

परिपत्र

परिपत्र संख्या: पीएफआरडीए/2023/33/आईसिएस/01

23 नवम्बर 2023

पीएफआरडीए के साथ पंजीकृत सभी मध्यस्थों के लिए

महोदया / महोदय,

**विषय: पीएफआरडीए द्वारा विनियमित मध्यस्थों द्वारा क्लाउड सेवाओं को अपनाने के सम्बन्ध में**

यह परिपत्र पीएफआरडीए अधिनियम, 2013 की धारा 14 (1) के साथ धारा 14 (2) खंड (क) के तहत प्रदत्त शक्तियों का प्रयोग करते हुए और अभिदाताओं के हितों की रक्षा के लिए जारी किया गया है। यह परिपत्र मध्यस्थों द्वारा प्रदान की जा रही सेवाओं के लिए मध्यस्थों द्वारा क्लाउड सेवाओं को अपनाने पर एक नीतिगत ढांचे के साथ मध्यस्थों को सक्षम और समर्थ करने के लिए जारी किया जा रहा है। नीति में मध्यस्थों द्वारा विनियामक और कानूनी आवश्यकताओं और अनुपालन को भी निर्धारित किया गया है, यदि वे क्लाउड सेवाओं को अपनाते हैं।

1. पीएफआरडीए के साथ पंजीकृत मध्यस्थ अपने व्यापार मॉडल और अपने अभिदाताओं को पेश किए जाने वाले उत्पादों और सेवाओं का समर्थन करने के लिए क्लाउड सेवाओं को अपनाने सहित सूचना प्रौद्योगिकी (आईटी) और आईटी सक्षम सेवाओं (आईटीईएस) का बड़े पैमाने पर लाभ उठा रहे हैं।
2. वित्तीय सेवा क्षेत्र में आईटी सेवाओं को वितरित करने के लिए क्लाउड सेवाओं को अपनाना बढ़ रहा है और सरकार द्वारा विभिन्न पहलों के माध्यम से भी प्रोत्साहित किया जा रहा है। जबकि क्लाउड समाधान अनेक लाभ प्रदान करते हैं जैसे कि रेडी टू स्केल, तैनाती में आसानी, भौतिक बुनियादी ढांचे को बनाए रखने का कोई ओवरहेड आदि नहीं, यह साइबर सुरक्षा जोखिमों और चुनौतियों को भी बढ़ाता है।
3. पीएफआरडीए ने इससे पहले आउटसोर्सिंग गतिविधियों पर अपने परिपत्र संख्या पीएफआरडीए/2016/4/सीआरए/टीबी/2 दिनांक 29/01/2016 के माध्यम से केंद्रीय अभिलेखपाल

अभिकरणों के लिए और पेंशन निधियों के लिए अपने परिपत्र सं पीएफआरडीए/2017/30/पीएफ/4 दिनांक.09/10/2017 के माध्यम से दिशा-निर्देश जारी किए हैं, जो मूल रूप से दिन-प्रतिदिन की गतिविधियों के प्रबन्धन से सम्बन्धित हैं और आईटी से संबंधित आउटसोर्सिंग गतिविधियों को सम्मिलित नहीं करते हैं।

4. उपर्युक्त को ध्यान में रखते हुए, प्राधिकरण जोखिमों को प्रभावी ढंग से संबोधित करने और विनियामक अनुपालन सुनिश्चित करने के लिए पंजीकृत मध्यस्थों द्वारा क्लाउड सेवाओं को अपनाने पर एक ढांचा या नीति तैयार करता है। उक्त नीति संदर्भित आउटसोर्सिंग दिशानिर्देशों के अतिरिक्त होगी और क्लाउड सेवाओं को अपनाने को पंजीकृत मध्यस्थों द्वारा गतिविधियों की आउटसोर्सिंग के अंतर्गत माना जाएगा।

5. जिन मध्यस्थों ने पहले ही क्लाउड सेवाओं को अपना लिया है या अपनाएंगे, उन्हें सलाह दी जाती है कि वे संलग्न की गई नीति का अनुपालन सुनिश्चित करें।

यह परिपत्र सक्षम प्राधिकारी के अनुमोदन से जारी किया जाता है।

भवदीय,

के. आर. दौलत  
(के.आर. दौलत अली खान)

महाप्रबंधक

सूचना और साइबर सुरक्षा विभाग

**पीएफआरडीए द्वारा विनियमित मध्यस्थों द्वारा क्लाउड सेवाओं को अपनाने की नीति:**

पृष्ठभूमि:

पीएफआरडीए के साथ पंजीकृत मध्यस्थ अपने व्यापार मॉडल और अपने अभिदाताओं को दिए जाने वाले उत्पादों और सेवाओं का समर्थन करने के लिए क्लाउड सेवाओं को अपनाने सहित सूचना प्रौद्योगिकी (आईटी) और आईटी सक्षम सेवाओं (आईटीईएस) का बड़े पैमाने पर लाभ उठा रहे हैं। इसके अलावा, मध्यस्थों द्वारा पीएफआरडीए से एनपीएस, एपीवाई और अन्य पेंशन योजनाओं से जुड़े डेटा और संबंधित अनुप्रयोगों के भंडारण के लिए क्लाउड सेवाओं को अपनाने की अनुमति देने के लिए कई अनुरोध किए गए हैं।

हाल के दिनों में आईटी सेवाओं को वितरित करने के लिए क्लाउड सेवाओं को अपनाने में वृद्धि हो रही है और सरकार द्वारा विभिन्न पहलों के माध्यम से भी प्रोत्साहित किया जा रहा है। जबकि क्लाउड समाधान कई लाभ प्रदान करते हैं जैसे कि रेडी टू स्केल, तैनाती में आसानी, भौतिक बुनियादी ढांचे को बनाए रखने का कोई ओवरहेड आदि नहीं, ऐसी तकनीक को अपनाने वाली संस्थाओं को नए साइबर सुरक्षा जोखिमों और चुनौतियों के बारे में भी पता होना चाहिए जो क्लाउड समाधान पेश करते हैं।

पीएफआरडीए ने इससे पहले अपने परिपत्र संख्या पीएफआरडीए/2016/4/सीआरए/टीबी/2 दिनांक 29.01.2016 के माध्यम से केंद्रीय रिकॉर्ड कीपिंग एजेंसियों के लिए गतिविधियों की आउटसोर्सिंग पर दिशा-निर्देश जारी किए हैं और पेंशन निधियों के लिए अपने परिपत्र सं. पीएफआरडीए/2017/30/पीएफ/4 दिनांक 09/10/2017 के माध्यम से पेंशन निधियों के लिए दिशा-निर्देश जारी किए हैं। ये मूल रूप से दिन-प्रतिदिन के संचालन पर नीति के लिए थे और आईटी और आईटीईएस से संबंधित आउटसोर्सिंग गतिविधियों को विस्तार से सम्मिलित नहीं करते हैं। इसके अलावा, सीआरए, पीएफ आदि जैसे मध्यस्थों के लिए प्राधिकरण द्वारा जारी पंजीकरण दिशानिर्देशों में क्लाउड कंप्यूटिंग जैसी उभरती प्रौद्योगिकियों को अपनाने का भी प्रावधान है।

उपर्युक्त को ध्यान में रखते हुए, प्राधिकरण ने मौजूदा व्यवस्थाओं की समीक्षा करने के बाद जोखिमों को प्रभावी ढंग से संबोधित करने और विनियामक अनुपालन सुनिश्चित करने के लिए पंजीकृत मध्यस्थों द्वारा क्लाउड सेवाओं को अपनाने पर एक रूपरेखा या नीति तैयार करने



का निर्णय लिया है। उक्त नीति संदर्भित आउटसोर्सिंग दिशानिर्देशों के अतिरिक्त होगी और क्लाउड सेवाओं को अपनाने को पंजीकृत मध्यस्थों द्वारा गतिविधियों की आउटसोर्सिंग के अंतर्गत माना जाएगा।

