पेंशन निधि विनियामक और विकास प्राधिकरण
PENSION FUND REGULATORY AND DEVELOPMENT AUTHORITY

परिपत्र

परिपत्र संख्या : पीएफआरडीए/2024/14/आईसीएस/01 **01 अगस्त, 2024**

सेवा में,

पीएफआरडीए के सभी मध्यवर्ती / विनियमित संस्थाएं

महोदया / महोदय,

सूचना और साइबर सुरक्षा नीति दिशानिर्देश - 2024 पर मध्यवर्ती / विनियमित संस्थाओं के लिए परिपत्र

1. प्रौद्योगिकी में लगातार हो रहे संवर्धन और उभरते हुए खतरों के बीच, साइबर सुरक्षा उपायों के माध्यम से आईटी अवसंरचना और डेटा की सुरक्षा भी बहुत महत्त्वपूर्ण है। यह उम्मीद की जा रही है कि विनियमित संस्थाओं ने साइबर सुरक्षा मामलों पर रोक लगाने के लिए अतीत में उपाय किए होंगे, लेकिन अभिदाताओं के हितों की रक्षा करने और विकसित हो रहे स्थापत्य की सुरक्षा और उसकी सत्यनिष्ठा सुनिश्चित करने के लिए, प्राधिकरण द्वारा सूचना और साइबर सुरक्षा नीति दिशानिर्देश - 2024 को **अनुलग्नक** में प्रदान किया गया है। ये दिशानिर्देश, विनियमित संस्थाओं के लिए साइबर खतरों को प्रभावी ढंग से प्रबंधित करने, महत्वपूर्ण आस्तियों की रक्षा करने और डिजिटल युग में विश्वास और भरोसा बनाए रखने के लिए एक रोडमैप के रूप में काम करेंगे। ये दिशानिर्देश विनियमित संस्थाओं के लिए एक व्यापक मानदंड के रूप में भी कार्य करेंगे ताकि वे अपनी सूचना और संचार प्रौद्योगिकी (आईसीटी) अवसंरचना को साइबर खतरों से बचाने के लिए आवश्यक नियंत्रणों और प्रक्रियाओं को समझ सकें और उन्हें कार्यान्वित कर सकें।

2. यह परिपत्र, पेंशन निधि विनियामक और विकास प्राधिकरण अधिनियम की धारा 14 के अंतर्गत प्रदत्त शक्तियों का प्रयोग करते हुए जारी किया गया है।

3. ये दिशानिर्देश **01 अगस्त, 2024** से लागू होंगे।

सचिन

सचिन जोनेजा
महाप्रबंधक
सूचना और साइबर सुरक्षा विभाग

पेंशन निधि विनियामक और विकास प्राधिकरण
PENSION FUND REGULATORY AND DEVELOPMENT AUTHORITY

बेटी बचाओ बेटी पढ़ाओ

CIRCULAR

Circular No.: PFRDA/2024/14/ICS/01 **01.08.2024**

To

All Intermediaries / Regulated Entities of PFRDA

Madam/Sir,

Circular on Information & Cybersecurity Policy Guidelines- 2024 for Intermediaries/Regulated entities

1. With the rapid technological advancements and emerging threats, protection of IT infrastructure and data through cybersecurity measures is of considerable importance. While the regulated entities are expected to have taken measures in the past to prevent the cyber security issues, in order to protect the interest of the subscribers and ensure safety and integrity of the evolving architecture the Authority hereby lays down Information & Cybersecurity Policy guidelines - 2024 as per **Annexure**. These guidelines will serve as a roadmap for Regulated Entities to effectively manage cyber risks, protect critical assets and maintain trust and confidence in the digital age. The guidelines shall also act as a broad standard for the Regulated Entities to understand and implement essential controls and procedures to protect their Information & Communication Technology (ICT) infrastructure from cyber threats.

2. This circular is issued in exercise of powers conferred under section 14 of the Pension Fund Regulatory and Development Authority Act.

3. These guidelines shall come into effect from **01st August, 2024.**

Sachin Joneja
General Manager
Information & Cyber Security Department

ANNEXURE

PENSION FUND REGULATORY AND DEVELOPMENT AUTHORITY

Information and Cyber Security Policy Guidelines - 2024

For

Intermediaries / Regulated Entities

Table of Contents

1. Introduction and scope

In today's interconnected digital landscape, the financial services sector stands as a prime target for cyber threats due to the vast amounts of sensitive data it handles, including personal and financial information. Cyber-attacks are increasing in frequency, sophistication and impact, with perpetrators continually refining their efforts to compromise systems, networks and information world-wide. A key driver of this trend is the increasing usage of technology by the financial services sector to improve customer service and operational efficiency.

The following emerging trends in technology and their extensive use in almost all spheres of financial services is creating opportunities and threats in the form of Cybersecurity risk to the business:

- Cloud storage has revolutionized the way we manage and access data, offering unparalleled convenience and flexibility. It enables users to store vast amounts of information remotely, accessible from anywhere with an internet connection. However, this convenience comes with its own set of cybersecurity risks.
- APIs (Application Programming Interfaces) serve as the backbone of modern software, enabling different systems to communicate and share data efficiently. Vulnerabilities in these APIs, such as injection flaws or insecure direct object references, can be exploited by attackers to access or manipulate data without proper authorization.
- Mobile applications introduce significant cybersecurity risks due to their access to sensitive data and widespread usage. These risks include data breaches, malware infiltration, insecure data storage and communication, weak authentication mechanisms, vulnerabilities in third-party dependencies, code tampering, and susceptibility to phishing attacks.
- The increasing use of artificial intelligence (AI) as a tool by industry as well as by cyber attackers also introduces new challenges and risks, as cyber attackers leverage AI-driven techniques to launch more sophisticated and targeted attacks. Still, AI technologies have the potential to revolutionize cybersecurity practices, offering innovative solutions for threat detection, incident response, and vulnerability management.

