पेंशन निधि विनियामक और
विकास प्राधिकरण
बी-14/ए, छत्रपति शिवाजी भवन,
कुतुब संस्थागत क्षेत्र,
कटवारिया सराय, नई दिल्ली-110016.
दूरभाष : 011-26517501, 26517503, 26133730
फैक्स : 011-26517507
वेबसाइट : www.pfrda.org.in

**PENSION FUND REGULATORY
AND DEVELOPMENT AUTHORITY**
B-14/A, Chhatrapati Shivaji Bhawan,
Qutab Institutional Area,
Katwaria Sarai, New Delhi-110016.
Ph : 011-26517501, 26517503, 26133730
Fax : 011-26517507
Website : www.pfrda.org.in

Circular

No.: PFRDA/2017/31/CRA/5.

Date: 04.10.2017

Cyber security policy for intermediaries registered with PFRDA

Applicability: The policy guidelines shall be applicable to Central Recordkeeping Agencies (CRAs), Pension Funds and Custodian which form part and parcel of the critical Information Technology infrastructure under the National Pension System (NPS).

The intermediaries as mentioned above shall comply with the framework as provided below on cyber security of the critical IT infrastructure being developed and maintained by them:

1. As part of the operational risk management framework to manage risk to systems, networks and databases from cyber-attacks and threats, intermediaries shall formulate a comprehensive cyber security and cyber resilience policy document encompassing the framework mentioned hereunder. The policy document should be approved by the Board, and in case of deviations from the suggested framework, reasons for such deviations should also be provided in the policy document. The policy document should be reviewed by the Board of the intermediary at least annually with the view to strengthen and improve its cyber security and cyber resilience framework.
2. The cyber security policy should encompass the principles and provisions prescribed under the Information Technology Act 2000 (such as section 43A of the IT Act, 2000). Further, the intermediaries shall be liable to pay damages for negligence in implementing and maintaining reasonable security practices and procedures as per section 43A of the IT Act.

Broadly, the following steps shall be undertaken by the intermediary to arrive at the comprehensive cyber security and cyber resilience policy document:

A. Risk assessment

Intermediaries should conduct risk assessments. Risk assessment identifies threats and vulnerabilities and should be sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications. Risk assessment will allow determination of the acceptable level of risk and assist the selection of appropriate controls to manage the risk of potential harm to information systems and networks in light of the nature and importance of the information to be protected. Because of the growing interconnectivity of information systems, risk assessment should include consideration of the potential harm that may originate from others or be caused to others.

Intermediary shall 'Identify' critical IT assets and risks associated with such assets,

- Intermediary should identify critical assets based on their sensitivity and criticality for business operations, services and data management. To this end, intermediary should maintain up-to-date inventory of its hardware and systems, software and information assets (internal and external), details of its network resources, connections to its network and data flows.
- Intermediary should accordingly identify cyber risks (threats and vulnerabilities) that it may face, along with the likelihood of such threats and impact on the business and thereby, deploy controls commensurate to the criticality.
- Intermediaries should also encourage its third-party providers, such as service providers, stock brokers, depository participants, etc. to have similar standards of Information Security.

B. Security design and implementation

Intermediaries should incorporate security as an essential element of information systems and networks. Systems, networks and policies need to be properly designed, implemented and coordinated to optimise security. A major, but not exclusive, focus of this effort is the design and adoption of appropriate safeguards and solutions to avoid or limit potential harm from identified threats and vulnerabilities. Both technical and non-technical safeguards and solutions are required and should be proportionate to the value of the information on the organisation's systems and networks. Security should be a fundamental element of all products, services, systems and networks, and an integral part of system design and architecture. For end users, security design and implementation consists largely of selecting and configuring products and services for their system.

Intermediary shall plan for all efforts to 'Protect' assets by deploying suitable controls, tools and measures,

In order to protect the assets, policies with respect to the following shall be clearly laid down and adhered to by the intermediary at all times:

- Access Controls
- Physical security
- Network Security Management

- Security of Data
- Hardening of Hardware and Software
- Application Security and Testing
- Patch Management
- Disposal of systems and storage devices
- Vulnerability Assessment and Penetration Testing (VAPT)
- Testing of all application software with respect to cyber security

C. Security management

Intermediaries should adopt a comprehensive approach to security management. Security management should be based on risk assessment and should be dynamic, encompassing all levels of intermediary's activities and all aspects of their operations. It should include forward-looking responses to emerging threats and address prevention, detection and response to incidents, systems recovery, ongoing maintenance, review and audit. Information system and network security policies, practices, measures and procedures should be coordinated and integrated to create a coherent system of security. The requirements of security management depend upon the level of involvement, the role of the intermediary, the risk involved and system requirements.