### 1. प्रयोज्यता

इस नीति के प्रावधान पीएफआरडीए के सभी पंजीकृत मध्यस्थों पर लागू होंगे।

### 2. परिभाषाएँ : जब तक कि अन्यथा संदर्भ आवश्यक न हो, इस नीति के उद्देश्य के लिए;

- i. बीसीपी : बिज़नेस कंटीन्यूटी प्लान (व्यापार निरंतरता योजना)
- ii. सीआईएसओ : चीफ इन्फोर्मेशन सिक्योरिटी ऑफिसर (मुख्य सूचना सुरक्षा अधिकारी)
- iii. क्लाउड सेवाएं : ऐसे बुनियादी ढांचा, प्लेटफॉर्म या सॉफ्टवेयर जो तृतीय-पक्ष प्रदाताओं द्वारा होस्ट किए जाते हैं और इंटरनेट के माध्यम से अभिदाताओं को उपलब्ध कराए जाते हैं, जिसमें क्लाउड कंप्यूटिंग अन्तर्निहित है।
- iv. क्लाउड कंप्यूटिंग : क्लाउड कंप्यूटिंग कॉन्फ़िगर करने योग्य कंप्यूटिंग संसाधनों (जैसे, नेटवर्क, सर्वर, स्टोरेज, एप्लिकेशन और सेवाओं) के साझा पूल तक सर्वव्यापी, सुविधाजनक, ऑन-डिमांड नेटवर्क पहुंच को सक्षम करने के लिए एक मॉडल है, जिसे न्यूनतम प्रबंधन प्रयास या सेवा प्रदाता इंटरैक्शन के साथ तेजी से प्रावधान करके जारी किया जा सकता है- (जैसा एनआईएसटी (नेशनल इंस्टीट्यूट ऑफ स्टैंडर्ड्स एंड टेक्नोलॉजी - यूएस) द्वारा परिभाषित किया गया है)।
- v. सीएसपी : क्लाउड सेवा प्रदाता ।
- vi. मध्यस्थ : इसमें पीएफआरडीए अधिनियम, 2013 के संदर्भ में पेंशन निधि, केंद्रीय अभिलेखपाल अभिकरण, राष्ट्रीय पेंशन प्रणाली न्यास और उपस्थिति अस्तित्व शामिल हैं।
- vii. एसओसी : सुरक्षा संचालन केंद्र

**3. उद्देश्य :** नीति का अंतर्निहित सिद्धांत, तकनीकी प्रगति को अपनाने के लिए एक ढांचा तैयार करना है ताकि मध्यस्थ यह सुनिश्चित कर सके कि क्लाउड सेवाओं जैसी तकनीकी प्रगति को अपनाने से न तो अभिदाताओं के प्रति उनके दायित्वों को पूरा करने की क्षमता में कमी आती हो और न ही आगत जोखिमों के उचित मूल्यांकन के साथ प्राधिकरण द्वारा प्रभावी पर्यवेक्षण में बाधा उत्पन्न होती हो। क्लाउड सेवाओं या अन्य आईटी सक्षम सेवाओं को अपनाने समय मध्यस्थ यह सुनिश्चित करने के लिए कदम उठाएगा कि सेवा प्रदाता सेवाओं को

निष्पादित करने में उसी उच्च मानक को ध्यान में रखें जैसा कि, उसी गतिविधि को आउटसोर्स न करने पर मध्यस्थ द्वारा नियोजित करने की दशा में किया गया होता ।

#### 4. क्लाउड सेवाएं

आजकल कई ऐसे लोकप्रिय क्लाउड परिनियोजन और सेवा-मॉडल हैं जो समय के साथ उभरे हैं। ये आम तौर पर प्रौद्योगिकी स्टैक की उस सीमा पर आधारित होते हैं जिसे उपभोक्ता इकाई द्वारा अपनाया जाना प्रस्तावित होता है। इनमें से प्रत्येक मॉडल संबंधित सेवा, व्यावसायिक लाभ और जोखिम प्रोफाइल के साथ आते हैं। मध्यस्थ अपने कार्यों के निर्वहन के लिए क्लाउड सेवाओं को अपनाते समय निम्नलिखित की जांच करें :

क. क्लाउड समाधान अपनाने पर विचार करते समय, वर्तमान आईटी अनुप्रयोगों के पदचिह्न और संबंधित लागतों के लिए अपनाई गई व्यावसायिक रणनीति और लक्ष्यों का विश्लेषण करना अनिवार्य है। क्लाउड अपनाने में केवल गैर-व्यावसायिक महत्वपूर्ण कार्यभार को क्लाउड पर ले जाने से लेकर एसएएस अपनाने जैसे महत्वपूर्ण व्यावसायिक अनुप्रयोगों और बीच में कई संयोजनों को स्थानांतरित करना भी शामिल है, जो व्यवसाय प्रौद्योगिकी जोखिम मूल्यांकन पर आधारित हो।

ख. क्लाउड सेवाओं को संलग्न करने में, मध्यस्थों को अन्य बातों के साथ-साथ यह भी सुनिश्चित करना होगा कि ऐसी आउटसोर्सिंग आंकड़ों के संपूर्ण जीवनचक्र को संबोधित करती हो, अर्थात्, डेटा के निर्माण से लेकर क्लाउड में इसके प्रवेश तक की पूरी अवधि को कवर करती हो, जब तक कि डेटा स्थायी रूप से मिटा या हटा नहीं दिया जाता । मध्यस्थ यह सुनिश्चित करेगा कि निर्दिष्ट प्रक्रियाएं व्यावसायिक आवश्यकताओं , कानूनी और विनियामक आवश्यकताओं के अनुरूप हों।

ग. क्लाउड सेवाओं को अपनाने में, मध्यवर्ती उचित जोखिम प्रबंधन ढांचा स्थापित करते समय क्लाउड सेवा विशिष्ट कारकों, जैसे मल्टी-टेनेंसी, डेटा के मल्टी-लोकेशन भंडारण/प्रसंस्करण तथा आगत जोखिमों आदि को ध्यान में रखें।

घ. क्लाउड गवर्नेंस : मध्यस्थों द्वारा एक अच्छी तरह से स्थापित और प्रलेखित क्लाउड रखने की नीति को अपनाना और प्रदर्शित करना होगा। इस तरह की नीति द्वारा अन्य बातों के साथ-साथ उन गतिविधियों की पहचान भी करनी होगी जिन्हें क्लाउड पर स्थानांतरित किया जा सकता है, तथा विभिन्न हितधारक हितों की सुरक्षा को सक्षम और समर्थन प्रदान करना होगा, डेटा वर्गीकरण के साथ संरेखित गोपनीयता, सुरक्षा, डेटा संप्रभुता, पुनर्प्राप्ति और डेटा भंडारण आवश्यकताओं सहित विनियामक आवश्यकताओं का अनुपालन सुनिश्चित करना होगा।



नीति में सीएसपी से जुड़े जोखिमों के प्रबंधन और सतत निगरानी के लिए उचित सावधानी बरतनी होगी ।

#### 5. मध्यस्थों द्वारा क्लाउड सेवाओं को अपनाने के लिए नीति और सिद्धांत

क्लाउड सेवाओं को अपनाने के लिए प्राधिकरण के सभी पंजीकृत मध्यस्थों द्वारा अनुपालन की जाने वाली व्यापक नीति और सिद्धांत निम्नलिखित होंगे :

- क. मध्यस्थ के बोर्ड द्वारा क्लाउड कंप्यूटिंग को अपनाने की आवश्यकता, निहितार्थ (वित्तीय, विनियामक, आदि), जोखिम, लाभ आदि के उचित मूल्यांकन के बाद क्लाउड आधारित सेवाओं को अपनाने के मामले पर निर्णय लेना होगा।
- ख. मध्यस्थ का बोर्ड क्लाउड सेवाओं को अपनाने के संबंध में अपनी उचित जांच करते समय सभी प्रासंगिक कानूनों, विनियमों, नियमों, दिशानिर्देशों और अनुमोदन लाइसेंस या पंजीकरण की शर्तों पर विचार करेगा। संदर्भित उचित परिश्रम के दौरान गुणात्मक, मात्रात्मक, वित्तीय, परिचालन, कानूनी और प्रतिष्ठा संबंधी कारकों को ध्यान में रखेगा। क्लाउड सेवाओं सहित कार्यों की ऐसी आउटसोर्सिंग से संबंधित सभी पहलुओं के लिए जिम्मेदारी और जवाबदेही मध्यस्थ की होगी। इस तरह की जवाबदेही में क्लाउड एप्लिकेशन की उपलब्धता, उसके डेटा और लॉग की गोपनीयता, अखंडता और सुरक्षा शामिल होगी, और मध्यस्थ द्वारा क्लाउड सेवाओं को अपनाने की स्थिति में पीएफआरडीए द्वारा जारी अधिनियम, नियमों, विनियमों, परिपत्रों आदि के संबंध में अनुपालन सुनिश्चित करना होगा।
- ग. बोर्ड सभी संगत कार्यकलापों के उचित मूल्यांकन के पश्चात् एक व्यापक बोर्ड अनुमोदित क्लाउड एडॉप्शन नीति लागू करेगा, जिसमें वरिष्ठ प्रबंधन की भूमिका, सीआईएसओ की भूमिका सहित आईटी कार्य, व्यावसायिक कार्य और क्लाउड सेवाओं को अपनाने के संबंध में निरीक्षण और आश्वासन कार्यों पर स्पष्ट नीति निर्धारित करना शामिल होगा। इसके अलावा सेवा प्रदाताओं के चयन के मानक, इस तरह के अपनाने से संबंधित विभिन्न गतिविधियों के लिए जोखिम और भौतिकता के आधार पर प्राधिकरण का प्रत्यायोजन, डेटा स्थानीकरण, डेटा स्वामित्व, पहुंच, जोखिम मूल्यांकन और क्लाउड सेवा प्रदाताओं (सीएसपी), सुरक्षा नियंत्रण, आपदा रिकवरी नियंत्रण और व्यवसाय निरंतरता योजनाओं के साथ, इन गतिविधियों के संचालन की निगरानी और समीक्षा करने के लिए सिस्टम और समाप्ति प्रक्रियाओं और निकास रणनीतियों तथा विक्रेता लॉक-इन, जिसमें किसी तृतीय-पक्ष सेवा प्रदाता या सीएसपी के व्यवस्था से बाहर निकलने की स्थिति में व्यवसाय निरंतरता को शामिल किया जाएगा। ।

