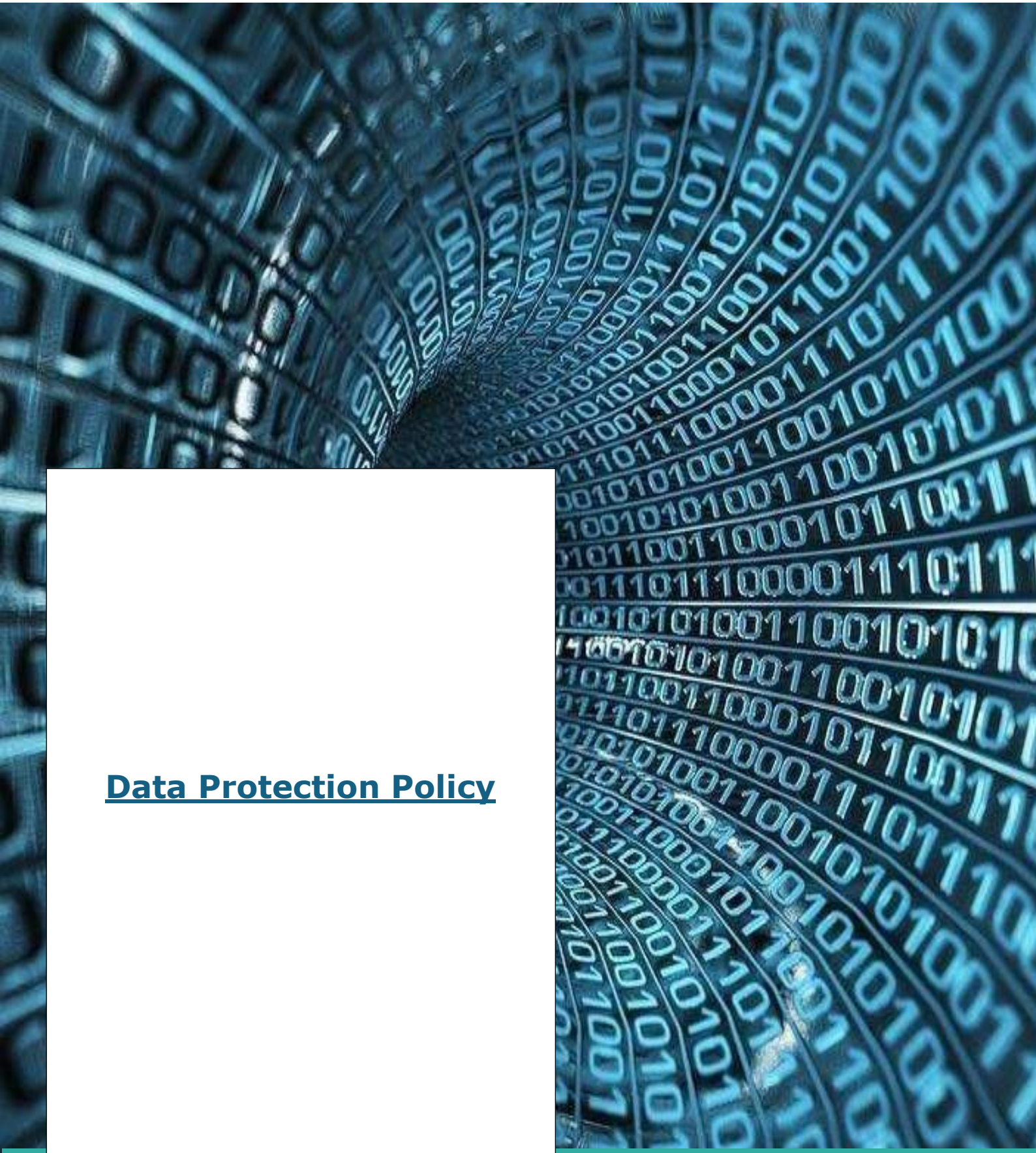

# Data Protection Policy

**Public Financial Management System (PFMS)**

**O/o Controller General of Accounts**

# Public Financial Management System

## Data Protection Policy

This Data Protection Policy defines the principles and controls governing the collection, processing, storage, and protection of data within the Public Financial Management System hereinafter referred as PFMS. It is established to ensure confidentiality, integrity, and availability of data, and to mitigate risks related to data breaches, misuse, and unauthorized access. The policy ensures compliance with applicable data protection and information security regulations. It is applicable to all employees, contractual staff, and third-party service providers who access the system and involved in the design, operation, and management within PFMS.

Contents

## 1. Purpose

This policy defines the principles, controls, and practices adopted by the PFMS to protect data processed during the operations. It ensures compliance with the applicable legal, regulatory, and contractual requirements and aims to safeguard data against authorized access, misuse, or disclosure.

This policy supports the organization's commitment to confidentiality, integrity, and availability of information.

## 2. Scope

This policy applies to:

- This policy covers both digital and physical forms of data.
- All employees, contractual staff, and third-party service providers who access the system
- All data collected, processed, stored, and transmitted by the PFMS systems
- All environments including production, testing, staging, backup, and disaster recovery.

## 3. Definitions

**Data:** Data means any information, whether in electronic, digital, physical, or other form, that is collected, generated, processed, stored, transmitted, or accessed by the organization, including but not limited to personal data, financial data, transactional records, identifiers, credentials, logs, documents, communications, and any information relating to an identified or identifiable individual, customer, employee, business partner, or system.

