रजिस्ट्री सं. डी.एल.- 33004/99 REGD. No. D. L.-33004/99

भारत का राजपत्र
The Gazette of India

सी.जी.-डी.एल.-अ.-05082026-275218
CG-DL-E-05082026-275218

असाधारण
EXTRAORDINARY

भाग III—खण्ड 4
PART III—Section 4

प्राधिकार से प्रकाशित
PUBLISHED BY AUTHORITY

सं. 484] नई दिल्ली, शुक्रवार, जुलाई 31, 2026/श्रावण 9, 1948
No. 484] NEW DELHI, FRIDAY, JULY 31, 2026/SHRAVAN 9, 1948

केन्द्रीय विद्युत प्राधिकरण

अधिसूचना

नई दिल्ली, 31 जुलाई, 2026

फा. सं. सीईए-एचवाई-91-19/8/2024-साइबर सुरक्षा प्रभाग.- विद्युत (पूर्व प्रकाशन की प्रक्रिया) नियम, 2005 के नियम 3 के उप नियम (2) के साथ पठित विद्युत अधिनियम, 2003 (2003 का 36) की धारा 177 की उप धारा (3) के द्वारा यथाअपेक्षित केंद्रीय विद्युत प्राधिकरण (विद्युत क्षेत्र में साइबर सुरक्षा) विनियम, 2025 के प्रारूप का विज्ञापन करने वाली सार्वजनिक सूचनाएं छह दैनिक समाचार पत्रों में प्रकाशित की गईं थीं, ताकि उनसे प्रभावित होने की संभावना वाले सभी व्यक्तियों से उक्त प्रारूप विनियमों की प्रतियां जनता को उपलब्ध कराए जाने की तारीख से तीस दिन की अवधि समाप्त होने से पहले आपत्तियां और सुझाव आमंत्रित किए जा सकें;

और सार्वजनिक सूचनाएं अंतर्विष्ट करने वाले उक्त समाचार पत्रों की प्रतियां और प्रारूप विनियम केन्द्रीय विद्युत प्राधिकरण की वेबसाइट पर 07 अक्टूबर, 2025 को जनता के लिए उपलब्ध करा दी गई थीं;

और उक्त प्रारूप विनियमों पर जनता से प्राप्त आपत्तियों और सुझावों पर केन्द्रीय विद्युत प्राधिकरण ने विचार किया था;

और इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय ने विद्युत क्षेत्र के लिए साइबर सुरक्षा के संबंध में इन विनियमों को बनाने के लिए अपनी सहमति दे दी है।

अतः, अब, केन्द्रीय विद्युत प्राधिकरण विद्युत अधिनियम, 2003 (2003 का 36) की धारा 73 की खंड (ग) के साथ पठित धारा 177 की उप-धारा (1) द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए, विद्युत संयंत्रों और विद्युत लाइनों के सुरक्षित संचालन और रखरखाव को सुनिश्चित करने के लिए विद्युत क्षेत्र में साइबर सुरक्षा से संबंधित निम्नलिखित विनियम बनाता है, अर्थात:-

अध्याय I

प्रारंभिक

1. संक्षिप्त नाम और प्रारंभ - (1) इन विनियमों का संक्षिप्त नाम केंद्रीय विद्युत प्राधिकरण (विद्युत क्षेत्र में साइबर सुरक्षा) विनियम, 2026 है।

(2) ये विनियम 1 अप्रैल 2027 से प्रवृत्त होंगे:

परंतु विनियम 5(9), 5(24), 5(33), 5(39), 6(2) और 6(7) उन तारीखों से प्रवृत्त होंगे, जिन्हें प्राधिकरण केंद्रीय सरकार के पूर्व अनुमोदन से पृथक आदेशों के माध्यम से विनिर्दिष्ट करे।

2. लागू होने की परिधि और विस्तार - (1) ये विनियम इन निम्नलिखित को लागू होंगे: -

(क) सभी संस्थाएं, अपने विद्यमान और आगामी अवसंरचना के लिए, जो आपस में जुड़ी विद्युत प्रणाली से जुड़े परिचालन प्रौद्योगिकी अवसंरचना और उनके सूचना प्रौद्योगिकी अवसंरचना, जो ऐसे परिचालन प्रौद्योगिकी अवसंरचना से भौतिक या तार्किक रूप से जुड़ी हुई हैं, का स्वामित्व, संचालन या प्रबंधन करती हैं:

परंतु बिजली बनाने वाली कंपनियों, कैप्टिव विद्युत संयंत्र और उर्जा भण्डारण प्रणाली वाले संगठनों के मामले में, ये विनियम तभी लागू होंगे जब उनकी संस्थापित क्षमता 50 मेगावाट या उससे अधिक हो:

परंतु यह और कि, जिन संस्थाओं की संस्थापित क्षमता 50 मेगावाट से कम है, उन्हें 'भारतीय कंप्यूटर आपात मोचन दल' द्वारा जारी "सूक्ष्म, लघु और मध्यम उद्यम के लिए 15 बुनियादी साइबर सुरक्षा कंट्रोल" में बताए गए न्यूनतम साइबर सुरक्षा उपायों को लागू करने के लिए प्रोत्साहित किया जाता है;

(ख) विनियम 6, 11 और 12 के सिवाय, विद्युत विनियय एक्सचेंज और ओवर-द-काउंटर प्लेटफ़ॉर्म।

(2) वेंडर इन विनियम के विनियम 11 और विनियम 12 का पालन करेगा, जैसा लागू हो।

3. **परिभाषाएँ - (1)** इन विनियमों में, जब तक संदर्भ से अन्यथा अपेक्षित न हो -

(क) **"अधिनियम"** से विद्युत अधिनियम, 2003 (2003 का 36) अभिप्रेत है;

(ख) **"सामानों का बिल"** से किसी उत्पाद या प्रणाली में उपयोग किए जाने वाले घटकों, उप-घटकों, सामग्री, पुस्तकालयों, और मॉड्यूल की एक व्यापक सूची और संरचित वस्तु सूची अभिप्रेत है, ताकि ऐसे उत्पाद या प्रणाली की संरचना में व्यापक दृश्यता और पारदर्शिता को सुविधाजनक बनाया जा सके;

(ग) **"कारबार निरंतरता योजना"** से दस्तावेज़ीकृत प्रक्रियाएं अभिप्रेत हैं जो किसी संगठन को निरंतर संचालन के एक परिभाषित स्तर को बनाए रखने में मार्गदर्शन करती हैं;

(घ) **"मुख्य सूचना सुरक्षा अधिकारी"** से किसी संस्था के वरिष्ठ प्रबंधन स्तर का नामित कर्मचारी अभिप्रेत है, जिसे साइबर सुरक्षा और उससे जुड़े मामलों की जानकारी हो, और जो साइबर सुरक्षा के प्रयासों और पहलों के लिए उत्तरदायी है;

(ङ) **"मुख्य सूचना सुरक्षा अधिकारी- विद्युत मंत्रालय"** से विद्युत मंत्रालय का मुख्य सूचना सुरक्षा अधिकारी अभिप्रेत है;

(च) **"संचार प्रणाली"** से पृथक-पृथक संचार नेटवर्क, संचार मीडिया, रिलेइंग स्टेशन, ट्रिब्यूटरी स्टेशन, टर्मिनल उपकरण का एक संग्रह अभिप्रेत है जो आमतौर पर विद्युत क्षेत्र के लिए एक एकीकृत संचार बनाने के लिए अंतर्संबंध और अंतर-प्रचालन में सक्षम होते हैं;

(छ) **"कंप्यूटर सुरक्षा घटना मोचन दल- विद्युत"** से विद्युत क्षेत्र में साइबर सुरक्षा घटनाओं का समायोजन करने, रिपोर्ट करने और उनका मोचन करने के लिए विद्युत मंत्रालय द्वारा भारतीय कंप्यूटर आपात मोचन दल के एक विस्तारित शाखा के रूप में स्थापित एक संगठन अभिप्रेत है;

(ज) **"नाजुक सूचना प्रौद्योगिकी प्रणाली"** से किसी संगठन की सूचना प्रौद्योगिकी प्रणाली अभिप्रेत है, जिनकी अनुपलब्धता या खराबी उसके कारबार प्रचालन पर प्रतिकूल प्रभाव डालेगी;

(झ) **"नाजुक परिचालन प्रौद्योगिकी प्रणाली"** से किसी संगठन की प्रचालन प्रौद्योगिकी प्रणाली अभिप्रेत है, जिनकी अनुपलब्धता या खराबी उसके कारबार प्रचालन पर प्रतिकूल प्रभाव डालेगी;

(ञ) **"नाजुक प्रणाली"** से नाजुक प्रचालनात्मक प्रौद्योगिकी प्रणाली या नाजुक सूचना प्रौद्योगिकी प्रणाली या दोनों अभिप्रेत है, जिसमें लागू होने पर, किसी संस्था की जटिल सूचना अवसंरचना शामिल है;

(ट) **"नाजुक सूचना अवसंरचना"** से वह जटिल सूचना अवसंरचना अभिप्रेत है, जिसे सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) की धारा 70 की उप-धारा (1) के स्पष्टीकरण में परिभाषित किया गया है;