- घ. ऐसी बोर्ड अनुमोदित नीति में क्लाउड सेवाओं को अपनाने के संबंध में लेखा परीक्षा और आश्वासन गतिविधियों का विवरण भी शामिल होगा। लेखापरीक्षा/आवधिक समीक्षा/तृतीय-पक्ष प्रमाणपत्रों में प्रयोज्यता और क्लाउड उपयोग के अनुसार, अन्य बातों के साथ-साथ, क्लाउड प्रशासन, अभिगम और नेटवर्क नियंत्रण, विन्यास, निगरानी तंत्र, डेटा एन्क्रिप्शन, लॉग समीक्षा, परिवर्तन प्रबंधन, घटना अनुक्रिया और लचीलापन की तैयारी और परीक्षण आदि में मध्यस्थ और सीएसपी दोनों की भूमिकाओं और जिम्मेदारियों जैसे पहलुओं को शामिल किया जाना चाहिए।
- ड. क्लाउड में किसी भी रूप में मध्यस्थ से संबंधित लॉग और किसी भी अन्य डेटा सहित डेटा (डीसी, डीआर, नियर डीआर आदि) का भंडारण / प्रसंस्करण भारत की विधिक सीमाओं के भीतर रहना चाहिए/ संसाधित किया जाना चाहिए। डेटा का संग्रह और प्रसंस्करण भारत के कानूनों और नीतियों द्वारा शासित होना चाहिए और समय-समय पर मंत्रालयों / विभागों और सरकारी एजेंसियों द्वारा जारी विभिन्न विनियमों, दिशानिर्देशों के अनुपालन में होना चाहिए। इसके अलावा, डेटा को वैध एसटीक्यूसी (या भारत सरकार द्वारा नियुक्त किसी अन्य समकक्ष एजेंसी) ऑडिट स्थिति रखने वाले एमईआईटीवाई (Meity) द्वारा सूचीबद्ध क्लाउड सेवा प्रदाताओं के डेटा केंद्रों के भीतर निवास/संसाधित किया जाना चाहिए।
- च. मध्यस्थ, क्लाउड में रहने वाले अपने डेटा और संबंधित डेटा, एन्क्रिप्शन कुंजी, लॉग आदि का पूर्ण स्वामित्व बनाए रखेगा।
- छ. मध्यस्थ और सीएसपी के बीच क्लाउड सेवाओं की सभी गतिविधियों (तकनीकी, प्रबंधकीय, शासन से संबंधित आदि शामिल, लेकिन सीमित नहीं) के संबंध में जिम्मेदारियों का एक स्पष्ट चित्रण / सीमांकन होगा। आदर्श रूप से, मध्यस्थ और सीएसपी के बीच किसी भी कार्य / क्रिया / गतिविधि के लिए कोई "साझा जिम्मेदारी" या "संयुक्त स्वामित्व" नहीं होगा। यदि मध्यस्थ और सीएसपी द्वारा संयुक्त रूप से कोई कार्य/क्रिया/गतिविधि की जानी है, तो कार्य के भीतर प्रत्येक उप-कार्य/लाइन-आइटम के लिए जिम्मेदारी का स्पष्ट चित्रण और निर्धारण किया जाएगा। जिम्मेदारियों के उपर्युक्त चित्रण को मध्यस्थ और सीएसपी के बीच हस्ताक्षरित समझौते में स्पष्ट रूप से जोड़ा जाएगा। उदाहरण के लिए, क्लाउड में रहने वाले डेटा की सुरक्षा अंतिम उपयोगकर्ता की जिम्मेदारी होगी और क्लाउड इंफ्रास्ट्रक्चर स्तर की सुरक्षा क्लाउड सेवा प्रदाता (सीएसपी) की जिम्मेदारी होगी।
- ज. मध्यस्थों को यह सुनिश्चित करना होगा कि क्लाउड-आधारित अनुप्रयोगों का समर्थन करने वाली सेवा और प्रौद्योगिकी संरचना विश्व स्तर पर मान्यता प्राप्त संरचना सिद्धांतों और मानकों के अनुपालन में बनाई गई हो। मध्यस्थ एक ऐसी प्रौद्योगिकी



संरचना को प्राथमिकता देंगे जो सुरक्षित कंटेनर-आधारित डेटा प्रबंधन प्रदान करता हो , जहां एन्क्रिप्शन कुंजी और हार्डवेयर सुरक्षा मॉड्यूल मध्यस्थ के नियंत्रण में हों। मल्टी टेनेंसी वातावरण को डेटा अखंडता और गोपनीयता जोखिमों के खिलाफ और डेटा के सह-मिलान के खिलाफ संरक्षित किया जाना चाहिए। संरचना की सुचारू रिकवरी को सक्षम करना चाहिए और क्लाउड संरचना में किसी भी एक या घटकों के संयोजन की किसी भी विफलता के परिणामस्वरूप डेटा / सूचना सुरक्षा से समझौता नहीं किया जाना चाहिए।

- झ. क्लाउड सेवा प्रबंधन और सुरक्षा विचार : मध्यस्थ, क्लाउड सेवा प्रबंधन और सुरक्षा के संबंध में **अनुलग्नक 1** में दिए गए विषय और मामलों को ध्यान में रखेगा और यह सुनिश्चित करेगा कि उनका अनुपालन किया जाए।
- ञ. मध्यस्थ साइबर सुरक्षा, मापनीयता, अखंडता और सिस्टम के लचीलेपन को ध्यान में रखते हुए सिस्टम और क्लाउड संरचना के सेटअप, संरचना को अंतिम रूप देगा और पीएफआरडीए किसी भी तरह से ऐसे कॉन्फिगरेशन के कार्यात्मक या परिचालन दक्षता या तकनीकी पहलुओं के लिए जिम्मेदार नहीं होगा।
- ट. मध्यस्थ केवल सीएसपी के साथ एक अनुबंध में प्रवेश करेंगे, जो उन क्षेत्राधिकारों के अधीन हैं जो भारतीय कानूनों के तहत किए गए समझौतों की प्रवर्तनीयता और मध्यस्थों को उपलब्ध कराए गए अधिकारों को बनाए रखते हैं, जिनमें डेटा भंडारण, डेटा संरक्षण और गोपनीयता जैसे पहलुओं से संबंधित अधिकार शामिल हैं।
- ठ. मध्यस्थ यह सुनिश्चित करेंगे कि उनके अधिकार और दायित्व और क्लाउड सेवा प्रदाताओं (सीएसपी) को स्पष्ट रूप से परिभाषित किया गया है और कानूनी रूप से बाध्यकारी लिखित समझौते में निर्धारित किया गया है। सिद्धांत रूप में, समझौते के प्रावधानों को मध्यस्थ के व्यवसाय, संबंधित जोखिमों और उन्हें कम करने या प्रबंधित करने के लिए रणनीतियों हेतु आउटसोर्स किए गए कार्य के महत्व को उचित रूप से मानना चाहिए। मध्यस्थ को क्लाउड सेवाओं के संबंध में सभी गतिविधियों पर पर्याप्त नियंत्रण बनाए रखने और कानूनी और विनियामक दायित्वों को पूरा करने के लिए उचित उपायों के साथ हस्तक्षेप करने का अधिकार देने के लिए यह समझौता पर्याप्त लचीला बनाया जाएगा।
- ड. मध्यस्थ के पास घटना प्रबंधन नीति, प्रक्रियाएं और प्रणालियाँ होंगी। मध्यस्थ क्लाउड में की जा रही तैनाती के लिए उसी का अनुपालन करेगा।
- ढ. उपर्युक्त संदर्भित करार में अन्य बातों के साथ-साथ यह सुनिश्चित किया जाएगा कि इसमें निम्नलिखित पहलुओं को शामिल किया जाए:



- i. सूचना प्रौद्योगिकी अधिनियम के प्रावधानों, अन्य लागू कानूनी अपेक्षाओं और अभिदाता डेटा की सुरक्षा के लिए मानकों का अनुपालन;
- ii. सेवाओं का दायरा, सेवाओं के लिए शुल्क और अभिदाता के डेटा की गोपनीयता बनाए रखना, क्लाउड सेवाओं की उपलब्धता, प्रदर्शन, सुरक्षा, आपदा रिकवरी और डेटा बैकअप प्रबंधन, आदि जैसे विवरण,
- iii. सेवा स्तरों की गुणवत्ता और मात्रा और अन्य प्रासंगिक मुद्दों को मापने के लिए प्रदर्शन मानकों को औपचारिक रूप देने वाले सेवा-स्तरीय समझौतों (एसएलए) सहित वितरण; एसएलए में निकास कार्यनीति और सेवा स्तर की शर्तों में, अन्य बातों के साथ-साथ, निम्नलिखित को ध्यान में रखा जाएगा:
  1. अनुबंध की अवधि;
  2. सीएसपी द्वारा आयोजित मध्यस्थ की सेवा संपार्श्विक (Collateral) और डेटा वापसी के लिए सहमत प्रक्रियाएं और नियतकालिक समय;
  3. डेटा पूर्णता और पोर्टेबिलिटी;
  4. सीएसपी के वातावरण से मध्यस्थ की जानकारी को सुरक्षित एवं शुद्ध करना;
  5. सेवाओं का सुचारू संक्रमण; और
  6. देनदारियों, क्षति, दंड और क्षतिपूर्ति की स्पष्ट परिभाषा;
  7. यह निर्दिष्ट करना चाहिए कि क्लाउड-होस्टेड सेवा (ओं) और डेटा को क्लाउड से कैसे बाहर ले जाया जाएगा, एक सीएसपी से दूसरे सीएसपी में माइग्रेट करते समय जबकि अखंडता और सुरक्षा बनाए रखते हुए मध्यस्थ के व्यवसाय की निरंतरता पर न्यूनतम प्रभाव पड़ेगा। डेटा ट्रांसफर शुल्क, डेटा दिशानिर्देशों को हटाने जैसे विभिन्न खंडों को अनुबंध दस्तावेज में स्पष्ट रूप से उल्लेख किया जाना चाहिए।
- iv. डेटा का भंडारण केवल भारत में;
- v. सेवा प्रदाता को कैप्चर किए गए, संसाधित और संग्रहीत, डेटा प्रतिधारण / अभिलेखीय डेटा का विवरण प्रदान करने की आवश्यकता वाले खंड;
- vi. मध्यस्थों और उसके अभिदाताओं के डेटा की गोपनीयता बनाए रखने के लिए नियंत्रण, और सुरक्षा उल्लंघन और ऐसी जानकारी के लीक होने की स्थिति में मध्यस्थ के लिए सेवा प्रदाता की देयता को शामिल करना;
- vii. समाधान प्रक्रिया, चूक की घटनाओं, क्षतिपूर्ति, उपचार और संबंधित पक्षों के लिए उपलब्ध साधन निर्दिष्ट करना;

- viii. व्यवसाय निरंतरता और परीक्षण आवश्यकताओं को सुनिश्चित करने के लिए आकस्मिक योजना (ओं);
- ix. मध्यस्थ द्वारा सीएसपी की लेखा परीक्षा करने का अधिकार (सीएसपी सेवाओं के उपयोग तक सीमित), चाहे वह उसके आंतरिक या बाहरी लेखा परीक्षकों द्वारा हो, या उसकी ओर से कार्य करने के लिए नियुक्त एजेंटों द्वारा, और मध्यस्थ के लिए की गई सेवाओं के संयोजन में सेवा प्रदाता के बारे में की गई किसी भी लेखा परीक्षा या समीक्षा रिपोर्ट और निष्कर्षों की प्रतियां प्राप्त करने का अधिकार;
- x. सीएसपी से तीसरे पक्ष (आपूर्ति श्रृंखला में) के बारे में जानकारी प्राप्त करने का अधिकार;
- xi.. सेवा प्रदाता और उसके किसी भी उप-कांटेक्टर का निरीक्षण करने के लिए नियामकों के अधिकार को मान्यता देना। क्लाउड सेवाओं के संबंध में सीएसपी द्वारा दी गई, संग्रहीत या संसाधित की गई मध्यस्थ की आईटी बुनियादी संरचना, अनुप्रयोगों, डेटा, दस्तावेजों और अन्य आवश्यक जानकारी तक पहुंचने के लिए पीएफआरडीए या उसके द्वारा अधिकृत व्यक्ति (ओं) को अनुमति देने के लिए खंड जोड़ना;
- xii. क्लाउड सेवा प्रदाता को उसके उपठेकेदारों के प्रदर्शन और जोखिम प्रबंधन प्रथाओं के लिए संविदात्मक रूप से उत्तरदायी बनाने वाले खंड शामिल हैं, यदि कोई हो;
- xiii. मध्यस्थ के समाप्ति अधिकार, जिसमें प्रस्तावित क्लाउड सेवा व्यवस्था को किसी अन्य सेवा प्रदाता को व्यवस्थित रूप से स्थानांतरित करने की क्षमता शामिल है, यदि आवश्यक या वांछनीय हो।
- xiv. मध्यस्थ के दिवालिया/समाधान के मामले में संबंधित प्राधिकरणों के साथ सहयोग करने के लिए क्लाउड सेवा प्रदाता का दायित्व;
- xv.. साइबर घटनाओं और सेवा में व्यवधान और डेटा हानि/रिसाव सहित घटनाओं की सूचना क्लाउड सेवा प्रदाता द्वारा मध्यस्थ को तुरंत दी जाए, लेकिन पता लगने के एक घंटे के भीतर अवश्य की जाए।
- ण. मध्यस्थ क्लाउड प्रशासन, निगरानी और अनुवीक्षण के लिए योग्य मानव संसाधन कर्मियों की उपलब्धता सुनिश्चित करेंगे।
- त. सुरक्षा भंग होने और अभिदाताओं से संबंधित गोपनीय सूचना लीक होने की स्थिति में मध्यस्थों को तत्काल प्राधिकरण (पीएफआरडीए) को सूचित करना होगा। मध्यस्थ का अनुपालन अधिकारी सीईआरटी-इन या पीएफआरडीए सहित ऐसी समान संस्थाओं को घटना या घटना की रिपोर्ट दर्ज करने के लिए जिम्मेदार होगा। सूचना और साइबर सुरक्षा उल्लंघनों को पीएफआरडीए के परिपत्र दिनांक 30 जून 2021 के अनुसार सीईआरटी-इन को निर्धारित टीएटी के अनुसार सूचित किया जाना चाहिए।



- थ. ऊपर उल्लिखित नीति/सिद्धांत उन सभी मध्यस्थों पर भी लागू होंगे जिन्होंने पीएफआरडीए द्वारा अनुमोदन करने पर क्लाउड सेवाओं को पहले ही अपना लिया है और उन पर भी लागू होंगे जो ऐसी सेवाओं को भविष्य में अपनाने का प्रस्ताव करते हैं। उन मध्यस्थों के लिए जिन्होंने पहले से ही अपने संचालन के लिए क्लाउड सेवाओं को अपनाया है, ऐसे मध्यस्थ को इस परिपत्र के जारी होने के 120 दिनों के भीतर इन दिशानिर्देशों के अनुपालन पर एक रिपोर्ट दायर करनी होगी और पीएफआरडीए केवल असाधारण परिस्थितियों में इस समयसीमा को बढ़ाने का अधिकार सुरक्षित रखता है।
- द. क्लाउड सेवाओं को अपनाने में रुचि रखने वाले मध्यस्थों को उस प्राधिकरण के विनियम विभाग से अनुमोदन प्राप्त करना होगा जिसे वे रिपोर्ट करते हैं और अनुपालन अधिकारी के माध्यम से अन्य बातों के साथ-साथ यह पुष्टि करते हैं कि वे नीति में उल्लिखित निर्देशों/नीति/परामर्शों का पालन करने जा रहे हैं, जिसमें क्लाउड सेवाओं को अपनाने के प्रस्ताव, अपनाई जा रही रणनीति और इस तरह के अपनाने के लिए तैयार किए जा रहे ढांचे का पूरा विवरण प्रदान किया जाएगा। एक बार अपनाई गई क्लाउड सेवाएं लागू हो जाने के बाद, उसे अपनाने के संबंध में पूर्ण दस्तावेज प्राधिकरण को प्रदान किए जाएंगे। पर्यवेक्षी प्रभाग/विभाग नियत समय में उक्त क्लाउड अपनाने और प्रबंधन पर प्राधिकरण को रिपोर्ट करने के प्रारूप सहित दिशा-निर्देश जारी कर सकता है।
- ध. नीति की समीक्षा दो वर्षों में कम से कम एक बार की जाएगी, प्रस्तावित किसी भी परिवर्तन को अध्यक्ष द्वारा अनुमोदित किया जाएगा और इसे जानकारी के लिए बोर्ड के समक्ष रखा जाएगा।