Objective and Purpose:

In the NPS architecture there is significant element of data storage, transmission and recordkeeping with Central Recordkeeping Agencies (CRA's), PFMs, POPs, Custodian and Trustee bank and the safety and security of which is of primary concern to the regulator in order to ensure systemic protection. The continued safety and security of the systems, data and privacy of the information is of utmost importance to the regulator in light of the protection of subscriber's interest.

In order to ensure that the systems, data and privacy of information under NPS architecture are secure, PFRDA has put in place various guidelines which are aimed at preventing cyber-attacks and also to guide regulated entities / intermediaries in responding to cyber-related incidents, such as (a) Cyber security guidelines for intermediaries – 2017 and amendments thereof (b) Guidelines on Cloud adoption by intermediaries – 2023 (c) guidelines on outsourcing of activities by intermediaries, and Risk Management Framework (RMF) for CRAs etc.

The primary objective of having these information and cybersecurity policy guidelines is to establish a structured framework that outlines the principles, procedures, and best practices for protecting the regulated entities (REs) information assets and data from cyber threats. These guidelines serve as a roadmap for regulated entities (REs) to effectively manage cyber risks, protect critical assets, and maintain trust and confidence in the digital age. These guidelines may also act as a baseline document for administration and audit teams (internal, external/ Third-party auditors) to evaluate the regulated entities security posture against cyber security baseline requirements.

2. Preliminary

2.1 Short Title and Commencement

a) These guidelines shall be called the PFRDA (Information and Cybersecurity) guidelines for regulated entities/intermediaries, 2024.

b) These guidelines incorporate, consolidate and update the guidelines, instructions and circulars on Cybersecurity issued by the Authority including the following:

- Cybersecurity Guidelines issued vide circular PFRDA/2017/31/CRA/5 dt. 04.10.2017
- Guidelines issued vide circular PFRDA/2019/REG dt. 07.01.2019

c) These guidelines shall come into effect from **1st August, 2024.**

2.2 Applicability

These guidelines shall be applicable to all regulated entities / intermediaries governed under PFRDA Act, 2013 and the regulations issued thereunder. Further;

a) The provisions of these guidelines shall be in addition to, and not in derogation of the provisions of any other laws, rules, regulations or directions, for the time being in force.

b) For the purpose of these guidelines, the Regulated Entities (REs) / intermediaries are classified into two categories as (i) Category I - consisting of Central Recordkeeping Agencies (CRAs) and Pension Funds registered with PFRDA including PFs who also registered as Point of Presence (ii) Category II - consisting of Point of Presence (POPs) including APY-SPs, Trustee Bank, Custodian and Retirement Advisors excluding individuals. The applicability of these guidelines accordingly based on the categorization is as given below:

Category I:

- The complete Information and Cybersecurity Policy Guidelines – 2024 for Regulated Entities and Intermediaries as provided hereunder are applicable.

Category II:

- The Information and Cybersecurity Policy Guidelines – 2024 for Regulated Entities and Intermediaries are applicable. However, if a RE/Intermediary is covered under similar guidelines issued to protect the data, information and Cybersecurity of the IT systems by their principal regulator (such as RBI/SEBI/IRDAI/NHB) and certifies that they are complying with same, such a RE/Intermediary will be deemed to be in compliance with these guidelines provided they also comply with Sec 4.5 of these Guidelines on Reporting of Cybersecurity related incidents.

2.3 Definitions

In these guidelines, unless the context states otherwise, the terms herein shall bear the meanings assigned to them as below:

i. ‘Cyber security’ - Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.

ii. ‘Cyber risk’ includes any reasonably identifiable circumstance in relation to the use of network and information systems, - including a malfunction, capacity overrun, failure, disruption, impairment, misuse, loss or other type of malicious or non-malicious event - which, if materialized, may compromise the security of the network and information systems, of any technology-dependent tool or process, of the operation and process’ running, or of the provision of services, thereby compromising the integrity or availability of data, software or any other component of ICT services and infrastructures, or causing a breach of confidentiality, a damage to physical ICT infrastructure or other adverse effects;

iii. ‘Cyber incident’ includes an unforeseen identified occurrence in the network and information systems, whether resulting from malicious activity or not, which compromises the security of network and information systems, of the information that such systems process, stores or transmits, or has adverse effects on the availability, confidentiality, continuity or authenticity of financial services provided by the regulated entity / intermediary.

iv. ‘Cyber-attack’ means a malicious cyber incident by means of an attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset perpetrated by any threat actor;

v. ‘Information and communication technology (ICT)’ risk means the current or prospective risk of losses due to the inappropriateness or failure of the hardware and software of technical infrastructures, which may compromise the availability, integrity, accessibility and security of such infrastructures and of data.

vi. ‘Vulnerability’ means a weakness, susceptibility or flaw of an asset, system, process or control that can be exploited by a threat;

vii. ‘Information Asset’ - Any piece of data, device or other component of the environment that supports information-related activities. Information Assets include information system, data, hardware and software.

viii. ‘Information System’ - Set of applications, services, information technology assets or other information-handling components, which includes the operating environment and networks.

ix. ‘IT Risk’ - The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise.