(ठ) **"साइबर आस्ति"** से प्रोग्रामेबल इलेक्ट्रॉनिक डिवाइस, जिसमें कंप्यूटिंग क्षमताएं हों या न हों, अभिप्रेत है जिसमें उसका हार्डवेयर, सॉफ्टवेयर, सब-कंपोनेंट और उसका डेटा शामिल है जो एक नेटवर्क से जुड़े होते हैं;

(ड) **"साइबर आस्तियों रजिस्टर"** से एक ऐसा अभिलेख अभिप्रेत है जिसमें सभी साइबर आस्तियों की सूची और उनका विवरण होता है;

(ढ) **"साइबर संकट प्रबंधन योजना"** से साइबर संकट प्रबंधन योजना अभिप्रेत है, जैसा कि सूचना प्रौद्योगिकी (संरक्षित प्रणाली के लिए सूचना सुरक्षा अभ्यास और प्रक्रियाएं) नियम, 2018 के नियम 2 के उप-नियम (1) के खंड (घ) में परिभाषित किया गया है;

(ण) **"साइबर समुत्थान-शक्ति"** से साइबर आस्ति पर खराब स्थितियों, तनाव, आक्रमणों या समझौतों का अनुमान लगाने, उनका सामना करने, उनसे उबरने और उनके अनुरूप ढलने की क्षमता अभिप्रेत है;

(त) **"साइबर सुरक्षा संपरीक्षा"** से भारतीय कंप्यूटर आपातकालीन मोचन दल पैनल में शामिल संपरीक्षक या भारत सरकार के विद्युत मंत्रालय द्वारा पृथक आदेश से अभिहित किसी अन्य संपरीक्षक द्वारा साइबर सुरक्षा की स्थिति का निर्धारण करने के लिए की गई संपरीक्षा अभिप्रेत है;

(थ) **"साइबर सुरक्षा उल्लंघन"** से साइबर सुरक्षा उल्लंघन अभिप्रेत है, जैसा कि सूचना प्रौद्योगिकी (भारतीय कंप्यूटर आपातकालीन मोचन दल और कार्यों व कर्तव्यों के निष्पादन की रीति) नियम, 2013 के नियम के उप-नियम (1) के खंड (झ) में परिभाषित किया गया है;

(द) **"साइबर सुरक्षा घटना"** से साइबर सुरक्षा घटना अभिप्रेत है, जैसा कि सूचना प्रौद्योगिकी (भारतीय कंप्यूटर आपातकालीन मोचन दल और कार्यों व कर्तव्यों के निष्पादन की रीति) नियम, 2013 के नियम 2 के उपनियम (1) के खंड (ज) में परिभाषित किया गया है;

(ध) **"साइबर सुरक्षा नीति"** से जानकारी, कंप्यूटर संसाधनों, नेटवर्क, डिवाइस, औद्योगिक नियंत्रण प्रणाली और प्रचालन प्रौद्योगिकी संसाधन को सुरक्षित रखने और उनकी साइबर सुरक्षा स्थिति में सुधार करने के लिए नियम और प्रक्रियाऐं अभिप्रेत हैं;

(न) **"साइबर तोड़फोड़"** से विद्वेषपूर्ण प्रयोजन से सूचना प्रणाली, नेटवर्क, या उसमें प्रोसेस किए गए डेटा को बाधित करने, नुकसान पहुंचाने या नष्ट करने के लिए जानबूझकर की गई कार्रवाई अभिप्रेत है;

(प) **"वितरित उत्पादन संसाधन"** से एक ऐसा उत्पादन स्टेशन अभिप्रेत है जो 33 केवी से कम वोल्टेज स्तर पर विद्युत प्रणाली में बिजली फीड करता है, और इसमें ग्रिड से जुड़े रूफटॉप सोलर प्रणाली और ऊर्जा भंडारण प्रणाली शामिल हैं;

(फ) **"इलेक्ट्रॉनिक सुरक्षा परिधि":** से सूचना प्रौद्योगिकी प्रणाली या परिचालन तकनीक प्रणाली या दोनों के चारों

ओर की तार्किक सीमा अभिप्रेत है जो इलेक्ट्रॉनिक रूप से जुड़े हुए हैं, जिसके अंदर ऐसी प्रणाली की सुरक्षा के लिए एक्सेस की निगरानी एवं नियंत्रण किया जाता है;

(ब) "**संस्था**" में उत्पादन कंपनियाँ, कैप्टिव उत्पादन संयंत्र, ऊर्जा भंडारण प्रणाली वाली संस्थाएं; पारेषण लाइसेंसधारी; वितरण लाइसेंसधारी; राष्ट्रीय भार प्रेषण केंद्र; क्षेत्रीय भार प्रेषण केंद्र; राज्य भार प्रेषण केंद्र, ऊर्जा विनिमय, ओवर द काउंटर प्लेटफॉर्म शामिल हैं;

(भ) **"फ़ैक्ट्री स्वीकृति परीक्षण"** से वेंडर द्वारा, संस्था के प्रतिनिधि की उपस्थिति में, प्रणाली या उपकरण या उसके मुख्य कंपोनेंट की कार्यात्मक, प्रदर्शन, संविदात्मक और सुरक्षा अपेक्षाओं को सत्यापित करने के लिए, प्रेषण से पहले की जाने वाली संरचित और प्रलेखित परीक्षण प्रक्रिया अभिप्रेत है;

(म) **"सूचना प्रौद्योगिकी प्रणाली"** से सूचना प्रौद्योगिकी प्रणाली अभिप्रेत है जिसमें उपयोगकर्ता एंडपॉइंट्स, नेटवर्क संसाधन, एप्लीकेशन, सर्वर और उसमें तैनात किए गए संचार घटक शामिल हैं और जिसका प्रचालन प्रौद्योगिकी अवसंरचना के साथ भौतिक या तार्किक सम्बन्ध है;

(य) **"अप्रचलित आस्ति"** से ऐसी आस्ति अभिप्रेत है जिसे मूल उपकरण निर्माता या मूल उपकरण आपूर्तिकर्ता ने पुराना घोषित कर दिया है, जिसका उत्पादन और सेवाएं बंद कर दी गई हैं, और उसका सहयोग अब उपलब्ध नहीं है, और वह आस्ति तकनीकी तरक्की, प्रचालनात्मक बदलावों के कारण अपने आशयित प्रयोजन के लिए उपयुक्त नहीं है और इससे सुरक्षा या प्रचालनात्मक जोखिम हो सकता है;

(य क) "प्रचालनात्मक प्रौद्योगिकी" से प्रोग्रामेबल हार्डवेयर या प्रणाली अभिप्रेत है जो फिजिकल डिवाइस, प्रक्रिया और इवेंट की सीधी निगरानी या नियंत्रण के माध्यम से बदलावों का पता लगाता है या बदलाव करता है;

(य ख) "प्रोज़्यूमर" से एक ऐसा व्यक्ति अभिप्रेत है, जो ग्रिड से बिजली लेता है और उसी आपूर्ति बिंदु का उपयोग करके वितरण लाइसेंसधारी के लिए ग्रिड में बिजली डाल भी सकता है;

(य ग) "संरक्षित प्रणाली" से 'सूचना प्रौद्योगिकी (संरक्षित प्रणाली के लिए सूचना सुरक्षा प्रथाएं और प्रक्रियाएं) नियम, 2018' नियम 2 के उप-नियम (1) की धारा (ट) में बताई गई परिभाषा के अनुसार 'संरक्षित प्रणाली';

(य घ) "रिमोट एक्सेस" से किसी बाहरी नेटवर्क के माध्यम से किसी संगठन के किसी भी साइबर आस्ति तक पहुंच अभिप्रेत है;

(य ङ) "रिमोट प्रचालन" से किसी संस्था की सूचना प्रौद्योगिकी या परिचालन तकनीक प्रणाली का दिनप्रतिदिन का प्रचालन और नियंत्रण अभिप्रेत है, जो ऐसी प्रणाली से दूर किसी जगह से किया जाता है;

(य च) "स्व लेखा परीक्षा " से किसी संस्था द्वारा एक वित्तीय वर्ष में इन नियमों में विनिर्दिष्ट सभी लागू नियमों के पालन का आकलन करने के लिए लेखा परीक्षा अभिप्रेत है;

(य छ) "संवेदनशील जानकारी" से वह डेटा या जानकारी अभिप्रेत है जिसे अगर बताया जाए, बदला जाए, या नष्ट किया जाए तो किसी संगठन या व्यक्ति की निजता, अखंडता, सुरक्षा या कामकाज पर नकारात्मक प्रभाव पड़ सकता है;

(य ज) "साइट स्वीकृति परीक्षण" से स्थापना पर कार्यात्मक, प्रदर्शन, संविदात्मक और सुरक्षा अपेक्षाओं को सत्यापित करने के लिए किया गया संरचित और दस्तावेजित परीक्षण अभिप्रेत है, और यह सुनिश्चित करना कि कोई प्रणाली या उपकरण और उसके मुख्य घटक, प्रचालनारंभ/चालू करने से पहले, अपने अंतिम प्रचालनात्मक माहौल में जैसा आशयित किया गया है;