**अस्वीकरण:** जहां भी हिंदी और अंग्रेजी संस्करणों के बीच विरोध या अस्पष्टता मौजूद है, अंग्रेजी संस्करण मान्य होगा।

**क्लाउड सेवा प्रबंधन और सुरक्षा विचार :**

1. **सेवा और प्रौद्योगिकी संरचना:** मध्यस्थ यह सुनिश्चित करेंगे कि क्लाउड-आधारित अनुप्रयोगों का समर्थन करने वाली सेवा और प्रौद्योगिकी संरचना विश्व स्तर पर मान्यता प्राप्त संरचना सिद्धांतों और मानकों के पालन में बनाई गई हो। मध्यस्थ एक ऐसी प्रौद्योगिकी संरचना को प्राथमिकता देंगे जो सुरक्षित कंटेनर-आधारित डेटा प्रबंधन प्रदान करता हो, जहां एन्क्रिप्शन कुंजी और हार्डवेयर सुरक्षा मॉड्यूल मध्यस्थ के नियंत्रण में हों। संरचना को कंटेनरों, छवियों और रिलीज का प्रबंधन करने के लिए उपकरण और प्रक्रियाओं का एक मानक सेट प्रदान करना होगा। मल्टी टेनेंसी वातावरण को डेटा अखंडता और गोपनीयता जोखिमों और डेटा के को-मिंगलिंग के खिलाफ संरक्षित किया जाना चाहिए। संरचना की सुचारू रिकवरी को सक्षम करना चाहिए और क्लाउड संरचना में किसी भी एक या घटकों के संयोजन की किसी भी विफलता के परिणामस्वरूप डेटा / सूचना सुरक्षा में समझौता नहीं होना चाहिए।

2. **पहचान और अभिगम प्रबंधन (आईएम) :** आईएम को सीएसपी के साथ सहमत किया जाएगा और उपयोगकर्ता-एक्सेस और विशेषाधिकार प्राप्त एक्सेस के संबंध में क्लाउड होस्ट किए गए अनुप्रयोगों को भूमिका-आधारित पहुंच प्रदान करने के लिए सुनिश्चित किया जाएगा। क्लाउड-आधारित अनुप्रयोगों की पहचान और पहुंच प्रबंधन के लिए कड़े एक्सेस नियंत्रण, जैसा कि ऑन प्रिमाइस एप्लिकेशन के लिए लागू होता है, स्थापित किया जा सकता है। क्लाउड-होस्टेड एप्लिकेशन में सभी प्रकार की उपयोगकर्ता-एक्सेस और विशेषाधिकार प्राप्त-एक्सेस भूमिकाओं के लिए कर्तव्यों और रोल कनफ्लिक्ट मैट्रिक्स का पृथक्करण लागू किया जाना चाहिए, चाहे क्लाउड सेवा मॉडल कुछ भी हो। एक्सेस प्रोविजनिंग को 'जानने की आवश्यकता (need to know)' और 'कम से कम विशेषाधिकार (Least Privilege)' के सिद्धांतों द्वारा नियंत्रित किया जाना चाहिए और मध्यस्थ द्वारा अनुमोदन और निगरानी की जानी चाहिए। इसके अलावा, क्लाउड अनुप्रयोगों तक पहुंच के लिए बहु-कारक प्रमाणीकरण लागू किया जाना चाहिए।

3. **सुरक्षा नियंत्रण:** मध्यस्थ को यह सुनिश्चित करना होगा कि क्लाउड-आधारित एप्लिकेशन में सुरक्षा नियंत्रणों का कार्यान्वयन ऑन-प्रिमाइस एप्लिकेशन में / द्वारा प्राप्त किए गए नियंत्रण उद्देश्यों की तुलना में समान या उच्च स्तर के नियंत्रण उद्देश्यों को प्राप्त करे। इसमें नेटवर्क सुरक्षा संसाधनों और उनके कॉन्फिगरेशन की उचित पोस्टिंग के माध्यम से सुरक्षित कनेक्शन सुनिश्चित करना तथा मध्यस्थ द्वारा उपयोग की जाने वाली क्लाउड परिसंपत्तियों की उचित और सुरक्षित विन्यास, निगरानी;



क्लाउड अनुप्रयोगों और संबंधित संसाधनों में परिवर्तन को अधिकृत करने के लिए आवश्यक प्रक्रियाएं भी शामिल हैं। मध्यस्थ यह सुनिश्चित करेंगे कि सीएसपी आईएसओ 27017, आईएसओ 27018 जैसे क्लाउड सुरक्षा आईएसओ मानकों के नवीनतम संस्करण का अनुपालन करें और यह सुनिश्चित करेंगे कि डेटा या फ़ाइलों को एन्क्रिप्ट और डिक्రిप्ट करने के लिए सीएसपी द्वारा कम से कम 128-बिट एन्क्रिप्शन का उपयोग किया जाए।

**4. मजबूत निगरानी और अनुवीक्षण :** मध्यस्थ क्लाउड वातावरण में न्यूनतम निगरानी आवश्यकताओं को सटीक रूप से परिभाषित करेंगे।

5. क्लाउड पर तैनात सेवाओं से संबंधित घटनाओं की वास्तविक समय की घटना रिपोर्टिंग और हैंडलिंग के लिए क्लाउड में प्रासंगिक लॉग का प्रतिधारण सुनिश्चित किया जाएगा। सीएसपी से मध्यस्थ के एसओसी में लॉग, घटनाओं का उचित एकीकरण, जहां भी लागू हो, सुनिश्चित किया जाए।

6. इसके अनुप्रयोग को सुरक्षित करने में मध्यस्थों के अपने प्रयासों को सीएसपी के साइबर लचीलापन नियंत्रण द्वारा पूरित किया जाएगा। मध्यस्थ उन्नत खतरों / मैलवेयर से एप्लिकेशन की सुरक्षा के लिए अपग्रेड, फिक्स, पैच और सर्विस पैक सहित सुरक्षा से संबंधित सॉफ्टवेयर के निरंतर और नियमित अपडेट सुनिश्चित करेगा।

7. कोई भी इंटरफ़ेस जो इंटरनेट में बड़े पैमाने पर जनता के लिए एक सेवा / एपीआई / आदि के रूप में उजागर होता है, उसे इंटरनेट फेसिंग इंटरफ़ेस माना जाता है। आईपीएस, फ़ायरवॉल, डब्ल्यूएफ, एंटी डीडीओएस, एपीआई गेटवे आदि जैसे पर्याप्त सुरक्षा नियंत्रण होने चाहिए और 2एफए प्रमाणीकरण, एसएसएल वीपीएन समाधान जैसे अतिरिक्त नियंत्रणों पर विचार किया जाना चाहिए। इसी प्रकार, मध्यस्थों/प्रासंगिक संगठनों (P2P या LAN/MPLS आदि के माध्यम से) और CSP, सुरक्षा नियंत्रण जैसे IPS, फ़ायरवॉल, WAF, Anti DDOS, आदि के बीच जुड़े इंटरफ़ेस लागू होंगे और जहां भी आवश्यक हो, IPSEC VPN जैसे अतिरिक्त नियंत्रण को अपनाया जाएगा। नेटवर्क सुरक्षा संसाधनों, कॉन्फिगरेशन और अन्य लिंक किए गए आइटम खरीदते समय मध्यस्थों को IPv6 अनुपालन सुनिश्चित करना आवश्यक है।

8. मध्यस्थ उपयुक्त सुरक्षित सॉफ्टवेयर विकास जीवन चक्र (एसएसडीएलसी) प्रक्रियाओं को अपनाएगा, और सुरक्षा डिजाइन चरण से ही एक अभिन्न अंग होगा।

9. डेटा की गोपनीयता, निजता और अखंडता सुनिश्चित करने के लिए, मध्यस्थ द्वारा प्रचलित तकनीकी रुझानों और एन्क्रिप्शन की प्रक्रियाओं के अनुसार सर्वोत्तम प्रथाओं को अपनाया जाएगा।

10. **भेद्यता प्रबंधन:** मध्यस्थ यह सुनिश्चित करेंगे कि सीएसपी के पास अपेक्षित उद्योग-विशिष्ट संकट खुफिया क्षमताओं द्वारा समर्थित खतरों और कमजोरियों का प्रबंधन करने के लिए एक अच्छी तरह से शासित और संरचित ढांचा हो। मध्यस्थ के पास एक अच्छी तरह से परिभाषित भेद्यता प्रबंधन नीति होगी और इसका सख्ती से पालन करना होगा। नीति को क्लाउड में मध्यस्थ द्वारा प्रबंधित बुनियादी ढांचे / सेवाओं / आदि के भेद्यता प्रबंधन पहलुओं को भी संबोधित करना होगा। क्लाउड अवसंरचना पैच/ओएस/संस्करण आदि के संदर्भ में अद्यतित होगी। पैच प्रबंधन नीति क्लाउड के बुनियादी ढांचे को कवर करेगी और नीति समय पर पैच आवेदन को अनिवार्य करेगी।