3. Information and Cybersecurity Policy

i. Regulated entities / intermediaries shall formulate and put in place a comprehensive Information and Cybersecurity policy after taking note of the guidance provided hereunder by way of best practices and with the due approval of their Board. The guidance provided hereunder shall be the minimum and the RE’s being professional organizations may go beyond depending on the need and necessity.

ii. The policies related to Information and Cybersecurity policy, Business Continuity, Cyber Crisis Management Plan (CCMP), Information Security Audit policy and Information Security shall be approved by the Board of Directors of the regulated entity (RE).

iii. The Board of the Regulated entities / intermediary should review such policy at least once in two years, with an objective of strengthening and improving the cyber security and resilience of information systems. The following aspect shall be considered for review of the policy:

   a. Changes in regulatory and legal provisions relating to information and cybersecurity aspects effecting the business.

   b. Changes in or additions in industry standards

c. Changes in methods of operating business including changes in organizational structure

d. New channels of business

e. New technologies or functionalities introduced in the past one year

f. Incidents reported within or outside organization related to information and cybersecurity

g. Any other considerations requiring an intervention.

The policy which has been reviewed and approved by the Board shall be submitted to the Authority within 30 days of such approval by the Board of the regulated entity (RE).

iv. The Regulated entity (RE) shall frame the said information and cyber security policy as befitting a professional organization and own up its implementation and consequences thereon.

v. The Regulated entities / intermediary while drafting the Information and Cybersecurity policy should also consider the relevant provisions of the Information Technology Act, 2000, and Digital Personal Data Protection Act, 2023, to protect and secure personal data of subscribers as is envisaged under the said Act.

vi. The Information and 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.

4. Components of Information and Cybersecurity Policy (ICP)

The regulated entity (RE) shall put in place appropriate governance structure to effectively manage and mitigate information and cybersecurity risks while aligning cybersecurity with overall business goals and objectives. The structure shall consist of an Information and cyber security risk management committee (ICSRM) and comprising a Chief Information Security Officer (CISO), Chief Risk officer (CRO), Chief Technology officer (CTO) and other functional heads. The regulated entity may choose appropriate composition of the committee basing on size, complexity and nature of operations. The regulated entity shall provide the details of the ICSRM to the Authority including changes if any in an ongoing manner.

Major responsibilities of the ICSRM, *inter alia*, shall include:

a. Development of information and cyber security policies, implementation of set policies, standards and procedures to ensure that all identified risks are managed within the RE's risk appetite;

b. Approving and monitoring information security projects and security awareness initiatives;

c. Reviewing cyber incidents, information systems audit observations, monitoring and mitigation activities;

The following shall be the components of the information and cybersecurity policy that needs to be developed and put in place in terms of these guidelines. The sub-components provided thereunder showcase the best practices to be adopted for an enhanced cyber resilience and security of the information and IT assets of the RE.

4.1 Core Components of the Information and Cybersecurity Policy (ICP)

The core components of the ICP are;

4.1.1 Governance:

The key focus areas of IT Governance shall include strategic alignment, risk management, resource management, performance management and Business Continuity/ Disaster Recovery Management. REs shall put in place a robust IT Governance Framework based on the aforementioned focus areas that inter alia:

(i) specifies the governance structure and processes necessary to meet the RE's business/ strategic objectives;

(ii) specifies the roles (including authority) and responsibilities of the Board of Directors (Board) / Board level Committee and Senior Management; and CISO, CTO/CIO, Audit committee, Risk management committee and similar positions at the regulated entity.

(iii) includes adequate oversight mechanisms to ensure accountability and mitigation of IT and cyber/ information security risks.

The regulated entity (RE) shall have a CISO. The CISO should have a dedicated cybersecurity team and preferably separate from IT operations and infrastructure team. The team would be responsible for the following indicative roles:

a. monitoring network's security and responding to security alerts

b. conducting incident response

c. formulating, enforcing and reviewing IT security policies

d. conducting cybersecurity awareness drills and campaigns within the organization.

e. liaising with PFRDA, CERT-In and industry cybersecurity REs.

f. setting up and running of Security Operations Centre (SOC) including receiving, monitoring and closure of such incidents.

4.1.2 Identify

Understand and prioritize cybersecurity risks to systems, assets, data, and capabilities and after due examination of the following:

a. Threat and Risk Assessment

- The Regulated entity (RE) shall connect to the Network Time Protocol (NTP) Server of National Informatics Centre (NIC) or National Physical Laboratory (NPL) or with NTP servers traceable to these NTP servers, for synchronization of all their ICT systems clocks.
- The Regulated entity (RE) must identify the possible threat vectors, exploitation points, tools and techniques, which can compromise the security of the RE.
- The Regulated entity (RE) must perform vulnerability assessment to identify vulnerabilities and weaknesses in configuration devices and systems; vulnerabilities and threats associated with the use of specific ports, protocols and services and vulnerabilities introduced due to changes in ICT infrastructure.
- A defined and documented Risk Assessment Methodology shall be used to conduct the Risk Assessment Exercise. All risks having a risk rating above the acceptable level of risk shall have risk mitigation plans.
- Regulated entity (RE) shall 'Identify' critical IT assets and risks associated with such assets.
- Regulated entity (RE) 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.
- Regulated entity (RE) 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.