(य झ) "उप-क्षेत्रीय कंप्यूटर सुरक्षा घटना मोचन दल" से प्राधिकरण द्वारा नामित एक ऐसी संस्था अभिप्रेत है जो साइबर सुरक्षा से जुड़े मामलों में कंप्यूटर सुरक्षा घटना मोचन दल– विद्युत की सहायता करे;

(य ञ) "तकनीकी मानदंड प्रमाण-पत्र" से किसी संगठन को एक प्राधिकृत प्रमाणन निकाय द्वारा जारी किया गया प्रमाण-पत्र अभिप्रेत है, जो केंद्रीय सरकार द्वारा विनिर्दिष्ट साइबर सुरक्षा मानकों के अनुपालन को सुनिश्चित करने के लिए मान्यता प्राप्त हो;

(य ट) "खतरा" से कोई भी परिस्थिति या घटना अभिप्रेत है जिसमें किसी कमी का फायदा उठाने और किसी साइबर आस्ति या सूचना प्रौद्योगिकीप्रणाली या परिचालन तकनीक प्रणाली की गोपनीयता, अखंडता या उपलब्धता पर नकारात्मक असर डालने की क्षमता हो;

(य ठ) "विश्वसनीय स्रोत" से एक ऐसी मैकेनिजम अभिप्रेत है जिसे खास सुरक्षा अपेक्षाओं, खासकर साइबर सुरक्षा आपूर्ति चेन जोखिमों को कम करने के लिए यह सुनिश्चित करके डिज़ाइन किया गया है, कि विद्युत क्षेत्र से जुड़े उपकरण, निर्माता, सेवाएं और सेवा प्रदाता एक तय मानदंड को पूरा करते हैं;

(य ड) "भेद्यता" से सूचना प्रौद्योगिकी (भारतीय कंप्यूटर आपात मोचन दल और कार्यों तथा कर्तव्यों के निष्पादन की रीति) नियम, 2013 के नियम 2 के उप-नियम (1) के खंड (त) में बताई गई भेद्यता अभिप्रेत है;

(य ढ) "वेंडर" से मूल उपकरण निर्माता, मूल उपकरण आपूर्तिकर्ता, प्रणाली इंटीग्रेटर, मूल उपकरण से जुड़े हार्डवेयर या सॉफ्टवेयर का आपूर्तिकर्ता, ठेकेदार या सेवा प्रदाता, जिसमें क्लाउड सेवा प्रदाता भी शामिल है; और प्रोज़्यूमर के स्वामित्व वाले वितरित उत्पादन संसाधन के मूल उपकरण या कंट्रोल प्रणाली से जुड़े हार्डवेयर, फर्मवेयर या सॉफ्टवेयर का निर्माता और आपूर्तिकर्ता, इसमें इनवर्टर, कम्युनिकेशन मॉड्यूल, मॉनिटरिंग प्रणाली और संबंधित कंट्रोल या एनर्जी मैनेजमेंट सॉफ्टवेयर शामिल हैं, लेकिन ये इन्हीं तक सीमित नहीं हैं।

(2) इन विनियमों में प्रयुक्त लेकिन परिभाषित नहीं किए गए शब्दों और पदों का वही अर्थ होगा जो उनका अधिनियम, उसके अधीन बनाए गए नियमों और विनियमों में है।

अध्याय 2

कंप्यूटर सुरक्षा घटना मोचन दल– विद्युत

4. (1) कंप्यूटर सुरक्षा घटना मोचन दल – विद्युत

(क) विद्युत क्षेत्र से जुड़े साइबर सुरक्षा घटना की रिपोर्टिंग और उन पर कार्रवाई के लिए समन्वय एजेन्सी होगी;

(ख) साइबर सुरक्षा घटना के विश्लेषण, भविष्यवाणी और रोकथाम और उससे संबंधित जानकारी फैलाने के लिए विद्युत क्षेत्र की नोडल एजेंसी होगी;

(ग) किसी भी साइबर सुरक्षा घटना से संबंधित डेटा और जानकारी किसी भी संस्था से इकट्ठा करेगी, जिसमें नेटवर्क संरचना, आस्तियों का विवरण, लॉग्स, साइबर फोरेंसिक रिकॉर्ड, फोरेंसिक इमेज, पॉलिसी और प्रक्रिया, और कोई भी अन्य संबंधित जानकारी उस प्ररूप, रीति और ढंग में शामिल है, जैसा कि इसके द्वारा विनिर्दिष्ट किया गया है:

परंतु इकट्ठा किया गया संवेदनशील डेटा और संवेदनशील जानकारी को भंग होने से बचाया जाएगा और इसका प्रयोग सिर्फ़ अभिहित सरकारी अभिकरणों द्वारा साइबर सुरक्षा के प्रयोग से किया जाएगा, लेकिन संबंधित संस्था को प्रकट संसूचना के बिना किसी तीसरे पक्ष को इसका प्रकटन नहीं किया जाएगा।

(2) विद्युत क्षेत्र में 'कंप्यूटर सुरक्षा घटना मोचन दल- विद्युत' की भूमिकाओं और उत्तरदायित्वों में निम्नलिखित शामिल हैं, अर्थात्:

(क) विद्युत क्षेत्र से संबंधित साइबर घटनाओं, कमज़ोरियों और खतरों को इकट्ठा करना और उनका विश्लेषण करना;

(ख) विद्युत क्षेत्र से संबंधित साइबर सुरक्षा घटनाओं, खतरों और कमज़ोरियों का अनुमान लगाना;

(ग) विद्युत क्षेत्र से जुड़े साइबर सुरक्षा घटना को सुलझाने के लिए भारतीय कंप्यूटर आपात मोचन दल, राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र और केंद्र सरकार द्वारा अभिहित की गई अन्य अभिकरणों के साथ समन्वय और सहयोग करना;

(घ) भारतीय कंप्यूटर आपात मोचन दल, राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र और केंद्रीय सरकार द्वारा साइबर सुरक्षा के क्षेत्र में नामित किसी भी अन्य एजेंसी के साथ मिलकर अलर्ट, एडवाइजरी और दिशानिर्देश के साथ-साथ खतरे की जानकारी जारी करना;

(ङ) भारतीय कंप्यूटर आपात मोचन दल, राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र, उप-क्षेत्रीय कंप्यूटर सुरक्षा घटना मोचन दलों, विद्युत विनियामक आयोगों, संस्थाओं और केंद्रीय सरकार द्वारा साइबर सुरक्षा के क्षेत्र में नामित अन्य अभिकरणों के साथ सलाह करके मानक संचालन प्रक्रियाएं, सुरक्षा नीतियां, उप-क्षेत्र विशिष्ट बेंचमार्क, सुरक्षा नियंत्रण और घटना मोचन गतिविधियों के लिए सर्वोत्तम प्रथाएं बनाना या विकसित करना;

(च) क्षमता निर्माण पहलों और हस्तक्षेपों के माध्यम से साइबर सुरक्षा जागरूकता बढ़ाने के लिए सक्रिय उपाय करना;

(छ) साइबर सुरक्षा निर्धारण, साइबर सुरक्षा संपरीक्षा, प्रमाणीकरण संपरीक्षा, स्व- संपरीक्षा, थर्ड पार्टी संपरीक्षा और मॉक-ड्रिल और सिमुलेशन सहित अभ्यासों द्वारा विद्युत क्षेत्र की साइबर सुरक्षा स्थिति में सुधार सुनिश्चित करना;

(ज) उप-क्षेत्र विशिष्ट साइबर सुरक्षा ढांचा, प्रोटोकॉल और नियम बनाने के लिए समन्वय करना;

(झ) संस्थाओं को उनके साइबर संकट प्रबंधन योजना को तैयार करने में सलाह देना;

(ञ) वास्तविक साइबर संकट के दौरान उनके साइबर संकट प्रबंधन योजना के कार्यान्वयन को सुनिश्चित करने के लिए संस्था के साथ समायोजन करना;

(ट) उद्योग, अनुसन्धान संस्था और एकेडेमिया के साथ मिलकर साइबर सुरक्षा के क्षेत्र में अनुसन्धान एवं विकास को सुविधाजनक बनाना और बढ़ावा देना;

(ठ) केंद्रीय सरकार या प्राधिकरण द्वारा विनिर्दिष्ट साइबर आस्तियों की आपूर्ति चेन की साइबर सुरक्षा सुनिश्चित करने के लिए उपायों को विरचित और कार्यान्वित करना;

(ड) प्राधिकरण द्वारा जारी एक पृथक आदेश के अनुसार, कंप्यूटर सुरक्षा घटना मोचन दल- विद्युत को सहयोग करने के लिए विद्युत क्षेत्र के केंद्रीय साइबर सुरक्षा समन्वय मंच और क्षेत्रीय साइबर सुरक्षा समन्वय मंच स्थापित करना, ताकि साइबर सुरक्षा की स्थिति की समय-समय पर समीक्षा की जा सके, साइबर सुरक्षा की चुनौतियों पर विचार-विमर्श किया जा सके, जानकारी साझा की जा सके, समायोजित प्रत्युत्तर योजना बनाई जा सके और क्षेत्र की कुल स्थिति में सुधार किया जा सके;

