THIRD PARTY INFORMATION SECURITY POLICY

Table of Content

1. Purpose

The purpose of this policy document is to set out the minimum information security requirements expected of third parties who intend to carry out any work for or on behalf of the FINANCE DEPARTMENT. The overall objective is to maintain the confidentiality, integrity, availability, and privacy of FINANCE DEPARTMENT information to protect information assets for operational, contractual, regulatory, and legal reasons.

1.1. Scope

- The scope of this policy includes any third party that will have access to Jeevan Rekha FINANCE DEPARTMENT information either on-site or through remote access. This policy also applies to all Akshaya centres not limited to State Data Center (SDC) and the National Informatics Center (NIC).
- Any data that can be classified as Personal Data must be processed in compliance with the Aadhaar Act 2016, Information Technology (IT) Act 2000 (amended), and Jeevan Rekha , FINANCE DEPARTMENT's data protection and information security policies.

1.2. Ownership and Responsibilities

- This policy is owned and maintained by the Finance Department , and can be amended at the department's discretion, with or without notice, from time to time. Third parties will not be expected to comply with changes to this document until they have been provided with such changes in writing and given a reasonable period (not exceeding 120 days) to comply. This policy will be comprehensively reviewed and updated by FINANCE DEPARTMENT .

1.3. Information Security Assessments

- Third parties who fall within the above scope may be subject to compliance reviews against this policy and will be required to complete an assessment form. A review

will be undertaken to highlight potential risks, and third parties will be required to mitigate those risks before commencing any work.

2. Information Security Policy

- The Third Party shall at all times maintain a management-approved corporate Information Security Policy that defines responsibilities and outlines the Third Party's approach to information security. The Information Security Policies should align with Information Security frameworks such as ISO 27001, NIST, or other equivalent standards, as applicable.
- The Third Party shall agree to provide the FINANCE DEPARTMENT with copies of their Information Security policies upon request and demonstrate evidence of compliance with the adopted standards (e.g., ISO 27001).
- The Third Party shall maintain the adopted framework and policies covering all requirements set out in this policy document while adhering to industry best practices. These security policies must be communicated to all staff responsible for handling information related to the FINANCE DEPARTMENT.
- A Chief Information Security Officer (CISO) role shall be defined and assigned to an individual within the organization of the Third Party. This individual shall act as the primary contact for all Information Security matters and provide their contact details to the FINANCE DEPARTMENT.

3. Processes and Procedures

- All processes for managing the security of the FINANCE DEPARTMENT information must be assessed on an annual basis. Any changes to these processes must be communicated to FINANCE DEPARTMENT in a timely manner. The Third Party shall not process or use FINANCE DEPARTMENT's information or access FINANCE DEPARTMENT's systems for any purpose other than those directly required for the delivery of agreed services.
- The Third Party shall perform such services strictly in accordance with the contract. Disposal of any information related to the FINANCE DEPARTMENT must not occur without prior written approval from the Department.
- The Third Party shall establish and maintain safeguards to prevent accidental, deliberate, or unauthorized disclosure, access, manipulation, alteration, destruction, corruption, damage, loss, or misuse of FINANCE DEPARTMENT information. These safeguards shall also apply to any subcontractors or entities engaged by the Third Party.

4. Human Resources

4.1. Roles and Responsibilities

- The Third Party shall ensure that information security roles and responsibilities for all their employees and subcontractors are clearly defined, documented, and communicated.
- The Third Party shall maintain a comprehensive disciplinary policy, code of conduct, and work rules to safeguard the interests and security of the FINANCE DEPARTMENT personnel and information.

4.2. Contractual Agreements (IS IT NECESSARY)

- All personnel of the Third Party must enter into a written contract of employment. This contract must include agreements to comply with all relevant Third Party policies, rules, and procedures, including those related to information protection.

4.3. Training and Awareness

- The Third Party must conduct structured security awareness sessions for their personnel. These sessions should emphasize risks associated with poor information security practices, as well as legal and regulatory requirements for protecting information.

5. Compliance and Asset Management

5.1. Security Reviews

- The Third Party shall conduct annual security reviews of their processes and any subcontractors who have access to Jeevan Rekha,FINANCE DEPARTMENT's information. This includes processes confirming appropriate security controls and processes are in place. Detailed audit reports must document identified security risks, recommendations, and remedial actions.
- Security reviews must align with the requirements outlined in this Policy and comply with any additional instructions issued by the FINANCE DEPARTMENT.

5.2. Information Classification

- The Third Party shall classify Jeevan Rekha ,FINANCE DEPARTMENT's information according to its value, legal requirements, sensitivity, and criticality. Appropriate procedures for labeling, handling, and safeguarding Jeevan Rekha, FINANCE DEPARTMENT's information must be established and periodically reviewed, especially after significant changes in operations or policies.