- Regulated entity (RE) should also encourage its third-party providers, such as service providers, stock brokers, depository participants, etc. to have similar standards of Information Security.

b. Inventory Management of Information Assets

- Maintain an up-to-date information asset Inventory Register.
- Classify data/information based on sensitivity criteria of the information.

4.1.3 Protect

Implement safeguards to ensure the delivery of critical services and protect against cyber threats: The Regulated Entity/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)

The following indicative controls provide the regulated entities (RE's) with guidance on the matter:

a. Preventing access of unauthorized software

- Put in place a mechanism to control installation of software/ applications on end-user PCs, laptops, workstations, servers, mobile devices, etc. In addition, put in place a mechanism to block/ prevent and identify installation and running of unauthorized software/ applications on such devices/ systems.

b. Physical and Environmental Controls

- Put in place appropriate controls for securing physical location of critical assets, providing protection from natural and man-made threats.

c. Network Management and Security

- Define an appropriate network architecture including the network perimeter, any internal networks, and links with other REs such as service providers or partners. Manage the network perimeter by controlled access to ports, protocols and applications by filtering and inspecting all traffic at the network perimeter to ensure that only traffic which is required to support the business is being exchanged. Control and manage all inbound and outbound network connections and deploy technical controls to scan for malicious content.
- Use firewalls to create a buffer zone between the Internet (and other untrusted networks) and the networks used by the business. The firewall rule set should deny traffic by default and a whitelist should be applied that only allows authorized protocols, ports and applications to exchange data across the boundary.
- Network Intrusion detection / prevention and other appropriate security devices should be deployed and monitored for North-South (Internet to LAN) and East-West (Between Intranet for monitoring unauthorized lateral movements) by trained/certified personnel. Alerts generated from the devices should be thoroughly verified as most of them could be indicating an imminent attack.
- The RE shall develop an accurate mapping of the core components, connections and information of the network to build RE's network diagram including network components such as routers, switches, firewall and other Perimeter Security devices, computer systems, IP addresses, data flow routes, blacklisted or white listed systems/IP addresses, open/entry ports, subnet mask, administrative interface, zones, access control lists, network name etc. RE must store this document in confidential manner as this contains sensitive information.
- All devices placed within the network should have logging enabled. Logs of perimeter security devices and end points should be integrated with Security Information and Event Management (SIEM) and alerts from SIEM should be monitored and acted upon. Logs of perimeter security devices and SIEM should be stored for a rolling period of 180 days.

- For protection against the distributed denial of service (DDoS) and denial of service (DoS) attacks, appropriate protection should be incorporated through DDoS mitigation devices and DDoS mitigation service through service providers. Clearly define the SLAs with service providers while planning for DDoS mitigation services.
- Use secure protocols such as SSH, SSL, or IP Security (IPSec) encryption for all remote connections to the router/switch/server.
- Ensure that Virtual Private Network (VPN) is used for accessing Network Resources from Remote location. Enable Multi Factor Authentication (MFA) for VPN accounts. Enable VPN account logging and integrate VPN logs with Security Information and Event Management (SIEM) system.
- Boundary defenses should be multi-layered with properly configured firewalls, proxies, De-Militarized Zone (DMZ) perimeter networks, and network-based Intrusion Prevention System (IPS)/Intrusion Detection System (IDS). A mechanism to filter both inbound and outbound traffic shall be put in place.
- Implement Network access control (NAC) to enhance security by regulating and monitoring devices' access to a network based on predefined policies.

d. Wireless LAN security

- Ensure that the communication between the user system and wireless Access Point (AP) is secured using highest graded encryption (WPA-2 or higher) for data confidentiality and integrity.
- Ensure that there is a segmentation of Wi-Fi users and/or devices on the basis of SSID and customized access policies are applied per SSID as per the requirements.
- If the RE sets up external WLANs primarily to provide Internet access to visitors, such WLANs should be designed so that their traffic does not traverse the RE's internal trusted networks. Configure a guest WLAN with a "separate" SSID and limit guest access to Internet only. Ensure that guest accounts require login (guest authentication).
- RE should implement appropriate technical security controls to separate Wi-Fi network and wired network. Devices used for connecting the Wi-Fi network should not be allowed to connect simultaneously to the wired network to protect against bridging of networks.

- Ensure that there are tools in the WLAN platform to identify rogue Access Point or those potentially spoofing corporate SSIDs.
- It is recommended to use 802.1x for authentication in the Wi-Fi.
- Wireless LAN should not be permitted in sensitive REs. REs should watch out for unauthorized mobile / smartwatch with networking capabilities being connected to the USB ports of the computer devices. This allows bridging of networks and paves a way for attackers to reach the network without the security restrictions.
- The RE should ensure that there is proper physical isolation of sensitive and wireless networks.
- Disable SSID broadcasting to prevent the access points from broadcasting the SSID. Allow only authorized users with preconfigured SSID to access the Wireless network.
- Disable DHCP and assign static IP addresses to all wireless users.
- The RE should identify ports, protocols and services required to carry out daily operations and block all others, including all non-IP based and unencrypted protocols, by establishing policies in routers and wireless access points.

e. Perimeter threat protection

- The RE must ensure perimeter threat protection of its network infrastructure through implementation of capabilities such as a firewall, IPS etc.

f. Secure Configuration

- Desktops shall be hardened to the extent possible.
- The configurations at all layers such as network, operating system, application, database should be set to the highest security level and reviewed periodically.

g. Patch Management

- As far as possible, maintain centralized patch management and centralized Antivirus server managing antivirus on all office systems with up to date patches and signatures.
- The RE must ensure that patch management is carried out at regular intervals or as soon as critical patches for ICT systems or software are available.
- Keep operating systems, browsers and any other applications up to date and apply all security patches.