(ढ) केन्द्रीय सरकार या प्राधिकरण द्वारा यथानिदेशित विद्युत क्षेत्र में साइबर सुरक्षा से संबंधित मामलों से जुड़े कोई अन्य कार्य।

(3) विद्युत क्षेत्र की साइबर सुरक्षा से जुड़े मामलों में कंप्यूटर सुरक्षा घटना मोचन दल– विद्युत के निदेशों और दिशा-निर्देशों का पालन, संस्थाओं और वेंडरों, जैसे लागू हो, द्वारा किया जाएगा।

(4) प्राधिकरण एक पृथक आदेश के माध्यम से विद्युत क्षेत्र में उत्पादन, पारेषण, वितरण, ग्रिड संचालन और किसी भी अन्य उप-क्षेत्र के लिए उप-क्षेत्रीय कंप्यूटर सुरक्षा घटना मोचन दल को नामित कर सकेगी, साथ ही कंप्यूटर सुरक्षा घटना मोचन दल–विद्युत की सहायता के लिए उनकी भूमिकाएं और जिम्मेदारियां भी तय कर सकेगी।

अध्याय 3

साधारण साइबर सुरक्षा अपेक्षाएं

5. संस्था-

(1) वरिष्ठ प्रबंधन स्तर के नियमित कर्मचारियों को मुख्य सूचना सुरक्षा अधिकारी और वैकल्पिक मुख्य सूचना सुरक्षा अधिकारी के रूप में नियुक्त करेगी;

(2) यह सुनिश्चित करेगी कि मुख्य सूचना सुरक्षा अधिकारी और वैकल्पिक मुख्य सूचना सुरक्षा अधिकारी पद एक ही समय पर रिक्त न रहें;

(3) केंद्रीय सरकार के नियामक रूपरेखा और संबंधित दिशा-निर्देश के अनुसार मुख्य सूचना सुरक्षा अधिकारी और वैकल्पिक मुख्य सूचना सुरक्षा अधिकारी की भूमिकाएं और जिम्मेदारियां तय करेगी;

(4) यह सुनिश्चित करेगी कि मुख्य सूचना सुरक्षा अधिकारी संस्था के प्रमुख को रिपोर्ट करे:

परंतु, यदि कोई संस्था, जैसे कि 'राज्य भार प्रेषण केंद्र', कोई स्वतंत्र संस्था न होकर किसी धृति कंपनी या मूल कंपनी का हिस्सा हो, जो भी लागू हो, तो ऐसी संस्था के लिए एक पृथक 'मुख्य सूचना सुरक्षा अधिकारी' नियुक्त किया जाएगा जो उस धृति कंपनी या मूल कंपनी के प्रमुख को रिपोर्ट करेगा और एक 'वैकल्पिक मुख्य सूचना सुरक्षा अधिकारी' भी नियुक्त किया जाएगा;

(5) यह सुनिश्चित करेगी कि एक कर्मचारी को कम से कम तीन वर्ष की अवधि के लिए मुख्य सूचना सुरक्षा अधिकारी के रूप में नियुक्त किया जाए;

(6) यह सुनिश्चित करेगी कि मुख्य सूचना सुरक्षा अधिकारी की भूमिका केवल साइबर सुरक्षा से संबंधित मामलों के कार्यों तक ही सीमित हो;

(7) मुख्य सूचना सुरक्षा अधिकारी और वैकल्पिक मुख्य सूचना सुरक्षा अधिकारी के संपर्क विवरण सार्वजनिक डोमेन में उपलब्ध कराएगी और उन्हें अद्यतित करेगी और ऐसी जानकारी कंप्यूटर सुरक्षा घटना मोचन दल–विद्युत के साथ-साथ सभी आंतरिक और बाह्य पणधारकों को भी देगी;

(8) यह सुनिश्चित करेगी कि मुख्य सूचना सुरक्षा अधिकारी प्रत्येक वित्तीय वर्ष में कम से कम पांच कार्य-दिवसों के लिए साइबर सुरक्षा प्रशिक्षण पाठ्यक्रम में भाग ले;

(9) भारत में, सभी साइबर सुरक्षा से जुड़े मामलों से निपटने के लिए, मुख्य सूचना सुरक्षा अधिकारी की अध्यक्षता में एक समर्पित सूचना सुरक्षा विभाग स्थापित किया जाएगा और यह चौबीसों घंटे प्रचालन में रहेगा। इसके अलावा-

(क) सूचना सुरक्षा विभाग में पर्याप्त कर्मचारी तैनात किये जायेंगे;

(ख) सूचना सुरक्षा विभाग में तैनात कर्मचारी के पास कार्यक्षेत्र विशिष्ट साइबर सुरक्षा पाठ्यक्रम सफलतापूर्वक पूरा करने का वैध प्रमाणपत्र होगा;

(ग) सूचना सुरक्षा विभाग में तैनात कर्मचारी को प्रत्येक वित्तीय वर्ष में कम से कम पांच कार्यदिवस के लिए विद्युत क्षेत्र से जुड़े साइबर सुरक्षा प्रशिक्षण पाठ्यक्रम में शामिल होना होगा;

(घ) कर्मचारी को सूचना सुरक्षा विभाग में कम से कम तीन वर्ष के कार्यकाल के लिए तैनात किया जाएगा;

(10) में एक तय और प्रलेखित साइबर सुरक्षा नीति हो, जिसे, यथास्थिति, संस्था के प्रमुख या बोर्ड द्वारा हर वर्ष अनुमोदित और समीक्षा किया जाए;

(11) कंप्यूटर सुरक्षा घटना मोचन दल–विद्युत के साथ परामर्श करके एक साइबर संकट प्रबंधन योजना तैयार करें, ताकि सभी संभावित साइबर संकट की स्थितियों से कम से कम समय में और व्यापार प्रचालनों पर कम से कम प्रभाव के साथ निपटा जा सके और उनसे सुरक्षित हो सके;

परंतु साइबर संकट प्रबंधन योजना को भारतीय कंप्यूटर आपातकालीन मोचन दल द्वारा विधीक्षा किया जाएगा और, यथास्थिति, संस्था के प्रमुख या बोर्ड द्वारा इसे मंज़ूरी दी जाएगी और प्रत्येक वर्ष इसकी समीक्षा की जाएगी;

(12) महत्वपूर्ण सूचना अवसंरचना वाले सूचना प्रौद्योगिकी नेटवर्क को इंटरनेट के साथ-साथ बाकी सूचना प्रौद्योगिकी नेटवर्क से पृथक रखना सुनिश्चित करे;

परंतु अगर महत्वपूर्ण सूचना अवसंरचना वाले सूचना प्रौद्योगिकी नेटवर्क के लिए इंटरनेट अपेक्षित हो, तो उसे केंद्रीय सरकार की नामित अभिकरणों द्वारा बताए गए उचित दृढ़ीकरण उपायों के साथ सुरक्षित रूप से सोर्स किया जाएगा;

(13) यह सुनिश्चित करे कि इलेक्ट्रॉनिक सुरक्षा प्राचल पर फ़ायरवॉल सहित सभी अपेक्षित सुरक्षा उपकरण लगाए जाएं, ताकि लगाया गया सुरक्षा प्रणाली पैकेट फ़िल्टरिंग; डीप पैकेट जांच; सामग्री, उपयोगकर्ता और एप्लिकेशन आधारित फ़िल्टरिंग; एन्क्रिप्टेड ट्रैफ़िक का पता लगाने और जांच; घुसपैठ का पता लगाने और रोकथाम; जियो-फेंसिंग; स्वतः हस्ताक्षर और व्यवहार अद्यतन की सुविधा; उपयोगकर्ता नियंत्रित अद्यतन; हस्ताक्षर और व्यवहार में गड़बड़ी के आधार पर पता लगाने, जांच और फ़िल्टरिंग जैसी अपेक्षाओं को पूरा करे;

(14) यह सुनिश्चित करे कि कोई भी वेब सर्विस या वेब-आधारित एप्लिकेशन, जिसमें वेबसाइट, वेब पोर्टल और एप्लिकेशन प्रोग्रामिंग इंटरफ़ेस शामिल हैं, जिनकी सार्वजनिक पहुँच है, उन्हें साइबर सुरक्षा संपरीक्षा मंज़ूरी के बाद ही परिनियोजित किया जाएगा;

परंतु वेब एप्लीकेशन और वेब सेवाओं में कोई भी सॉफ्टवेयर अद्यतन, जिसमें पैच भी शामिल है, सफल परीक्षण और पुष्टि के बाद ही परिनियोजित किया जाएगा, ताकि वह अद्यतन किसी भी साइबर सुरक्षा भेद्यता से मुक्त हो, और यह पुष्टि की जाएगी कि ऐसा अद्यतन किसी भी साइबर जोख़िम से मुक्त है;