Intermediary shall plan for all efforts to 'Detect' incidents, anomalies and attacks through appropriate monitoring tools / processes.

- Intermediary should establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events and timely detection of unauthorised or malicious activities, unauthorised changes, unauthorised access and unauthorised copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network devices should also be monitored for anomalies.
- Suitable alerts should be generated in the event of detection of unauthorized or abnormal system activities, transmission errors or unusual online transactions.

D. Response

Intermediaries should act in a timely and co-operative manner to prevent, detect and respond to security incidents. Recognising the interconnectivity of information systems and networks and the potential for rapid and widespread damage, intermediaries should act in a timely and co-operative manner to address security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective co-operation to prevent, detect and respond to security incidents.

Intermediary shall "respond' by taking immediate steps after identification of the incident, anomaly or attack.

- Alerts generated from monitoring and detection systems should be suitably investigated, including impact and forensic analysis of such alerts, in order to determine activities that are to be performed to prevent expansion of such incident of cyber-attack or breach, mitigate its effect and eradicate the incident.
- The response and recovery plan of the intermediary should aim at timely restoration of systems affected by incidents of cyber-attacks or breaches.
- The Intermediaries shall also report all the cyber incidents to Indian Computer Emergency Response Team (CERT-In) as prescribed under section 70B of the Information Technology Act,2000 and the Rules thereunder.

E. Recover

Intermediary shall "Recover' from incident through incident management, disaster recovery and business continuity framework.

- The recovery plan should be with reference to the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) specified by the Board of the intermediary and as accepted by the Authority.
- The response plan should define responsibilities and actions to be performed by its employees and support / outsourced staff in the event of cyber-attacks or breach of cyber security mechanism.
- Any incident of loss or destruction of data or systems should be thoroughly analyzed and lessons learned from such incidents should be incorporated to strengthen the security mechanism and improve recovery planning and processes.

F. Reassessment

Intermediaries should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures. New and changing threats and vulnerabilities are continuously discovered. Intermediaries should continually review, reassess and modify all aspects of security to deal with these evolving risks in accordance with the rules, regulations and guidelines prescribed by CERT-In and NCIIPC from time to time under the IT Act..

- Intermediary should also conduct suitable periodic drills to test the adequacy and effectiveness of response and recovery plan.

G. The intermediary shall follow the Information Technology Act, 2000 and other laws as may be prescribed with regard to cyber security/ cyber transactions from time to time."

3. The cyber security policy should include the following process to identify, assess, and manage cyber security risk associated with processes, information, networks and systems.
4. The cyber security policy of the intermediary should incorporate best practices from standards such as ISO 27001, ISO 27002, COBIT 5, etc., or their subsequent revisions, if any, from time to time.
5. Intermediary should designate a senior official as Chief Information Security Officer (CISO) whose function would be to assess, identify and reduce cyber security risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per the cyber security and resilience policy approved by the Board of the intermediary. Intermediary should establish a reporting procedure to facilitate communication of unusual activities and events to CISO or to the senior management in a timely manner. The aforementioned committee and the senior management of the intermediary, including the CISO, should periodically review instances of cyber-attacks, if any, domestically and globally, and take steps to strengthen cyber security framework in a holistic manner.
6. Quarterly reports containing information on cyber-attacks and threats experienced by intermediary and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities / threats that may be useful for other intermediaries shall be submitted to the Authority (PFRDA).
7. Intermediaries should conduct periodic training programs to enhance awareness level among the employees and outsourced staff, vendors, etc. on IT / Cyber security policy and standards. Special focus should be given to build awareness levels and skills of staff from non-technical disciplines. Such training program should be reviewed and updated at periodic intervals to ensure that the contents of the program remain current and relevant.
8. This circular is being issued in exercise of powers conferred under Section 14(1) of PFRDA Act, 2013 to protect the interests of subscribers and to promote the development of, and to regulate the National Pension System.

04/10/17

Venkateswarlu Peri
Chief General Manager