5.3. Asset Inventory

- All assets used to process Jeevan Rekha, FINANCE DEPARTMENT's information must be recorded in a maintained inventory. These include physical and digital assets such as hard copies, laptops, portable storage devices, and magnetic media. The Third Party must ensure these assets are securely handled, transported, encrypted, and used only with proper authorization.

5.4. Data Privacy

- The Third Party shall implement and abide by an appropriate Data Protection Policy to safeguard Jeevan Rekha, FINANCE DEPARTMENT's information in accordance with the contract terms and applicable data protection laws.
- Transfer of J e e v a n R e k h a , FINANCE DEPARTMENT information outside India is prohibited as per Data protection policy.

- The Third Party shall maintain retention and secure deletion/destruction policies for Jeevan Rekha, FINANCE DEPARTMENT information. A copy of these policies should be submitted to FINANCE DEPARTMENT for review.
- Transfer or exchange of Jeevan Rekha, FINANCE DEPARTMENT information must be conducted via secure, encrypted channels. The encryption solution and the contents of the transfer must be communicated to the FINANCE DEPARTMENT in advance and approval received before data exchange or transfer.
- The Third Party shall implement measures to mitigate risks associated with the use of mobile computing devices, teleworking activities, and communication facilities for delivering services to Jeevan Rekha ,FINANCE DEPARTMENT
- The Third Party must notify the FINANCE DEPARTMENT immediately in

the event of a data loss or breach, providing details about the severity of the exposure.

- The Third Party shall not create unauthorized copies of J e e v a n R e k h a FINANCE DEPARTMENT's information under any circumstances.

6. Network Security Management

6.1. Network Security Controls

- The Third Party shall ensure the confidentiality, integrity, and availability of Jeevan Rekha FINANCE DEPARTMENT information by:
  - Utilizing secure network architecture and operations;
  - Ensuring that networks carrying Jeevan Rekha FINANCE DEPARTMENT 's information are designed, built, monitored, and managed according to recognized industry standards and frameworks such as ISO 27001, OWASP, and ITIL to prevent unauthorized access.

6.2. Restriction of System Utilities

- Utility programs capable of overriding system and application controls shall be strictly restricted and tightly controlled by the Third Party.

6.3. Penetration Testing

- The Third Party shall ensure that regular penetration testing is conducted using tools and methods approved, owned, and secured by the Third Party to access Jeevan Rekha ,FINANCE DEPARTMENT information.

6.4. System Security Measures

The Third Party must implement robust system security measures to prevent accidental or deliberate unauthorized disclosure, access, manipulation, alteration, destruction, corruption, damage, or misuse of Jeevan Rekha ,FINANCE DEPARTMENT information. At the minimum, Software must mandatorily require all system users to enter a username and password before accessing Jeevan Rekha, FINANCE DEPARTMENT information or systems.

6.5. Access Controls

- The Third Party shall establish, document, and regularly review formal procedures for granting and limiting access to Jeevan Rekha ,FINANCE DEPARTMENT information. Access must be restricted to personnel who require it for contractual purposes.

6.6. Password and User Account Policy

- The Third Party shall implement a system-enforced password and user account policy that meets or exceeds FINANCE DEPARTMENT requirements. This includes:
  - A minimum password length of 8 characters with a mix of uppercase, lowercase, numeric, and special characters;
  - Automatic logout and system lock when a workstation is left unattended;
  - Processes to manage and deactivate user accounts promptly upon employment termination, contract completion, or role changes.

6.7. Credential Management

- Credentials issued by FINANCE DEPARTMENT to the Third Party must not be shared with any other Third Parties Any such requirements are to be directly dealt by FINANCE DEPARTMENT alone.

6.8. Change Management

- The Third Party shall document and manage changes to FINANCE DEPARTMENT information and systems in compliance with FINANCE DEPARTMENT's change management processes. All changes must be logged for auditing and security purposes wherever possible.

7. Incident Management

7.1. Policy and Procedure:

- The Third Party shall maintain and regularly update a comprehensive security incident response procedure to address potential security breaches and vulnerabilities.
- The Third Party shall require all its personnel to promptly report any observed or

suspected security weaknesses, breaches, or vulnerabilities in the systems or services to their designated internal contact. Subsequently, the Third Party must inform the FINANCE DEPARTMENT immediately about such incidents or weaknesses.

7.2. Reporting Incidents

- All incidents must be reported to the designated NIC or through any contact mechanism

7.3. Incident Documentation and Resolution

- The Third Party must maintain detailed documentation of all reported incidents, including their nature, timeline, resolution steps, and preventive measures adopted.
- The Third Party shall work collaboratively with NIC to mitigate the impact of incidents and ensure resolution in a timely manner.
- Any security breach involving sensitive or classified FINANCE DEPARTMENT information must be escalated immediately to FINANCE DEPARTMENT's designated security authority.

End of Document