परंतु यह और कि साइबर सुरक्षा नीति में बताए गए साइबर सुरक्षा संपरीक्षा की पिछली अपेक्षा को पूरा करने वाला कोई भी सॉफ्टवेयर अद्यतन, उसके साइबर सुरक्षा संपरीक्षा मंज़ूरी के बाद ही परिनियोजित किया जाएगा:

परंतु यह और भी कि इसके अलावा सभी सॉफ्टवेयर अद्यतन, जिनके लिए पहले साइबर सुरक्षा संपरीक्षा की ज़रूरत नहीं है, उनका निर्धारण अगले साइबर सुरक्षा संपरीक्षा के दौरान किया जाएगा;

(15) साइबर सुरक्षा नीति के अधीन बताई गई प्रक्रिया के अनुसार पहचाने गए सभी ज़रूरी वेब एप्लीकेशन के लिए सभी अपेक्षित सुरक्षा उपकरण लगाना सुनिश्चित करे, ताकि लगाया गया सुरक्षा प्रणाली, एप्लीकेशन लेयर फ़िल्टरिंग की अपेक्षाओं को पूरा करे, जिसमें वेब आधारित एन्क्रिप्टेड ट्रैफ़िक का पता लगाना और फ़िल्टर करना; दोनों तरफ़ से सुरक्षा सुनिश्चित करना; स्वचालित हस्ताक्षर और व्यवहार अद्यतन की सुविधा; घुसपैठ का पता लगाना और रोकना, उपयोगकर्ता नियंत्रित अद्यतन क्रियाविधि; सामग्री, उपयोगकर्ता और एप्लीकेशन आधारित फ़िल्टरिंग; भू-फेंसिंग; हस्ताक्षर और व्यवहार जन्य गड़बड़ियों के आधार पर एन्क्रिप्टेड ट्रैफ़िक का पता लगाना, जांच करना और फ़िल्टर करना शामिल हैं;

(16) साइबर सुरक्षा नीति में बताई गई प्रक्रिया के अनुसार, प्रणाली को महत्वपूर्ण और कम महत्वपूर्ण प्रणाली के रूप में पहचाने और पृथक करे;

(17) यह सुनिश्चित करे कि साइबर आस्तियों तक रिमोट पहुँच, यदि आवश्यक हो, तो साइबर सुरक्षा नीति के अधीन विनिर्दिष्ट प्रक्रिया के अनुसार, केवल समस्या निवारण और आपातकालीन अपेक्षाओं के लिए ही दिया जाए:

परंतु कम महत्वपूर्ण प्रणाली से जुड़े साइबर आस्तियों के लिए ऐसी पहुँच, केवल समस्या निवारण और आपातकालीन अपेक्षाओं के लिए, मुख्य सूचना सुरक्षा अधिकारी की मंज़ूरी के साथ और उचित सुरक्षा नियंत्रण उपायों के साथ ही दिया जा सकेगा:

परंतु यह और कि महत्वपूर्ण प्रणाली या उनके साइबर आस्तियों तक ऐसे पहुँच के लिए मंज़ूरी एक व्यापक जोखिम निर्धारण करने और उसके प्रभावी उपायों की पहचान करने के बाद ही दी जा सकेगी, और

ऐसे पहुँच की निरंतर निगरानी की जाएगी ताकि किसी भी गड़बड़ी या अनधिकृत उपयोग के प्रयासों का पता लगाया जा सके:

परंतु यह और भी कि इसके अलावा जोखिम मूल्यांकन का रिकॉर्ड, मंज़ूरी का भौतिक दस्तावेज़ और महत्वपूर्ण प्रणाली तक ऐसे प्रत्येक पहुँच से संबंधित लॉग को डेटा प्रतिधारण नीति में विनिर्दिष्ट अवधि के लिए बनाए रखा जाएगा;

(18) प्रत्येक छह महीने में कम से कम एक बार साइबर सुरक्षा जागरूकता कार्यक्रम और साइबर सुरक्षा अभ्यास आयोजित करे, जिसमें मॉक-ड्रिल और टेबलटॉप अभ्यास शामिल हैं;

(19) यह सुनिश्चित करे कि संवेदनशील जानकारी और संवेदनशील डेटा, जिसमें क्लाउड पर होस्ट किया गया ऐसा डेटा और जानकारी, साथ ही ऐसा ऐतिहासिक डेटा और जानकारी शामिल है, एक एन्क्रिप्टेड, सुरक्षित, और संरक्षित माहौल में संग्रहित किया जाए और केवल भारत में ही रहे;

(20) साइबर सुरक्षा नीति के अधीन, यथाविनिर्दिष्ट, वेंडरों के साथ सेवा स्तरीय अनुबंध में सभी साइबर सुरक्षा अपेक्षाओं के साथ-साथ केंद्रीय सरकार द्वारा जारी लागू साइबर सुरक्षा नियमों, विनियमों और गैर प्रकटीकरण अनुबंध को शामिल करे, ताकि उनके संविदा की अवधि के दौरान और ऐसी संविदा अवधि पूरी होने के बाद भी संवेदनशील जानकारी की गोपनीयता, अखंडता और उपलब्धता सुनिश्चित की जा सके:

परंतु महत्वपूर्ण प्रणाली तक साइबर या भौतिक पहुँच या दोनों रखने वाले वेंडर को, जिसमें ऐसे प्रणाली के संचालन या रखरखाव या दोनों के लिए लगाए गए वेंडर के कर्मचारी शामिल हैं, कार्मिक जोखिम निर्धारण करने और उसके बाद किए गए निवारक उपायों के साथ-साथ सेवा स्तरीय अनुबंध का पालन करने वाले एक वचनपत्र के बाद अनुमति दी जा सकेगी:

परंतु यह और कि इसके अलावा किसी भी साइबर सुरक्षा उल्लंघन के मामले में, संस्था मामले की जांच करेगी और ऐसे वेंडर, जिसमें क्लाउड सर्विस प्रदाता भी शामिल हैं, जिन्होंने साइबर सुरक्षा उल्लंघन किया है, के विरुद्ध कार्रवाई आरंभ करेगी;

(21) साइबर सुरक्षा नीति में यथाविनिर्दिष्ट, सभी महत्वपूर्ण प्रणाली का ऑनलाइन और ऑफलाइन बैकअप एक पृथक, सुरक्षित और संरक्षित माहौल में सुनिश्चित करे;

(22) विनियम 13 के अधीन यथाविनिर्दिष्ट सभी महत्वपूर्ण प्रणाली को शामिल करते हुए प्रत्येक वित्तीय वर्ष में कम से कम एक बार एक व्यापक साइबर सुरक्षा संपरीक्षा की सुविधा प्रदान करे, लेकिन दो लगातार साइबर सुरक्षा संपरीक्षा के बीच क्रमशः कम से कम नौ महीने और अधिकतम पंद्रह महीने का अंतर हो:

परंतु संस्था द्वारा नियुक्त साइबर सुरक्षा संपरीक्षा संस्था अपने योग्य कर्मियों को तैनात करेगी, लेकिन ऐसी संस्था के लिए तैनात किसी भी कर्मचारी को छोड़कर, यदि कोई हो:

परंतु यह और कि इसके अलावा लगातार तीन ऐसे संपरीक्षा एक ही संपरीक्षा संस्था या कर्मियों द्वारा नहीं किए जाएंगे;

(23) यह सुनिश्चित करे कि खरीदे गए सभी सूचना प्रौद्योगिकी उत्पाद केंद्रीय सरकार द्वारा जारी आदेशों के अनुपालन में हों और इन आदेशों के पालन में उनका परीक्षण किया गया हो;

(24) सभी महत्वपूर्ण प्रणाली को शामिल करते हुए आईएसओ/आईइसी 27001 प्रमाणपत्र या तकनीकी मानदंड प्रमाणपत्र का अनुपालन सुनिश्चित करे और प्राप्त करे:

परंतु आईएसओ 27001 या तकनीकी मानदंड प्रमाणपत्र के प्रमाणन के लिए निरंतर चार संपरीक्षा एक ही संपरीक्षा एजेंसी या कर्मियों द्वारा नहीं किए जाएंगे;

(25) आस्ति रजिस्टर बनाए रखे-

(क) जिसमें साइबर सुरक्षा नीति में परिभाषित प्रक्रिया के अनुसार, सभी साइबर आस्ति के लिए, स्वामित्व, हार्डवेयर, फर्मवेयर, सॉफ्टवेयर और पैच सहित ज़रूरी विवरण शामिल हों;

(ख) जिसमें सभी महत्वपूर्ण प्रणाली का विवरण रिकॉर्ड करना, उसका विन्यास, हार्डवेयर, सॉफ्टवेयर, डेटा प्रवाह दिखाने वाला नेटवर्क स्थापत्य और उसमें इस्तेमाल होने वाले संचार प्रोटोकाल शामिल हों:

परंतु ऐसे रजिस्टर की समीक्षा और अद्यतन प्रत्येक वित्तीय वर्ष में कम से कम एक बार या किसी नए साइबर आस्ति या महत्वपूर्ण प्रणाली के चालू होने पर, जिसमें उनके प्रतिस्थापन भी शामिल हैं, जो भी पहले हो, किया जाएगा;