- The RE must ensure that patch management is carried out at regular intervals or as soon as critical patches for ICT systems or software are available
- Put in place systems and processes to identify, track, manage and monitor the status of patches to servers, operating system and application software.

h. Endpoint security solutions & Anti-virus Management

- Endpoint security solutions should be deployed for continuously monitoring end user devices to detect and respond to cyber threats like ransomware, malware and unauthorized accesses. It should record all activities and security events taking place on all office end points, which should be continuously monitored by the IT Infra/expert team.
- The RE must block all unnecessary services and system level administrator privileges through methods such as active directory, group policies on endpoint devices and systems.
- Ensure that anti-virus solutions are implemented in all endpoints and are up to date.

i. User Access Control / Management

- Access privileges to users must be based on operational role and requirements. Access security matrix must be prepared which contains the access rights mapped to different roles. This must be done to achieve the objective of role-based access control (RBAC). Access to system must be granted based on access security matrix.
- Implement strict user access controls based on principle of least privilege.
- Disallow administrative rights on end-user workstations/ PCs/ laptops and provide access rights on a ‘need to know’ and ‘need to do’ basis.
- Implement multi-factor authentication (MFA) for all critical applications, especially for the privileged accounts. All access to outside stakeholders shall be based on 2 FA.
- Disable Remote Desktop Protocol (RDP). Restricted access in case of exceptions, may be provided only on need basis with appropriate monitoring.

j. Password Management

- All active sessions of a user must be terminated post 15 minutes of inactivity and must be activated only post re-authentication by specified mechanism such as re-entering password etc.
- Passwords should be with a minimum length of 8 characters, using a combination of capital letters, small letters, numbers and special characters.
- Force change passwords at least once in 120 days and as a system built process.
- Passwords must be encrypted when transmitting over an un-trusted communication network
- Implement strong password management policy with specific emphasis for sensitive activities like accessing critical systems.

k. Secure mail and messaging systems

- Implement secure mail and messaging systems that include measures to prevent email spoofing, identical mail domains, protection of attachments, malicious links, etc.

l. Remote access

- Implement appropriate security technologies to protect information or information systems being accessed via remote access, such as using VPN based on SSL/TLS, SSTP or IPSec with MFA.

m. Conduct of Vulnerability Assessment (VA) / Penetration Testing (PT)

- In the post implementation of an IT project/ system upgrade, new functionality etc., the VA/PT shall be performed on the production environment. Under unavoidable circumstances, if the PT is conducted in test environment, REs shall ensure that the version and configuration of the test environment resembles the production environment.
- REs shall ensure to fix the identified vulnerabilities and associated risks in a time bound manner by undertaking requisite corrective measures and ensure that the compliance is sustained to avoid recurrence of known vulnerabilities.
- REs shall put in place a documented approach for conduct of VA/ PT covering the scope, coverage, vulnerability scoring mechanism (e.g., Common Vulnerability Scoring System) and all other aspects. This may also apply to the RE's information systems hosted in a cloud environment.

- For critical information assets (applications, systems and IT infrastructure) and/ or those in the DMZ (De-Militarized Zone) having customer interface, VA shall be conducted at least once in every six months and PT at least once in 12 months. Also, REs shall conduct VA/ PT of such information assets throughout their lifecycle (pre-implementation, post implementation, after major changes, etc.). For all other information assets, a risk-based approach shall be adopted to decide the requirement and periodicity of conduct of VA/ PT.
- High risk gaps, reported from the VAPT, should be closed within a period of one month followed by validation testing. Priority for closure of audit gaps should be based on the risk associated with each gap; however, the outer time limit for closure of all the audit gaps is two months.

n. Data Security

- Identify and classify sensitive/personal data and apply measures for encrypting such data in transit and at rest. Deploy data loss prevention (DLP) solutions / processes.
- Evolve and implement a Data Backup policy. All the business-critical data should be backed up regularly to prevent data loss and to ensure faster recovery in case of an incident.
- Audit and remediate vulnerabilities in applications, which could cause data breaches/leaks that include Insecure Direct Object Reference (IDOR), SQL injection, Insecure API endpoints, Directory listing etc.
- Encryption of the data at rest should be implemented to prevent the attacker from accessing the unencrypted data. Identify and classify sensitive and Personally Identifiable Information (PII) data and apply measures for encrypting such data in transit and at rest.

o. Data Leak Prevention (DLP) Strategy

- Deploy DLP solutions to monitor and control the movement of sensitive data within the organization's network and endpoints. DLP solutions can detect and prevent unauthorized access, transmission, or exfiltration of sensitive data through email, web applications, removable storage devices, and other channels. Configure DLP policies to detect and block sensitive data based on predefined rules and patterns.

