelines in the Data retention and archival criteria

8. Security Measures

- **Encryption**: All archived data should be encrypted during storage and transmission.
- **Access Controls:** Implement role-based access controls to ensure that only authorized personnel can access archived data.
- **Regular Audits:** Regular audits should be conducted to ensure compliance with the archival policy and security measures.

9. Compliance and Legal Requirements

- The archival process should be in line with the Data retention guidelines of the Govt. of Punjab.
- Proper documentation of the archival process and retention schedules shall be maintained by Software team for audit and compliance purposes.

10. Review and Updates

- This policy should be reviewed annually or as needed to ensure it remains relevant and compliant with changing legal and regulatory requirements.
- Updates to the policy should be communicated to all stakeholders and personnel involved in the data archival process.