(26) साइबर आस्ति रजिस्टर में बताए गए सभी आस्तियों के लिए, साइबर सुरक्षा नीति में बताई गयी प्रक्रिया के अनुसार साइबर जोखिम निर्धारण और शमन योजना बनाए रखे:

परंतु साइबर जोखिम निर्धारण और शमन योजना को प्रत्येक छह महीने में कम से कम एक बार अद्यतन किया जाएगा और प्रत्येक वित्तीय वर्ष में कम से से एक बार पुनर्वलोकन किया जाएगा और ऐसे साइबर जोखिम आकलन और शमन योजना को उससे जुड़ी कमजोरियों, खतरों और जोखिमों को प्रबंधित करने के लिए क्रियान्वित किया जाएगा;

(27) यह सुनिश्चित करे कि किसी भी नए महत्वपूर्ण प्रणाली को चालू करने से पहले, जिसमें ऐसे प्रणाली को बदलना भी शामिल है, साइबर सुरक्षा संपरीक्षा, जिसमें भेद्यता आंकलन और प्रवेश जांच शामिल है, किया जाए और साइबर सुरक्षा नीति में बताए गए परिभाषित अनुसार महत्वपूर्ण प्रणाली के लिए भेद्यता और जोखिम को प्रबंधित किया जाए;

(28) चालू किए गए सभी नए महत्वपूर्ण प्रणाली, जिनमें बदले गए प्रणाली भी शामिल हैं, की ज़रूरी जानकारी, जिसमें प्रणाली विवरण और कार्यक्षमता शामिल हैं, महत्वपूर्ण प्रणाली से जुड़े आस्ति रजिस्टर के अनुसार, ऐसे चालू होने या बदलने के तीस दिनों के अंदर कंप्यूटर सुरक्षा घटना मोचन दल– विद्युत को दे;

(29) महत्वपूर्ण सूचना अवसंरचना की पहचान के लिए राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र को सुसंगत जानकारी प्रदान करे। इसके अतिरिक्त, राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र द्वारा किसी आस्ति को महत्वपूर्ण सूचना अवसंरचना के रूप में पहचाने जाने के साठ दिनों के भीतर, संस्था ऐसी आस्ति को संरक्षित प्रणाली के रूप में अधिसूचित करने के लिए समुचित सरकार से संपर्क करे;

(30) यह सुनिश्चित करे कि महत्वपूर्ण सूचना अवसंरचना और संरक्षित प्रणाली प्रणाली सार्वजनिक प्लेटफार्मों पर उपलब्ध न हों, जब तक कि संस्था के प्रमुख या बोर्ड द्वारा, लागू होने के अनुसार, व्यावसायिक अपेक्षाओं, महत्व और प्रणाली के जोखिम मूल्यांकन के आधार पर अनुमोदित न किया गया हो;

(31) यह सुनिश्चित करे कि खरीद प्रक्रिया में फैक्ट्री स्वीकृति परीक्षण और साइट स्वीकृति परीक्षण को शामिल करना अनिवार्य हो, जिसमें सायबर सुरक्षा अपेक्षाओं का परीक्षण शामिल हो;

(32) यह सुनिश्चित करे कि सूचना प्रौद्योगिकी और परिचालन तकनीक प्रणाली के भीतर सभी संबंधित सूचना प्रसंस्करण प्रणालियों के क्लॉक, लागू होने के अनुसार, साइबर सुरक्षा नीति में दिए गए संदर्भ समय स्रोत के साथ तुल्यकालन हों:

परंतु ऐसे संदर्भ समय स्रोत के चयन से पहले, विस्तृत साइबर जोखिम निर्धारण किया जाएगा;

(33) यह सुनिश्चित करे कि सभी कर्मियों, जिनमें वेंडर्स द्वारा सभी महत्वपूर्ण प्रणालियों के दैनिक संचालन और रखरखाव में लगे कर्मी भी शामिल हैं, ने विद्युत क्षेत्र से संबंधित निर्दिष्ट साइबर सुरक्षा पाठ्यक्रम अनिवार्य रूप से संपन्न किए हों;

(34) यह सुनिश्चित करे कि महत्वपूर्ण प्रणालियों की भौतिक सुरक्षा से संबंधित प्रणालियाँ, नेटवर्क, और अनुप्रयोग ऐसी महत्वपूर्ण प्रणालियों के नेटवर्क से भौतिक रूप से पृथक हों:

परंतु यदि ऐसा भौतिक पृथक्करण संभव न हो, तो संस्था के प्रमुख की स्वीकृति से, संबंधित प्रणालियों, नेटवर्क, और अनुप्रयोगों को ऐसी महत्वपूर्ण प्रणालियों के नेटवर्क से तार्किक रूप से पृथक किया जाएगा;

(35) साइबर सुरक्षा नीति में यथाविनिर्दिष्ट, साइबर घटनाओं से उबरने और जल्द से जल्द सामान्य संचालन फिर से आरंभ करने के लिए घटना मोचन और पुनर्प्राप्ति योजना बनाए रखे:

परंतु ऐसी योजना की प्रत्येक छह महीने में कम से कम एक बार समीक्षा और अद्यतन किया जाएगा;

(36) खतरों के साथ-साथ भेद्यताओं की पहचान के लिए सूचना प्रौद्योगिकी प्रणाली और परिचालन तकनीक प्रणाली, जैसा लागू हो, की निगरानी और लगातार मॉनिटरिंग करे, और घटना मोचन और समाधान सहायता प्रदान करे;

(37) यह सुनिश्चित करे कि इलेक्ट्रॉनिक सुरक्षा परिधि में मौजूद सभी सुरक्षा उपकरणों के लॉग सक्षम हों ताकि ऐसे उपकरणों से संचालित वाले डेटा और सूचना के आदान-प्रदान को रिकॉर्ड किया जा सके;

(38) परिधि सुरक्षा उपकरणों के नियमों और नीतियों की नियमित, कम से कम प्रत्येक वर्ष एक बार, समीक्षा और अद्यतन सुनिश्चित करे;

(39) यह सुनिश्चित करे कि सूचना प्रौद्योगिकी उपकरण और सेवाएं केन्द्रीय सरकार द्वारा समय-समय पर जारी किए गए आदेशों, निर्देशों या दिशानिर्देशों के अनुसार विश्वसनीय स्रोतों से खरीदी जाएं;

(40) इन विनियमों के अलावा, सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) के अधीन जारी निर्देशों और अपेक्षाओं और उसके अधीन बनाए गए सभी नियमों और विनियमों का पालन करे;

(41) वेंडर्स और कंप्यूटर सुरक्षा घटना मोचन दल- विद्युत के साथ संरचित भेद्यता प्रकटीकरण और प्रबंधन कार्यक्रम रखे;

(42) कंप्यूटर सुरक्षा घटना मोचन दल- विद्युत द्वारा निर्धारित प्रारूप के अनुसार, सभी साइबर सुरक्षा घटनाओं को प्रासंगिक विवरणों के साथ रिकॉर्ड करने के लिए एक रजिस्टर बनाए रखे।

अध्याय 4

परिचालन तकनीक प्रणाली से संबंधित संस्थाओं के लिए अतिरिक्त साइबर सुरक्षा अपेक्षाएं

6. विनियमन 5 के अधीन संस्था के लिए आवश्यक अनिवार्यताओं के अलावा, संस्था-

(1) यह सुनिश्चित करे कि परिचालन तकनीक प्रणाली को इंटरनेट के साथ-साथ सूचना प्रौद्योगिकी प्रणाली से भौतिक रूप से पृथक रखा जाए:

परंतु यदि व्यापार की अपेक्षाओं के कारण सूचना प्रौद्योगिकी प्रणाली से ऐसा अलगाव संभव नहीं है, तो साइबर सुरक्षा नीति में परिभाषित प्रक्रिया के अनुसार, ऐसे सूचना प्रौद्योगिकी और परिचालन तकनीक परस्पर संबंध की परिचालन तकनीक प्रणाली और सूचना प्रौद्योगिकी प्रणाली के बीच उचित मज़बूत तार्किक पृथक्कीकरण के साथ, ऐसे परस्पर संबंध के जोखिम आंकलन और संस्था के प्रमुख या बोर्ड की मंज़ूरी के आधार पर, जैसा भी लागू हो, अनुमति दी जा सकेगी:

परंतु यह और कि ऐसे परस्पर संबंध की निरंतर निगरानी की जाए ताकि अनुचित गतिविधियों का पता लगाया जा सके और उनके लिए सुधारात्मक उपाय किए जा सकें:

परंतु यह और भी कि इसके अलावा, ऐसी मंज़ूरी और ऐसे परस्पर संबंध से जुड़े लॉग को डेटा प्रतिधारण नीति में बताई गई अवधि के लिए रखा जाएगा;