11. **भेद्यता मूल्यांकन और प्रवेश परीक्षण (वीएपीटी):** मध्यस्थ द्वारा की गई वीएपीटी गतिविधि में क्लाउड समाधान पर होस्ट किए गए बुनियादी ढांचे और अनुप्रयोगों / सेवाओं को भी शामिल करना होगा। क्लाउड मूल जोखिमों और कमजोरियों का परीक्षण और आकलन करने के लिए वीएपीटी रणनीति, उपकरण और प्रक्रियाओं को ठीक करना होगा। किसी भी नई प्रणाली को चालू करने से पहले वीएपीटी भी आयोजित करनी होगी।

12. मध्यस्थ का व्यवसाय निरंतरता ढांचा यह सुनिश्चित करेगा कि, अपनी क्लाउड सेवाओं को प्रभावित करने वाली आपदा या सीएसपी की विफलता की स्थिति में, मध्यस्थ अखंडता और सुरक्षा सुनिश्चित करते हुए सेवाओं के न्यूनतम व्यवधान के साथ अपने महत्वपूर्ण संचालन को जारी रख सकता है।

13. मध्यस्थ के इन-हाउस सिक्योरिटी ऑपरेशंस सेंटर (एसओसी) समाधान को क्लाउड के बुनियादी ढांचे के साथ एकीकृत किया जाएगा। एसओसी संचालन की आउटसोर्सिंग में डेटा को बाहरी स्थान पर संग्रहीत और संसाधित करने और तीसरे पक्ष (प्रबंधित सुरक्षा सेवा प्रदाता (एमएसएसपी)) द्वारा प्रबंधित करने का जोखिम होता है, जिसके लिए मध्यस्थों की दृश्यता कम होती है। जोखिमों को कम करने के लिए, निर्धारित नियंत्रणों के अलावा, मध्यस्थ एसओसी संचालन की आउटसोर्सिंग के मामले में नीचे उल्लिखित आवश्यकताओं को अपनाएंगे:

क. सेवाओं (सिस्टम, सॉफ्टवेयर, स्रोत कोड, प्रक्रियाओं, अवधारणाओं, आदि) को प्रदान करने में उपयोग की जाने वाली संपत्ति के स्वामित्व की स्पष्ट रूप से पहचान करें;

ख. यह सुनिश्चित करें कि मध्यस्थ के पास नियम परिभाषा, अनुकूलन और संबंधित डेटा / लॉग, मेटा-डेटा और एनालिटिक्स (मध्यस्थ के लिए विशिष्ट) पर पर्याप्त निरीक्षण और स्वामित्व है;



ग. एसओसी के कामकाज का आकलन करना, जिसमें सेवा वितरण में शामिल सभी भौतिक सुविधाएं शामिल हैं, जैसे कि एसओसी और ऐसे क्षेत्र जहां अभिदाता डेटा समय-समय पर संग्रहीत / संसाधित किया जाता है;

घ. मध्यस्थ की घटना प्रतिक्रिया प्रक्रिया के साथ आउटसोर्स एसओसी रिपोर्टिंग और वृद्धि प्रक्रिया को एकीकृत करना; और

ड. अलर्ट/घटनाओं से निपटने की प्रक्रिया की समीक्षा करना।

#### 14. बैकअप और रिकवरी समाधान

क. मध्यस्थ यह सुनिश्चित करेगा कि क्लाउड परिनियोजन की बैकअप आवश्यकता को पूरा करने के लिए एक बैकअप और रिकवरी नीति हो। बैकअप की पर्याप्तता सुनिश्चित करने के लिए बैकअप और रिकवरी प्रक्रियाओं को वर्ष में कम से कम दो बार जांचा जाएगा।

ख. बैकअप को तार्किक रूप से उत्पादन / विकास वातावरण से अलग किया जाएगा ताकि यह सुनिश्चित किया जा सके कि उत्पादन प्रणालियों में मैलवेयर संक्रमण बैकअप वातावरण में न फैले।

ग. जब सीएसपी की बैकअप सेवाओं का उपयोग किया जाए तो एन्क्रिप्शन समाधान और कुंजी प्रबंधन के साथ पर्याप्त देखभाल करनी होगी।

\*\*\*\*\*

CIRCULAR

Circular no: PFRDA/2023/33/ICS/01

23<sup>rd</sup> November 2023

To

All Intermediaries registered with PFRDA

**Subject: Adoption of cloud services by intermediaries regulated by PFRDA**

This circular is issued in exercise of powers conferred under Sec 14(1) read with sec 14(2) clause (a) of the PFRDA Act, 2013 and to protect the interests of subscribers. The circular is being issued to enable and equip the intermediaries with a policy framework on adoption of cloud services by intermediaries for the services being rendered by them. The policy also lays down the regulatory and legal requirements and compliances by the intermediaries, if they adopt the cloud services.

1. Intermediaries registered with PFRDA have been extensively leveraging Information Technology (IT) and IT enabled services (ITeS) including adopting cloud services to support their business models and products and services offered to their customers.
2. Adoption of cloud services for delivering the IT services is increasing in financial services sector and is also being encouraged by the government through various initiatives. While cloud solutions offer multiple advantages viz. ready to scale, ease of deployment, no overhead of maintaining physical infrastructure etc., it also increases cyber security risks and challenges.
3. PFRDA has earlier issued guidelines on outsourcing of activities for Central Recordkeeping Agencies vide its circular no **PFRDA/2016/4/CRA/TB/2 dt.29/01/2016** And for pension funds vide its circular no: **PFRDA/2017/30/PF/4 dt.09/10/2017** which were basically meant for policy on day to day handling of the operations and do not cover the outsourcing activities pertaining to IT and ITeS.
4. In view of the above, the Authority puts in place a framework or policy on adoption of cloud services by registered intermediaries to address the risks effectively and ensure regulatory compliance. The said policy shall be in addition to the referred outsourcing guidelines and the adoption of cloud services shall be considered as part of the outsourcing of the activities by the registered intermediaries.
5. The intermediaries who have already adopted or those intend to adopt cloud services are hereby advised to comply with the policy which is being attached as **Annexure**.

The circular is issued with the approval of the Competent Authority.



K.R.Daulath Ali Khan,  
General Manager

Information and Cybersecurity Dept



**POLICY ON ADOPTION OF CLOUD SERVICES BY INTERMEDIARIES  
REGULATED BY PFRDA**

**Background:**

Intermediaries registered with PFRDA have been extensively leveraging Information Technology (IT) and IT enabled services (ITeS) including adopting cloud services to support their business models and products and services offered to their customers. Further, there have been several requests by the intermediaries to PFRDA for allowing them to adopt cloud services for storage of data and related applications associated with NPS, APY and other pension schemes.

In the recent times the adoption of cloud services for delivering the IT services is increasing and is also encouraged by the government through various initiatives. While cloud solutions offer multiple advantages viz. ready to scale, ease of deployment, no overhead of maintaining physical infrastructure etc., entities adopting such technology should also be aware of the new cyber security risks and challenges which cloud solutions introduce.

PFRDA has earlier issued guidelines on outsourcing of activities for Central Recordkeeping Agencies vide its circular no **PFRDA/2016/4/CRA/TB/2 dt.29/01/2016** And for pension funds vide its circular no: **PFRDA/2017/30/PF/4 dt.09/10/2017**. These were basically meant for policy on day-to-day handling of the operations and do not cover the outsourcing activities pertaining to IT and ITeS in detail. Further, the registration guidelines issued by the Authority for intermediaries like CRAs, PFs etc., also provide for adoption of emerging technologies like cloud computing.

In view of the above, the Authority after reviewing the existing arrangements has decided to come out with a framework or policy on adoption of cloud services by registered intermediaries to address the risks effectively and ensure regulatory compliance. The said policy shall in addition to the referred outsourcing guidelines and the adoption of cloud services shall be considered as part of the outsourcing of the activities by the registered intermediaries.

**1. Applicability**

The provisions of this policy shall be applicable to all the registered intermediaries of PFRDA.