**Processing**: Any operation performed on data, including collection, storage, transmission, modification, or deletion.

**Data Protection Officer:** Data Protection Officer (DPO) means the individual designated by the organization to oversee and ensure compliance with applicable data protection laws, regulations, and internal policies, and to act as the primary point of contact for data principals, regulatory authorities, and internal stakeholders on matters relating to the processing and protection of personal data.

**Management:** Management refers to Jt. CGA (TBRM), PFMS along with Jt. CGAs of other verticals under the overall supervision of Addl. CGA, PFMS.

**Policy/Policies:** Policy/Policies refer to ISMS policies formulated by PFMS

## 4.Data Protection Officer (DPO)

Dy. CGA(TRM) shall be designated as the Data Protection Officer (DPO) and shall be responsible for discharging the duties and obligations mentioned in 13.2 of this policy.

## 5. Data Protection Principles

The System shall adhere to the following principles:

**5.1 Lawfulness & Fairness**: Data shall be processed only for legitimate and lawful purposes.
**5.2 Purpose Limitation**: Data is collected strictly for the specified and explicit purposes listed below:

- Executing payment instructions under Government schemes.
- Authentication & verification of beneficiaries and stakeholders.
- Settling financial transactions.
- Generating transaction acknowledgments.
- Ensuring compliance with applicable laws and detect, prevent & investigate fraudulent or unauthorized transactions.
- Enhancing security, efficiency, accountability, monitoring, reporting and transparency in public fund management.
- Using data for analysis, modelling, reporting and other analytical purposes to derive insights, improve public financial management, support public decision making across current and future initiatives.
- Better targeting of public funds
- Detecting, preventing and mitigating fraud, security threats, or other unlawful or unauthorized activities.

***5.3*** **Data Minimization:** Only the minimum necessary data shall be collected and processed.

**5.4 Accuracy:** Reasonable steps are taken to ensure data accuracy and currency.

**5.5 Storage Limitation:** Data is retained only for legally mandated or business-justified periods.

**5.6 Confidentiality & Integrity**: Data shall be protected using appropriate technical and organizational controls.

**6. Data Classification**

All data shall be classified into the following categories:

**Public** – Information intended for public disclosure.

**Internal**– Operational information not intended for public release.

**Confidential** – Business or financial information.

**Restricted**– Personal data and sensitive financial data.

Restricted data shall receive the highest level of protection.

**7. Legal and Regulatory Compliance regarding data collection and consent**

- PFMS does not collect any PII data from vendors/beneficiaries/employees. The data is received

*** PFMS assumes that the Program Division/Agency/other users who are entering the PII Data of a beneficiary/vendor has obtained the individual's explicit consent to collect, use and process their data in the PFMS website in accordance with this policy and other applicable protection and privacy laws.*

- The System shall comply with applicable laws and standards, including but not limited to:

- Information security standard of ISO/IEC 27001:2022,
- IT Act, 2000
- Aadhaar Act, 2016

**8. Data Security Controls**

The following controls shall be implemented:

**8.1. Access Control**

- Access to data shall be based on the principle of least privilege.
- Role-based access control (RBAC) shall be implemented.
- Multi-factor authentication (MFA) shall be enforced for privileged users.
- Access rights shall be reviewed at least quarterly.
- All access shall be logged and monitored.

**8.2 Technical Controls**

- Encryption of data in transit.
- Secure key management.
- Secure APIs and application security testing.

**8.3 Organizational Controls**

- Mandatory security training for staff.
- Segregation of duties.
- Background verification for sensitive roles.

**8.4 Physical Controls**

- Secure data center.
- Restricted access to server rooms.
- CCTV and access logging.

**8.5 Secure Development:**

Security-by-design and security-by-default practices

**9.Incident Management and Breach Response**

All data breaches shall be handled under the Incident Response Policy. All incidents are reported to CERT-In as per extant rules.

**10. Data Sharing and Third Parties –**

- Since PFMS does not collect any data directly from individuals, the data can only be shared with the approval of competent authority.
- Data can be shared with a court of law to abide by an order in that regard.

- Any data sharing request by an individual or organisation must be routed through respective government ministries, departments and/or agencies who collected the data.

**11. Audit and Monitoring**

- Regular internal and external audits shall be conducted.
- Compliance metrics shall be reported to senior management.
- Logs shall be retained for forensic analysis.

Non-compliance shall result in corrective actions.

**12. Training and Awareness**

All personnel shall receive:

- Annual refresher training.
- Role-specific security education or standard operating procedures.

Training effectiveness shall be periodically assessed.

**13. Roles and Responsibilities**

**13.1 Management**

- Ensure adequate resources are aligned to execute and manage the operations within PFMS.
- Periodically review and approve any changes in the policy

**13.2 Data Protection Officer (DPO)**

- Monitor compliance with respect to the applicable regulations.
- Act as point of contact for regulators.
- Conduct privacy impact assessments for the applications, and processes.
- Highlight and alert Management for any observed gaps and non-compliances with the policy.

**13.3 Technical team users**

- Follow PFMS approved security practices provided within the role specific Standard Operating Procedures (SOPs).
- Report incidents through the Incident Management Forms available within the SOP documents.
- Protect credentials as per the PFMS approved protocols and standards.
- Abstain from any practices that may result in unauthorized access to PFMS data and maintain utmost vigil and attention to security practices