(2) यह सुनिश्चित करे कि विद्युत प्रणाली के संपर्क प्रणाली के साथ परिचालन तकनीक प्रणाली के परस्पर संबंध के बिंदु पर उपयुक्त परिधि स्तरीय साइबर सुरक्षा उपकरण, जिसमें फ़ायरवॉल शामिल है, की स्थापना हो, ताकि स्थापित सुरक्षा प्रणाली, अन्य अपेक्षाओं के अलावा, परिचालन तकनीक से संबंधित नियम और ट्रैफ़िक

का पता लगाने और फ़िल्टर करने; सामग्री, उपयोगकर्ता और एप्लिकेशन आधारित फ़िल्टरिंग; डीप पैकेट जांच, घुसपैठ का पता लगाने; जियो-फेंसिंग; उपयोगकर्ता नियंत्रित अद्यतन; हस्ताक्षर और व्यवहार संबंधी विसंगतियों के आधार पर पता लगाने और उन्हें फ़िल्टर करने की अपेक्षाओं को पूरा करें:

परंतु ऐसे सुरक्षा प्रणाली का हिस्सा बनने वाले उपकरण के लिए हस्ताक्षर सहित अद्यतन, साइबर सुरक्षा नीति में यथाविनिर्दिष्ट, ऑफ़लाइन मोड में किए जाएंगे;

(3) यह सुनिश्चित करे कि विद्युत प्रणाली के तत्वों का नियंत्रण और प्रचालन और उनकी जानकारी का आदान-प्रदान, जिसमें रियल टाइम डेटा शामिल है, इंटरनेट से पृथक एक समर्पित संचार चैनल पर होगा जो परिधि स्तरीय साइबर सुरक्षा उपकरण के माध्यम से होगा और यह केवल राष्ट्रीय सीमाओं तक ही सीमित रहेगा:

परंतु जिन संस्थाओं की कारबार अपेक्षाएं हैं या जिनके सीमा पार विद्युत प्रणाली तत्व हैं, उनके लिए साइबर सुरक्षा नीति के अधीन पहचानी गई जानकारी और वास्तविक समय डेटा का आदान-प्रदान राष्ट्रीय सीमाओं से परे एक समर्पित पृथक संचार प्रणाली और एकदिशीय गेटवे के माध्यम से भेजने और पाने के लिए, इंटरनेट से पृथक और साइबर सुरक्षा उपकरणों के साथ, अनुमति दी जा सकेगी, इस शर्त के साथ कि ऐसी जानकारी और डेटा की लगातार निगरानी की जाए ताकि किसी भी गड़बड़ी या अनधिकृत प्रयास का पता लगाया जा सके:

परंतु यह और कि अंतिम उपभोक्ताओं से संबंधित वास्तविक समय जानकारी और डेटा के आदान-प्रदान के मामले में, इसे सार्वजनिक पहुंच से पृथक, सुरक्षित कनेक्शन के माध्यम से अनुमति दी जा सकेगी, इस शर्त के अधीन कि ऐसे कनेक्शन पर संवेदनशील जानकारी और डेटा का आदान-प्रदान उसकी गोपनीयता, अखंडता और निजता सुनिश्चित करने के लिए एन्क्रिप्टेड होगा;

(4) यह सुनिश्चित करे कि यदि कारबार अपेक्षाओं के लिए रिमोट ऑपरेशन आवश्यक है, तो यह संस्था के प्रमुख या बोर्ड की पूर्व मंज़ूरी के साथ, जैसा भी लागू हो, साइबर सुरक्षा नीति में विनिर्दिष्ट प्रक्रिया के अनुसार, इंटरनेट से पृथक एक समर्पित संचार चैनल के माध्यम से, विनियमन 6(3) के अधीन अनिवार्य साइबर सुरक्षा प्रणाली के साथ भारत के भीतर ही होगा;

(5) यह सुनिश्चित करे कि विद्युत प्रणाली के नियंत्रण और प्रचालन के लिए उपयोग किए जाने वाले सभी परिचालन तकनीक उपकरण, अवयव और उनके हिस्से केंद्रीय सरकार द्वारा जारी किए गए आदेशों का पालन करेंगे;

(6) यह सुनिश्चित करे कि परिचालन तकनीक प्रणाली की संचार प्रणाली सूचना प्रौद्योगिकी प्रणाली की संचार प्रणाली से पृथक हो;

(7) यह सुनिश्चित करे कि परिचालन तकनीक उपकरण और सेवाएँ केंद्रीय सरकार द्वारा समय-समय पर जारी किए गए आदेशों, निर्देशों या दिशानिर्देशों के अनुसार विश्वसनीय स्रोतों से उपाप्त की जाएँ;

(8) यह सुनिश्चित करे कि परिचालन तकनीक पर्यावरण को महत्ता, सुरक्षा अपेक्षाओं और जोखिम मूल्यांकन के आधार पर पृथक-पृथक ट्रस्ट स्तर में बाँटा गया हो;

(9) यह सुनिश्चित करे कि संचार प्रणाली, विशेष रूप से चैनल, जो दो संस्थाओं के बीच परिचालन तकनीक डेटा और जानकारी प्रदान करता है, ऐसे प्रणाली के धारक द्वारा साइबर सुरक्षा खतरों से संरक्षित हो।

अध्याय 5

मुख्य सूचना सुरक्षा अधिकारी और सूचना सुरक्षा विभाग के कार्य

7. (1) मुख्य सूचना सुरक्षा अधिकारी और वैकल्पिक मुख्य सूचना सुरक्षा अधिकारी भारत के नागरिक और निवासी होने चाहिए और उनके पास किसी मान्यता प्राप्त संस्थान से इंजीनियरिंग या समकक्ष डिग्री होनी चाहिए, साथ ही विद्युत क्षेत्र या सूचना प्रौद्योगिकी के क्षेत्र में कम से कम पंद्रह वर्ष का अनुभव होना चाहिए;

इन विनियमनों में निहित किसी भी बात के होते हुए भी, प्राधिकरण पृथक-पृथक आदेशों के माध्यम से संस्था के मुख्य सूचना सुरक्षा अधिकारी के लिए अतिरिक्त अर्हताएं तय कर सकती है;

परंतु मुख्य सूचना सुरक्षा अधिकारी की अनुपस्थिति में, मुख्य सूचना सुरक्षा अधिकारी की भूमिकाएं और उत्तरदायित्व वैकल्पिक मुख्य सूचना सुरक्षा अधिकारी द्वारा निभाई और पूरी की जाएंगी।

(2) मुख्य सूचना सुरक्षा अधिकारी-

(क) साइबर सुरक्षा से संबंधित सभी मामलों के लिए नोडल अधिकारी होगा;

(ख) साइबर सुरक्षा से संबंधित मामलों से जुड़े सभी संबंधित पणधारकों के साथ समन्वय करेगा;

(3) सूचना सुरक्षा विभाग की सहायता से मुख्य सूचना सुरक्षा अधिकारी के कार्यों में, अन्य बातों के अलावा, निम्नलिखित शामिल होंगे:

(क) साइबर सुरक्षा घटनाओं की रिपोर्ट छह घंटे के भीतर कंप्यूटर सुरक्षा घटना मोचन दल– विद्युत और भारतीय कंप्यूटर आपातकालीन मोचन दल को देना;

परंतु यदि किसी घटना को महत्वपूर्ण प्रणाली में साइबर सबोटाज के रूप में निष्कर्ष निकाला जाता है, तो इसकी रिपोर्ट चौबीस घंटे के भीतर दी जाएगी;

(ख) साइबर सुरक्षा नीति में आज्ञापक रूप से किए गए अनुपालनों की तिमाही समीक्षा;

(ग) साइबर सुरक्षा नीति में विनिर्दिष्ट महत्वपूर्ण प्रणाली के लिए साइबर सुरक्षा नियंत्रण उपायों को लागू करना, जिससे उनकी साइबर परिवर्तनीयता सुदृढ़ हो सके;

(घ) महत्वपूर्ण सूचना अवसंरचना या संरक्षित प्रणाली के मामले में, राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र के दिशानिर्देशों के अनुसार मान्य साइबर सुरक्षा नियंत्रण उपायों को लागू करना;

(ङ) केंद्रीय सरकार, प्राधिकरण, भारतीय कंप्यूटर आपातकालीन मोचन दल और कंप्यूटर सुरक्षा घटना मोचन दल– विद्युत द्वारा जारी साइबर सुरक्षा से संबंधित निर्देशों, दिशानिर्देशों और सलाह पर कार्रवाई करना;

(च) साइबर खतरे की खुफिया जानकारी इकट्ठा करना, उसका विश्लेषण, खतरे के वेक्टर की पहचान, साइबर सुरक्षा जोखिमों का आकलन और उनके शमन के उपाय करना;

(छ) प्राप्त की गयी साइबर सुरक्षा घटनाओं की विस्तृत रिपोर्ट, की गई कार्रवाई की रिपोर्ट, मूल कारण विश्लेषण और अन्य सुसंगत जानकारी कंप्यूटर सुरक्षा घटना मोचन दल–विद्युत और भारतीय कंप्यूटर आपातकालीन मोचन दल के साथ साझा करना;

(ज) डेटा प्रतिधारण नीति में विनिर्दिष्ट रीति से, रूप और अवधि के अनुसार सभी साइबर सुरक्षा से संबंधित डेटा, सूचना और दस्तावेजों को रखना;