**2. Definitions: for the purpose of this policy, unless the context otherwise requires;**

- i. BCP means Business Continuity Plan
- ii. CISO means Chief Information Security Officer
- iii. Cloud services means infrastructure, platforms, or software that are hosted by third party providers and made available to users through the

- internet and includes cloud computing.
- iv. Cloud computing means Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction- (as defined by NIST (National Institute of Standards and Technology - US)).
  - v. CSP means Cloud Service Provider
  - vi. Intermediary includes pension fund, central recordkeeping agency, National Pension System Trust and point of presence in terms of PFRDA Act, 2013.
  - vii. SOC means Security Operation Center

### **3. Purpose:**

The underlying principle of the policy is to lay a framework for adoption of technological advances so that the intermediary ensures that adoption of technological advances like adoption of cloud services neither diminish its ability to fulfil its obligations to subscribers nor impede effective supervision by the authority with due assessment of the attendant risks. Intermediary while adopting cloud services or other IT enabled services shall take steps to ensure that the service provider employs the same high standard of care in performing the services as would have been employed by the intermediary if the same activity was not outsourced.

### **4. Cloud Services**

There are several popular cloud deployment and service models that have emerged over time. These are generally based on the extent of technology stack that is proposed to be adopted by the consuming entity. Each of these models come with corresponding service, business benefit and risk profiles. The intermediaries shall examine the following while adopting cloud services for discharge of their functions:

- a. While considering adoption of cloud solution, it is imperative to analyse the business strategy and goals adopted to the current IT applications footprint and associated costs. Cloud adoption ranges from moving only non-business critical workloads to the cloud to moving critical business applications such as SaaS adoption and the several combinations in-between, which should be based on a business technology risk assessment.
- b. In engaging cloud services, intermediaries shall ensure, inter alia, that such outsourcing addresses the entire lifecycle of data, that is, covering the entire span of time from generation of the data, its entry into the cloud, till the data is permanently erased/ deleted. The intermediary shall ensure that the procedures specified are consistent with business needs and legal and regulatory requirements.
- c. In adoption of cloud services, intermediaries shall take into account the cloud service specific factors, viz., multi-tenancy, multi-location storing/ processing of data, etc., and attended risks while establishing appropriate risk management framework.



- d. Cloud Governance: intermediaries shall adopt and demonstrate a well-established and documented cloud adoption policy. Such a policy should, inter alia, identify the activities that can be moved to the cloud, enable and support protection of various stakeholder interests, ensure compliance with regulatory requirements, including those on privacy, security, data sovereignty, recoverability and data storage requirements, aligned with data classification. The policy should provide for appropriate due diligence to manage and continually monitor the risks associated with CSPs.

## **5. Policy and principles for adoption of cloud services by intermediaries**

The following shall be the broad policy and principles to be followed and adhered to by all registered intermediaries of the Authority for adoption of cloud services:

- a. The Board of the intermediary shall decide upon the matter of adoption of Cloud based services after due evaluation of the need, implications (financial, regulatory, etc.), risks, benefits, etc. of adopting cloud computing.
- b. The Board of the intermediary shall consider all relevant laws, regulations, rules, guidelines and conditions of approval/licensing or registration, when performing its due diligence in relation to adoption of cloud services. The due diligence referred to shall take into consideration qualitative, quantitative, financial, operational, legal and reputational factors. The Intermediary shall be responsible and accountable for all aspects related to such outsourcing of functions including the cloud services. Such accountability shall encompass availability of cloud applications, confidentiality, integrity and security of its data and logs, and ensuring Intermediary's compliance with respect to the Act, rules, regulations, circulars, etc. issued by PFRDA, if the intermediary decides to adopt cloud services.
- c. The Board after due evaluation of all relevant activities, shall put in place a comprehensive Board approved cloud adoption policy including laying clear policy on the role of Senior Management, IT function including the role of CISO, business function, and oversight & assurance functions in respect of adoption of cloud services. It shall further cover the criteria of selection of service providers, delegation of authority depending on risk and materiality for various activities related to such adoption, data localization, data ownership, access, risk assessment and due-diligence on cloud service providers (CSPs), security controls, disaster recovery and business continuity plans, systems to monitor and review the operations of these activities and termination processes and exit strategies, vendor lock-in, including business continuity in the event of a third-party service provider or CSP exiting the arrangement.
- d. Such board approved policy shall also contain details of audit and assurance activities in relation to such adoption of cloud services. The audit/ periodic review/ third-party certifications should cover, as per applicability and cloud usage, inter alia, aspects such as roles and responsibilities of both intermediary and CSP in cloud governance, access and network controls, configurations, monitoring mechanism, data encryption, log review, change management, incident response and resilience preparedness and testing, etc.



- e. The storage/ processing of data (DC, DR, near DR etc.) including logs and any other data pertaining to the intermediary in any form in cloud should reside/be processed within the legal boundaries of India. Data collection and processing of data must be governed by the laws and policies of India and shall be in compliance to the various regulations, guidelines issued by Ministries / Departments and Government agencies from time to time. Further, the data should reside/ be processed within the MeitY empanelled Cloud Service Providers' data centres holding valid STQC (or any other equivalent agency appointed by Government of India) audit status.
- f. The Intermediary shall retain the complete ownership of its data and associated data, encryption keys, logs etc. residing in cloud.
- g. There shall be an explicit and unambiguous delineation/ demarcation of responsibilities with respect to all activities (including but not limited to technical, managerial, governance related, etc.) of the cloud services between the intermediary and CSP. Ideally, there shall be no "shared responsibility" or "joint ownership" for any function/ task/ activity between the intermediary and CSP. If any function/ task/ activity has to be performed jointly by the intermediary and CSP, there shall be a clear delineation and fixing of responsibility for each sub-task/ line-item within the task. The aforementioned delineation of responsibilities shall be added explicitly in the agreement signed between the intermediary and the CSP. For example, the security of the data residing in the Cloud will be the responsibility of the end user and the security of the Cloud Infrastructure level will be the responsibility of the Cloud Service Provider (CSPs).
- h. Intermediaries shall ensure that the service and technology architecture supporting cloud-based applications is built in adherence to globally recognised architecture principles and standards. Intermediaries shall prefer a technology architecture that provides for secure container-based data management, where encryption keys and Hardware Security Modules are under the control of the Intermediary. Multi-tenancy environments should be protected against data integrity and confidentiality risks and against co-mingling of data. The architecture should enable smooth recovery and any failure of any one or combination of components across the cloud architecture should not result in data/ information security compromise.
- i. Cloud Services Management and Security Considerations: The intermediary shall take into account the subject matters as detailed in **Annexure I** regarding the cloud services management and security and ensure that the same are complied with.
- j. The intermediary shall finalise the setup, architecture of the systems and cloud architecture keeping in view of the Cyber security, scalability, integrity and resilience of the systems and PFRDA shall not be liable in any manner or responsible for the functional or operational efficiency or technical aspects of such configurations.
- k. Intermediaries shall enter into a contract only with CSPs subject to jurisdictions that uphold enforceability of agreements cast under Indian laws and the rights



available thereunder to Intermediaries, including those relating to aspects such as data storage, data protection and confidentiality.

- l. Intermediaries shall ensure that their rights and obligations and those of the cloud service providers (CSPs) are clearly defined and set out in a legally binding written agreement. In principle, the provisions of the agreement should appropriately reckon the criticality of the outsourced task to the business of the intermediary, the associated risks and the strategies for mitigating or managing them. The agreement shall be sufficiently flexible to allow the intermediary to retain adequate control over all the activities in relation to the cloud services and the right to intervene with appropriate measures to meet legal and regulatory obligations.
- m. The intermediary shall have incident management policy, procedures and processes in place. The intermediary shall adhere with the same for deployments being done in cloud.
- n. The above referred agreement inter alia at minimum shall ensure that the following aspects are covered:
  - i. compliance with the provisions of IT Act, other applicable legal requirements and standards to protect the customer data;
  - ii. details like scope of services, charges for services and maintaining confidentiality of customer's data, Availability of Cloud services, Performance, Security, Disaster recovery and data backup management, etc.
  - iii. the deliverables, including Service-Level Agreements (SLAs) formalising performance criteria to measure the quality and quantity of service levels and other relevant issues; the exit strategy and service level stipulations in the SLA shall factor in, inter alia,
    1. contract duration;
    2. agreed processes and turnaround times for returning the intermediary's service collaterals and data held by the CSP;
    3. data completeness and portability;
    4. secure purge of intermediary's information from the CSP's environment;
    5. smooth transition of services; and
    6. unambiguous definition of liabilities, damages, penalties and indemnities.
    7. should specify how the cloud-hosted service(s) and data will be moved out from the cloud with minimal impact on continuity of the intermediary's business, while maintaining integrity and security. While migrating from one CSP to another. various clauses such as data transfer charges, deletion of data guidelines should be explicitly mentioned in contract document.
  - iv. storage of data only in India;
  - v. clauses requiring the service provider to provide details of data (related to intermediary and its customers) captured, processed and stored, data retention/archival;