- Encrypt sensitive data both in transit and at rest to protect it from unauthorized access or interception. Use strong encryption algorithms and secure key management practices to safeguard data confidentiality. Implement encryption for data stored in databases, file systems, and during transmission over networks.
- Develop a comprehensive incident response plan to effectively respond to data leaks or breaches. Define roles and responsibilities, establish communication protocols, and outline procedures for containing, investigating, and mitigating data security incidents. Test the incident response plan regularly through tabletop exercises and simulations to ensure readiness to respond to real-world threats.

p. Application security

- The Regulated Entity (RE) should incorporate security at each level of software development lifecycle such as during development, deployment, and maintenance of application etc. to reduce vulnerabilities. During development secure coding practices should be followed. Testing should be conducted during development, deployment. And maintenance of application.
- Ensure privacy protection of user/customer data at each stage of application life cycle.
- The Regulated Entity (RE) should identify ports, protocols and least privileged services required to carry out daily operations of applications / platforms and restrict or block all others.
- Regulated Entity (RE) should ensure that applications validate the data on the server-side.
- Ensure applications execute proper error handling and should not provide detailed system information, deny service, impair security mechanisms, or crash the system.
- Implement measures for securing Application Program Interfaces (APIs). Include API security in Vulnerability Assessment and Penetration Testing and mitigate vulnerabilities in APIs.
- Log monitoring on a continuous basis to be carried out with the ability to alert the operations team when a security anomaly is suspected.

- Implement Integrity checks and disallow the binary from executing that does not confirm to the application / system security.

q. Application Security Life Cycle (ASLC)

- Ensure that maintenance and necessary support of software applications is provided by the software vendors and the same is enforced through formal agreement. It is recommended that source codes for all critical applications are received from the vendors or a software escrow agreement is in place with the vendors for ensuring continuity of services in case the vendor defaults or is unable to provide services.
- The development/ test and production environments shall be properly segregated. The data used for development and testing should be appropriately masked.

r. Mobile Application Security

- Ensure that their mobile applications address the Open Web Application Security Project (OWASP) Mobile Top 10 vulnerabilities.
- The mobile application should implement SSL Pinning to prevent man-in-the-middle attacks.
- Only permissions required for essential functionality of the application should be sought from the user.
- Sensitive data should be shared over secure SSL/TLS connection only.
- Should maintain an updated document containing the list of authorized applications, their usage: custodian(s) assigned to each application, level of criticality: version implemented: number of installed instances, application license details etc.
- Debug logs should be disabled. Obfuscation of the code by packers, encryptors and related tools could be considered for preventing reverse engineering of the applications.

s. Protect against API attacks

i. Authentication and Authorization

  - Use strong authentication mechanisms such as API keys, OAuth, or JWT (JSON Web Tokens).

- If using tokens like JVVT, set appropriate expiration times and implement secure token management practices to prevent token misuse or replay attacks.
- Implement granular access control to limit API access based on user roles and permissions.
- Always validate user credentials and tokens before granting access to sensitive data.

ii. API Gateway and Firewall:

- Employ an API gateway for centralized security enforcement, monitoring, and management.
- Implement web application firewall (WAF) to protect against common web threats.

iii. Data Protection and Secure Communication:

- Encrypt sensitive data using appropriate encryption algorithms and key management.
- Apply data masking techniques to hide sensitive information in logs and responses.
- Use secure communication protocols to prevent eavesdropping and man-in-the-middle attacks.
- Employ secure headers and practices to prevent information leakage.

iv. Input Validation and Sanitization

- All user inputs should be validated and sanitized to prevent injection attacks (e.g., SQL injection, XSS) and parameter manipulation.

v. Output Encoding

- Encode output to protect against HTML/JavaScript injection (XSS) and other data manipulation attacks.

vi. Rate Limiting and Throttling

- Implement rate limiting and throttling mechanisms to prevent abuse of the API and DDoS attacks by limiting the number of requests from a single client within a specific time frame.

vii. Error Handling and Logging

- Ensure proper error handling to avoid exposing sensitive information.

- Implement comprehensive logging for monitoring and auditing purposes.

viii. CORS (Cross-Origin Resource Sharing)

- Configure CORS properly to restrict which domains can access the API from the client-side, thereby preventing unauthorized cross-origin requests.

ix. Secure Storage of Secrets

- Store API keys, credentials, and sensitive data securely using encryption and access controls.

x. Regular Security Assessments

- Conduct regular security assessments of APIs such as penetration testing, security audits and code reviews to identify potential vulnerabilities and security flaws.

xi. Education and Documentation

- Clear documentation should be provided containing steps to use the API securely, including examples of proper authentication and authorization methods.

xii. Privacy Protection

- Minimize data collection and storage to only what is necessary.
- Comply with relevant privacy regulations and obtain user consent for data processing.
- Integrate privacy considerations from the initial stages of API development. Perform a Privacy Impact Assessment (PIA) to identify and mitigate potential privacy risks.

xiii. Secure Development Lifecycle (SDLC)

- Integrate security considerations into the entire API development process.
- Conduct security training for developers to raise awareness of secure coding practices.

t. Strengthening the security of cloud infrastructure

- Enable multi factor authentication of users particularly for cloud, virtual private networks, webmail and accounts that access critical systems.

