परिपत्र सं.:पीएफआरडीए/2025/05/आईसीएस/01 **04.09.2025**

परिपत्र

सेवा में
सभी मध्यस्थ एवं विनियमित संस्थाएँ

विषय: साइबर सुरक्षा घटनाओं के वर्गीकरण संबंधी दिशा-निर्देश

1. यह परिपत्र सं. PFRDA/24/14/ICS/01 दिनांक 01.08.2024 से संबद्ध है, जो मध्यस्थों/विनियमित संस्थाओं हेतु सूचना एवं साइबर सुरक्षा नीति दिशा-निर्देश – 2024 से संबंधित है।
2. उक्त दिशा-निर्देशों में पीएफआरडीए के अधीन विनियमित संस्थाओं एवं मध्यस्थों के लिए साइबर घटनाओं एवं प्रत्युत्तर प्रबंधन की व्यापक रूपरेखा दी गई है। साथ ही, घटनाओं का प्रभावी प्रबंधन सुनिश्चित करने हेतु उनका उचित प्राथमिकता निर्धारण अत्यंत आवश्यक है।
3. विनियमित संस्थाओं/मध्यस्थों को परिशिष्ट-I में संलग्न दिशा-निर्देशों के आधार पर घटनाओं का उपयुक्त वर्गीकरण एवं प्राथमिकता निर्धारण सुनिश्चित करने की सलाह दी जाती है।
4. यह परिपत्र पेंशन निधि विनियामक और विकास प्राधिकरण अधिनियम, 2013 की धारा 14 के अंतर्गत प्रदत्त शक्तियों के अधीन जारी किया जाता है।

कविता सिंगम ज़ेवियर

महाप्रबंधक
सूचना एवं साइबर सुरक्षा विभाग

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

Circular No.: PFRDA/2025/05/ICS/01 **04.09.2025**

CIRCULAR

To
All Intermediaries & Regulated entities

Subject: Guidelines on Classification of Cybersecurity Incidents

1. This is with reference to the circular no PFRDA/24/14/ICS/01 dated 01.08.2024 pertaining to Information & Cyber Security Policy Guidelines – 2024 for intermediaries/Regulated Entities.

2. The said section outlines broad framework for Cyber Incident and Response Management for REs & Intermediaries under PFRDA. Further, in order to effectively manage the incidents, proper prioritization of incidents is crucial.

3. REs/Intermediaries are advised to ensure appropriate classification and prioritization of incidents based on guidelines attached as Annexure I.

4. This circular is issued in exercise of the powers conferred under Section 14 of the Pension Fund Regulatory and Development Authority Act, 2013.

Kavita Singam Xavier

General Manager
Information & Cyber Security Department

ई–500, टॉवर–ई, पांचवां तल, वर्ल्ड ट्रेड सेंटर, नौरोजी नगर, नई दिल्ली–110029
दूरभाषः 91–11–40717900, वेबसाइटः www.pfrda.org.in
E-500, Tower-E, Fifth Floor, World Trade Center, Nauroji Nagar, New Delhi-110029
Phone: 91-11-40717900, Website: www.pfrda.org.in

Annexure I

Guidelines on Classification of Cybersecurity Incidents

1. It is to inform that Section 4.1.5 of Information & Cyber Security Policy Guidelines – 2024 for Intermediaries/Regulated Entities dt 01.08.2024 issued by Authority outlines broad framework for Cyber Incident and Response Management for REs & Intermediaries under PFRDA. However, the classification of incidents is not part of the existing policy.

2. Security incidents may impact the confidentiality, integrity, and availability of an organization's information. Prioritizing the response to such incidents is one of the most critical aspects of the incident handling process.

3. It is advised that incidents be addressed based on their priority, rather than on a first-come, first-served basis. Regulated Entities (REs) should determine the response priority by assessing the potential business impact and the estimated effort required for recovery, rather than the ease of recoverability.

4. REs/Intermediaries should assess the impact of an incident on the current functionality of the affected systems. In addition to evaluating the immediate functional disruption, REs should also consider the potential future impact if the incident is not promptly contained.

5. REs/Intermediaries may classify Cybersecurity incidents into the following four categories. The parameters for classification of the incidents are as follows:

S. No.	Category	Parameters
1	Critical	Cyber incidents of critical nature (such as successful penetration or Denial of Service attacks detected with significant impact on operations; ransomware attack; exfiltration of sensitive data; widespread instances of data corruption causing impact on operations; significant risk of negative financial or public relations impact, etc.) on any part of IT infrastructure.
2	High	Penetration or Denial of Service attacks attempted with limited impact on operations; widespread instances of a new malwares not handled by anti-virus software; unauthorized access to servers and network devices; unauthorized or unexpected configuration changes on network devices detected; data exfiltration; unusually high count of phishing emails; instances of outbound phishing emails; some risk of negative financial or public relations impact, etc.

3	Medium	Target recon or scans detected; penetration or Denial of Service attacks attempted with no impact on operations; widespread instances of known malwares easily handled by antivirus software; isolated instances of a new malwares not handled by anti-virus software; instances of phishing emails that were not recognized by employees and were clicked by them; instances of data corruption, modification and deletion being reported, etc.
4	Low	System probes or scans detected on external systems; intelligence received concerning threats to which systems may be vulnerable; intelligence received regarding username password compromise; isolated instances of known malwares easily handled by antivirus software, etc.

6. Any cyber incident that results in disruption, stoppage or variance in the normal functions/ operations of systems of the entity thereby impacting normal/ regular service delivery and functioning of the entity, must be classified as High or Critical incident.

7. REs/Intermediaries to ensure timely and effective response to incidents, consistent with the principles of operational resilience and continuity of critical functions.

****