- vi. controls for maintaining confidentiality of data of intermediaries and its customers', and incorporating service provider's liability to intermediary in the event of security breach and leakage of such information;
  - vii. specifying the resolution process, events of default, indemnities, remedies, and recourse available to the respective parties;
  - viii. contingency plan(s) to ensure business continuity and testing requirements;
  - ix. right to conduct audit of the CSP by the intermediary (limited to its usage of CSP services), whether by its internal or external auditors, or by agents appointed to act on its behalf, and to obtain copies of any audit or review reports and findings made about the service provider in conjunction with the services performed for the intermediary;
  - x. right to seek information from the CSP about the third parties (in the supply chain) engaged by the former;
  - xi. recognising the authority of regulators to perform inspection of the service provider and any of its sub-contractors. Adding clauses to allow PFRDA or person(s) authorised by it to access the intermediary's IT infrastructure, applications, data, documents, and other necessary information given to, stored or processed by the CSP in relation to the cloud services;
  - xii. including clauses making the cloud service provider contractually liable for the performance and risk management practices of its sub-contractors, if any;
  - xiii. termination rights of the intermediary, including the ability to orderly transfer the proposed cloud services arrangement to another service provider, if necessary or desirable.
  - xiv. obligation of the cloud service provider to co-operate with the relevant authorities in case of insolvency/ resolution of the intermediary;
  - xv. that incidents, including cyber incidents and those resulting in disruption of service and data loss/ leakage are reported to them by the cloud service provider immediately but not later than one hour of detection to the intermediary.
- o. Intermediaries shall ensure availability of qualified human resource personnel for cloud administration, monitoring and surveillance.
- p. The intermediaries shall immediately notify the Authority (PFRDA) in the event of breach of security and leakage of confidential customer related information. The compliance officer of the intermediary shall be responsible for filing the incident or event reporting to CERT-In or such similar entities and including PFRDA. Information and Cyber Security breaches may be informed as per prescribed TAT to CERT-In as per PFRDA Circular dated 30th June 2021.
- q. The policy/principles stated above shall also be applicable to all those intermediaries who have already adopted cloud services upon approval by PFRDA and also to those who propose to adopt such services. For those who have already adopted the cloud services for their operations, such an intermediary shall file a compliance report on the adherence to these guidelines within 120 days of issuance of this circular and PFRDA reserves the right to extend this timeline only in exceptional circumstances.



- r. The intermediaries interested in adoption of cloud services shall seek approval from the regulations department of the authority to whom they report and through the compliance officer inter alia confirming that they are going to adhere to the directions/policy/advisories mentioned in the policy, providing the complete details of proposed adoption of cloud services, strategy being adopted and the framework being put in place for such adoption. Once, the cloud services adopted are in place, complete documentation with respect to the said adoption shall be provided to the Authority. The supervisory division/department may issue the guidelines including the formats of reporting to the Authority on the said cloud adoption and management in due course.
- s. The policy shall be reviewed at least once in two years, any changes proposed shall be approved by the Chairman and the same shall be put up to the Board for information.

**Cloud Services Management and Security Considerations:**

1. **Service and Technology Architecture:** Intermediaries shall ensure that the service and technology architecture supporting cloud-based applications is built in adherence to globally recognised architecture principles and standards. Intermediaries shall prefer a technology architecture that provides for secure container-based data management, where encryption keys and Hardware Security Modules are under the control of the Intermediary. The architecture should provide for a standard set of tools and processes to manage containers, images and releases. Multi-tenancy environments should be protected against data integrity and confidentiality risks and against co- mingling of data. The architecture should enable smooth recovery and any failure of any one or combination of components across the cloud architecture should not result in data/ information security compromise.
2. **Identity and Access Management (IAM):** IAM shall be agreed upon with the CSP and ensured for providing role-based access to the cloud hosted applications, in respect of user-access and privileged-access. Stringent access controls, as applicable for an on-premise application, may be established for identity and access management to cloud-based applications. Segregation of duties and role conflict matrix should be implemented for all kinds of user-access and privileged-access roles in the cloud-hosted application irrespective of the cloud service model. Access provisioning should be governed by principles of 'need to know' and 'least privileges' and require the intermediary's approval and monitoring. In addition, multi-factor authentication should be implemented for access to cloud applications.
3. **Security Controls:** Intermediaries shall ensure that the implementation of security controls in the cloud-based application achieves similar or higher degree of control objectives than those achieved in/ by an on-premise application. This includes ensuring - secure connection through appropriate deployment of network security resources and their configurations; appropriate and secure configurations, monitoring of the cloud assets utilised by the Intermediary; necessary procedures to authorise changes to cloud applications and related resources. The Intermediaries shall ensure that the CSPs shall comply to latest version of Cloud Security ISO Standards like ISO 27017, ISO 27018 and shall ensure at least 128-bit encryption is used by CSPs to encrypt and decrypt data or files.
4. **Robust Monitoring and Surveillance:** Intermediaries shall accurately define minimum monitoring requirements in the cloud environment.
5. **Retention of relevant logs in cloud** shall be ensured for real-time incident reporting and handling of incidents relating to services deployed on the cloud. Appropriate integration of logs, events from the CSP into the intermediary's SOC, wherever applicable.
6. The intermediaries' own efforts in securing its application shall be complemented by the CSP's cyber resilience controls. The CSP / intermediary



shall ensure continuous and regular updates of security-related software including upgrades, fixes, patches and service packs for protecting the application from advanced threats/ malware.

7. Any interface which is exposed to public at large in internet in the form of a service/API/etc. is considered as internet facing interface. Adequate security controls such as IPS, Firewall, WAF, Anti DDOS, API gateways etc. should be in place and additional controls such as 2FA authentication, SSL VPN solutions should be considered. Similarly, Interfaces connected between intermediary's/relevant organizations (Through P2P or LAN/MPLS etc.) and CSP, Security controls such as IPS, Firewall, WAF, Anti DDOS, etc. shall be in place and additional controls such as IPSEC VPN wherever necessary shall be adopted. Intermediaries are required to ensure IPv6 compliance when procuring network security resources, configurations and other linked items.
8. Intermediary shall adopt appropriate Secure Software Development Life Cycle (SSDLC) processes, and security shall be an integral part right from the design phase itself.
9. To ensure the confidentiality, privacy and integrity of the data, best practices as per prevailing technological trends and procedures of encryption shall be adopted by the intermediary.
10. **Vulnerability Management:** Intermediary's shall ensure that CSPs have a well-governed and structured approach to manage threats and vulnerabilities supported by requisite industry-specific threat intelligence capabilities. The intermediary shall have a well-defined Vulnerability Management policy in place and should strictly adhere with the same. The policy should also address the vulnerability management aspects of the infrastructure /services/etc. managed by intermediary in the cloud. The cloud infrastructure shall be up to date in terms of patches/OS/version etc. The patch management policy shall cover the infrastructure of cloud and the policy shall mandate timely patch application.
11. **Vulnerability Assessment and Penetration Testing (VAPT):** The VAPT activity undertaken by intermediary should also cover the infrastructure and applications/services hosted on cloud solution. The VAPT Tactics, Tools and Procedures should be fine-tuned to test and assess the cloud native risks and vulnerabilities. VAPT should also be conducted before commissioning of any new system.
12. The intermediary's business continuity framework shall ensure that, in the event of a disaster affecting its cloud services or failure of the CSP, the intermediary can continue its critical operations with minimal disruption of services while ensuring integrity and security.
13. In-house Security Operations Centre (SOC) solution of intermediary shall be integrated with the infrastructure of cloud. Outsourcing of SOC operations has the risk of data being stored and processed at an external location and managed by a third party (Managed Security Service Provider (MSSP)) to which intermediaries have lesser visibility. To mitigate the risks, in addition to the controls prescribed, intermediaries shall adopt the below mentioned

requirements in the case of outsourcing of SOC operations:

- a) unambiguously identify the owner of assets used in providing the services (systems, software, source code, processes, concepts, etc.);
- b) ensure that the intermediary has adequate oversight and ownership over the rule definition, customisation and related data/ logs, meta-data and analytics (specific to the intermediary);
- c) assess SOC functioning, including all physical facilities involved in service delivery, such as the SOC and areas where client data is stored / processed periodically;
- d) integrate the outsourced SOC reporting and escalation process with the intermediary's incident response process; and
- e) review the process of handling of the alerts / events.

#### **14. Backup and recovery solution**

- a) The intermediary shall ensure that a backup and recovery policy is in place to address the backup requirement of cloud deployments. The backup and recovery processes shall be checked at least twice in a year to ensure the adequacy of the backups.
- b) The backup shall be logically segregated from production/dev environment to ensure that the malware infection in production systems should not percolate to backup environment.
- c) When CSP's backup services are utilized, adequate care should be taken with encryption solution and key management.

\*\*\*\*\*