- Strong password policy should be implemented which includes periodic password expiration. Passwords should not be reused across multiple accounts or stored on the system where an adversary may have access.
- Enable and monitor all logs of events and incidents to identify unusual patterns and behaviours.
- Enforce application whitelisting on all endpoint workstations. This will prevent droppers or unauthorized software from gaining execution on endpoints.
- Check public accessibility of all cloud instances in use. Make sure that no server/bucket is inadvertently leaking data due to inappropriate configurations.
- Ensure proper security of AWS/Azure/GCP access tokens. The tokens should not be exposed publicly in website source code, any configuration files etc.
- Implement appropriate security measures for testing, staging and backup environments hosted on AWS/Azure/GCP. Ensure that the production environment is kept properly segregated from these. Disable/remove older or testing environments if their usage is no longer required.
- Ensure encryption of data at rest and in transit
- Implement least privilege principle for access control with granular permission to cloud resources.
- It must be noted that cloud service providers follow a model wherein a number of security aspects are the customer's responsibility. It is advised to be thoroughly aware of these and implement appropriate security policies and controls.
- Carry out vulnerability Assessment and Penetration Testing (VAPT) and information security audit of critical servers from CERT-In empanelled auditors. Conduct red-team exercises and repeat such audits/exercises at regular intervals.

u. Strengthening the cyber security of the websites and digital infrastructure

- Web application should rely on server-side access control rather than client-side.
- Encrypt the parameter values passed in the **http** requests.
- Ensure that all Websites and Applications are **“https”** enabled with a valid SSL/TLS Certificate.

- Implement rate limiting for the number of requests processed from a single IP address.
- Limit exposure of the APIs to internet i.e. route API calls through application calls only.
- Session timeouts should be set to the minimum value possible based on the sensitivity of the data and the application's risk profile. Timeouts and expiration should be enforced on both the client and the server sides.
- Block the malicious domains/IPs after diligently verifying them without impacting the operations. CERT-In advisories which are published periodically should be referred for latest malicious domains/I Ps.
- Application security testing, vulnerability assessment and penetration testing, should be performed at a frequency determined by sensitivity of the information handled by applications (at least once in a year or whenever there is change in application).
- Implement measures for securing Application Program Interfaces (APIs). Include API security in Vulnerability Assessment and Penetration Testing and mitigate vulnerabilities in APIs.

4.1.4 Detect

The Regulated Entity (RE) shall develop and implement capabilities to detect cybersecurity events in a timely manner and shall:

a. Log Management

- Ensure storage of all types of logs pertaining to the systems are maintained for a rolling period of 180 days.

b. Security Operation Centre

- Establish appropriate security mechanism through Security Operation Centre (SOC) [RE’s own SOC or a managed SOC] for continuous monitoring of security events and timely detection of anomalous activities.

4.1.5 Respond

Take action to mitigate the impact of cybersecurity incidents and restore normal operations

a. Cyber Crisis Management Plan

- Put in place Cyber Crisis Management Plan (CCMP) and which shall encompass incident detection and monitoring, swift containment, and mitigation measures to prevent further damage. Recovery and remediation efforts focus on restoring systems and services, followed by continuous training and improvement initiatives to enhance organizational resilience shall be part of such a policy.

b. Cyber Incident Response and Recovery Management

- There shall be a cyber incident response and recovery management policy and which shall address the classification and assessment of incidents; include a clear communication strategy and plan to manage such incidents, contain exposures and achieve timely recovery.
- REs shall analyze cyber incidents (including through forensic analysis, if necessary) for their severity, impact and root cause. REs shall take measures, corrective and preventive, to mitigate the adverse impact of incidents on business operations.
- REs shall have written incident response and recovery procedures including identification of key roles of staff/ outsourced staff handling such incidents.
- Have clear communication plans for escalation and reporting the cyber incidents to the Board and Senior Management as well as to customers, as required. Also, pro-actively notify CERT-In and the regulator regarding cyber incidents, as per defined regulatory requirements.

4.1.6 Recover

Develop and implement plans to restore capabilities and services affected by cybersecurity incidents

a. Business Continuity Plan (BCP) and Disaster Recovery Management (DRM)

- There shall be a BCP and DR policy and which shall adopt best practices to guide its actions in reducing the likelihood or impact of the disruptive incidents and maintaining business continuity. The business continuity and disaster recovery plans should be prepared and tested at least on an annual basis.
- RE's BCP/ DR capabilities shall be designed to effectively support its resilience objectives and enable it to rapidly recover and securely resume its critical operations (including security controls) post cyber-attacks/ other incidents.

- Periodicity of DR drills for critical information systems shall be at least on a half yearly basis and for other information systems, as per RE's risk assessment. The DR testing shall involve switching over to the DR / alternate site and thus using it as the primary site for sufficiently long period where usual business operations of at least a full working day (including Beginning of Day to End of Day operations) are covered.
- Up-to-date backups of all critical items i.e., Data files, Utilities programmes, Databases, Operating system software, Applications system software, Encryption keys, Pre-printed forms, Device configurations, etc., should be maintained to ensure the continued provision of the minimum essential level of service.
- One set of the original disks for all operating system and application software should be maintained to ensure that a valid, virus-free backup exists and is available for use at any time.
- Backups of the system, application and data should be performed on a regular basis as per the DR and BCP policy of the Regulated Entity (RE)s. Backups should also be made for application under development and data conversion efforts.
- Data backup is required for all systems which are deemed critical for the Regulated Entity (RE) including personal computers, servers and distributed systems, databases, network, security equipment.
- Critical system data and file server software should have incremental backups taken daily. Based on the criticality of the applications hourly/concurrent backup can also be considered based on the BCP policy of the Regulated Entity (RE).
- Regularly test and verify the integrity of backup data to ensure it can be restored successfully. Regularly review and audit access to backup data.

4.2 Cyber security audits

- Regulated Entities (REs) shall ensure that
  - REs shall put in place an Information Security (IS) Audit Policy. The IS Audit Policy shall contain a clear description of its mandate, purpose, authority, audit universe, periodicity of audit etc. The policy shall be approved by the Audit Committee of the Board / Risk Management Committee.

- The regulated entities / intermediaries shall conduct an internal and external audit of the entire ICT infrastructure and the external audit shall be through a CERT-In empaneled cybersecurity auditor at least once in a financial year. A security audit shall be conducted as and when any changes are made in the source code and any vulnerabilities observed during the audit should be remedied on priority. Internal security audit shall be performed at least once in 6 months or the audit done for the purposes of ISO certifications in the said period of 6 months may also be considered for the purpose.

4.3 Capacity Management

- Regulated Entity's (RE's) shall ensure that information systems and infrastructure are able to support business functions and ensure availability of all service delivery channels and which shall include human resources.
- REs shall ensure that IT capacity planning across components, services, system resources, supporting infrastructure is consistent with past trends (peak usage), the current business requirements and projected future needs as per the IT strategy of the Regulated Entity's (RE's).

4.4 Audit Trails

- Regulated Entity's (RE's) shall ensure that every IT application which can access or affect critical or sensitive information, shall have necessary audit and system logging capability and should provide audit trails. Regulated Entity's (RE's) shall put in place a system for regularly monitoring the audit trails and system logs to detect any unauthorized activity.
- The audit trails must be detailed enough to facilitate the conduct of audit, serve as forensic evidence when required and assist in dispute resolution, including for non-repudiation purposes.

4.5 Reporting of Cyber incidents

a. **Reporting to CERT-In:**

- A Regulated Entity (RE) shall mandatorily report cyber incidents as mentioned below to CERT-In and PFRDA within 6 hours of noticing such incidents or being brought to notice about such incidents. The incidents can be reported to CERT-In via email (incident@CERT-In.org.in) or any other medium permitted by

CERT-In. This shall be applicable to both Category I and Category II Regulated Entities (Refer point no: 2.2 of these guidelines) The details regarding methods and formats of reporting cyber security incidents are also published on the website of CERT-In (www.CERT-In.org.in). For PFRDA, such reporting shall be done by the compliance officer to the supervisory department dealing with the RE at the regulator.

- Types of cyber security incidents mandatorily to be reported by Regulated Entity (RE)s to CERT-In shall be as follows: [Refer Rule 12(1)(a) of The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013].
    - Targeted scanning/probing of critical networks/systems
    - Compromise of critical systems/information; Unauthorized access of IT systems/data
    - Defacement of website or intrusion into a website and unauthorized changes such as inserting malicious code, links to external websites etc.
    - Malicious code attacks such as spreading of virus/worm/Trojan/Bots/ Spyware/Ransomware/Crypto miners
    - Attack on servers such as Database, Mail and DNS and network devices such as Routers
    - Identity Theft, spoofing and phishing attacks
    - Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
    - Attacks on Critical infrastructure, SCADA and operational technology systems and Wireless networks
    - Attacks on Application such as E-Governance, E-Commerce etc.
    - Data Breach, Data Leak
    - Attacks on Internet of Things (IoT) devices and associated systems, networks, software, servers
    - Attacks or incident affecting Digital Payment systems
    - Attacks through Malicious mobile Apps, Fake mobile Apps
    - Unauthorized access to social media accounts
    - Attacks or malicious/ suspicious activities affecting Cloud computing systems/servers/software/applications
    - Attacks or malicious/suspicious activities affecting systems/ servers/ networks/ software/ applications related to Big Data, Block chain, virtual

assets, virtual asset exchanges, custodian wallets, Robotics, 3D and 4D Printing, additive manufacturing, Drones

- Attacks or malicious/ suspicious activities affecting systems/ servers/software/ applications related to Artificial Intelligence and Machine Learning

b. **Reporting to PFRDA**

Category I entities (Refer point no: 2.2)

- All incidents that have been reported to CERT-In shall be reported to PFRDA on a quarterly basis along with the remedial actions taken.
- A specific report on the incidents (in addition to the reporting done to CERT-In and PFRDA as mentioned at 4.5(a) above) that in the opinion of the Regulated Entity have an impact on subscribers and other stakeholders shall be made to PFRDA within 48 hours of occurrence of any such incident.
- An annual compliance reporting shall be made to PFRDA on compliance of the Cybersecurity guidelines along with the Board approved “Information and Cybersecurity Policy” within 30 days from the close of the financial year.

Category II entities (Refer point no: 2.2)

- An annual compliance reporting shall be made to PFRDA on compliance of the Cybersecurity guidelines along with the Board approved “Information and Cybersecurity Policy” within 30 days from the close of the financial year.
- The compliance report shall contain a certification by the compliance officer that
  - the principal regulator has been notified of the incidents that have occurred and in terms of the Information and Cybersecurity policy of the principal regulator (such as RBI/SEBI/IRDAI/NHB) and as mentioned at point 4.5 (a) above.
  - The Cyber Security audits have been conducted according to the principal regulator’s guidelines and as applicable. The necessary remedial actions have been undertaken on the basis of the Cyber security that has been undertaken.