(झ) इन विनियमों की पहली अनुसूची में विनिर्दिष्ट सभी दस्तावेजों का संरक्षण करना;

(ञ) साइबर सुरक्षा नीति में प्रदान किए गए पैच के साथ, सभी महत्वपूर्ण प्रणाली के फर्मवेयर और सॉफ्टवेयर के अद्यतन को सुनिश्चित करना;

(ट) सभी सूचना और संचार प्रौद्योगिकी प्रणाली के लॉग और साइबर सुरक्षा घटनाओं से संबंधित फोरेंसिक रिकॉर्ड को, साइबर सुरक्षा नीति में बताई गई अवधि के लिए संरक्षित करना सुनिश्चित करना;

(ठ) कंप्यूटर सुरक्षा घटना मोचन दल– विद्युत को ज़रूरी जानकारी देना, जिसमें आवंटित किए गए, उपयोग किए गए और उपयोग न किए गए पब्लिक आईपी शामिल हैं;

(ड) महत्वपूर्ण प्रणाली के दिनप्रतिदिन के प्रचालनों की यादृच्छिक जांच यह सुनिश्चित करने के लिए करना कि वे साइबर सुरक्षा नीति के अनुरूप हैं और सुधारात्मक उपाय करना;

(ढ) अनावश्यक प्रणाली से जुड़े साइबर आस्तियों तक रिमोट पहुँच को आसान बनाने के लिए एक प्रक्रिया तैयार

करना, जिससे गड़बड़ी ठीक करने वालों और आपातकालीन अपेक्षाओं को पूरा किया जा सके, जिसमें ज़रूरी सुरक्षा नियंत्रण और ऐसे पहुँच के लिए मंज़ूरी देने की प्रक्रिया शामिल है;

(ण) साइबर सुरक्षा नीति में बताए अनुसार, परिचालन तकनीक प्रणाली के सुरक्षित रिमोट ऑपरेशन और उसके अद्यतन को आसान बनाने के लिए एक प्रक्रिया तैयार करना;

(त) साइबर सुरक्षा नीति, साइबर संकट प्रबंधन योजना, डेटा प्रतिधारण नीति, और बैकअप नीति के विकास, कार्यान्वयन, समीक्षा और अद्यतन को सुनिश्चित करना;

(थ) साइबर आस्तियों और महत्वपूर्ण प्रणाली के साथ-साथ साइबर जोखिम आकलन और शमन योजना के लिए आस्ति रजिस्टर तैयार करना, अद्यतन करना और समीक्षा करना सुनिश्चित करना;

(द) साइबर सुरक्षा नीति के अधीन बताए गए अनुसार, सभी सूचना प्रौद्योगिकी प्रणाली और परिचालन तकनीक प्रणाली को संदर्भ समय स्रोत के साथ तुल्यकालन करना सुनिश्चित करना;

अध्याय 6

साइबर सुरक्षा नीति

8. साइबर सुरक्षा नीति को संस्था के व्यापार निरंतरता योजना के साथ संरेखित किया जाएगा, जिसमें परिचालन तकनीक और सूचान प्रौद्योगिकी वातावरण, जैसा लागू हो, शामिल होगा, और इसमें ये शामिल हो सकते हैं-

(1) परिभाषित प्रयोजन और परिधि, साथ ही सभी लागू साइबर सुरक्षा अपेक्षाएं और उनका पालन;

(2) संरक्षित प्रणाली के लिए, राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र दिशानिर्देशों और नियंत्रण आवश्यकताओं के साथ संरेखन सुनिश्चित करने वाले उपबंध;

(3) संबंधित आंतरिक और बाहरी पणधारकों की परिभाषित भूमिकाएँ और उत्तरदायित्व;

(4) सभी साइबर आस्तियों का साइबर आस्ति रजिस्टर तैयार करने की परिभाषित प्रक्रिया, जिसमें सभी साइबर आस्तियों और साइबर जोखिम आकलन और शमन योजना में पहचाने गए उनकी गंभीरता और जोखिम के आधार पर उनका वर्गीकरण शामिल है; और ऐसी प्रक्रिया को सभी साइबर आस्तियों की विस्तृत दृश्यता और प्रबंधन के लिए अद्यतन करना;

(5) व्यवसाय निरंतरता योजना पर उनके प्रभाव पर विचार करते हुए एक परिभाषित मानदंड के आधार पर सभी प्रणालियों की पहचान करने और ऐसी प्रणालियों को महत्वपूर्ण प्रणालियों के रूप में वर्गीकृत करने के लिए परिभाषित प्रक्रिया, साथ ही एक रजिस्टर में ऐसी प्रणालियों के विवरण को दर्ज करनाः

परंतु ऐसी प्रक्रिया की समीक्षा की जाएगी और प्रत्येक वित्तीय वर्ष में कम से कम एक बार अद्यतन किया जाएगा;

(6) प्रत्येक साइबर आस्ति और उससे जुड़े जोखिम के विरुद्ध भेद्यताओं और खतरों की पहचान करने के लिए साइबर जोखिम मूल्यांकन और शमन योजना के लिए परिभाषित प्रक्रिया, ऐसे जोखिमों और उनके कार्यान्वयन की महत्वपूर्णता के अनुरूप नियंत्रण और शमन उपायः

परंतु ऐसी प्रक्रिया की समीक्षा की जाएगी और प्रत्येक वित्तीय वर्ष में कम से कम एक बार अद्यतन किया जाएगा;

(7) महत्वपूर्ण प्रणाली में कमजोरियों और जोखिमों को प्रबंधित करने के लिए परिभाषित तंत्र, जिसमें ऐसे प्रणाली में कमियों और खतरों की समय पर पहचान करना शामिल है, जिसमें आंतरिक और बाहरी स्रोतों से संबंधित जानकारी प्राप्त करना, ऐसी जानकारी का विश्लेषण, जोखिम मूल्यांकन और उसका प्रबंधन शामिल है:

परंतु ऐसे तंत्र की समीक्षा और उसे हर वित्तीय वर्ष में कम से कम एक बार या किसी भी नए महत्वपूर्ण प्रणाली के चालू होने पर, जिसमें उसका प्रतिस्थापन भी शामिल है, जो भी पहले हो, अद्यतन किया जाएगा;

(8) महत्वपूर्ण प्रणाली में साइबर नुकसान की पहचान करने और रिपोर्ट करने की प्रक्रिया, जिसमें आंतरिक और बाहरी पणधारकों से ऐसी जानकारी प्राप्त करना शामिल है;

(9) परिभाषित घटना मोचन और पुनर्प्राप्ति योजना, जिसमें सभी प्रकार की घटनाओं की सूची, जोखिम विश्लेषण, और प्रभावित प्रणाली की प्रभावी और समय पर बहाली के लिए जोखिम-आधारित घटना-विशिष्ट मोचन योजना का विवरण दिया गया है:

परंतु कोई ऐसी घटना जिसके लिए संस्था स्तर कार्यनीतिक पुनर्प्राप्ति योजना की ज़रूरत हो, उसे संकट के रूप में वर्गीकृत किया जाएगा;

(10) महत्वपूर्ण प्रणाली के दिनप्रतिदिन के प्रचालनों की यादृच्छिक जाँच के लिए प्रणाली, जिससे वे साइबर सुरक्षा के क्षेत्र में केंद्र सरकार द्वारा नामित कंप्यूटर सुरक्षा घटना मोचन दल– विद्युत और अन्य अभिकरणों द्वारा जारी लागू नीतियों, नियमों और विनियमों के अनुरूप हों:

परंतु ऐसी जांच से ऐसे प्रणाली के प्रचालनों और कार्यक्षमता और उनकी सुरक्षा में कोई रुकावट न आए;

(11) महत्वपूर्ण प्रणाली और उनसे जुड़े साइबर आस्तियों, सार्वजनिक पहुँच वाले एप्लिकेशन, संवेदनशील जानकारी और संवेदनशील डेटा के लिए पहुँच नियंत्रण प्रणाली, प्रमाणीकरण, प्राधिकृत और अकाउंटिंग मानदंडों और उनकी आवश्यकता के सिद्धांतों के आधार पर पहुँच प्रबंधन द्वारा नियंत्रित किया जाएगा:

परंतु डेटा प्रतिधारण नीति के अधीन निर्दिष्ट दस्तावेज़ और रिकॉर्ड्स तक भौतिक और तार्किक पहुँच को प्रतिबंधित करने के लिए एक विस्तृत प्रक्रिया अभिकथित की जा सकती है;

(12) वेंडर द्वारा तैनात कर्मियों से जुड़े जोखिमों की पहचान करने के लिए कार्मिक जोखिम मूल्यांकन प्रक्रिया, जिनके पास महत्वपूर्ण प्रणाली और उनसे जुड़े आस्तियों तक अधिकृत साइबर या भौतिक पहुँच है या जो ऐसे प्रणाली के संचालन या रखरखाव या दोनों के लिए लगे हुए हैं, उनकी भूमिकाओं और उत्तरदायित्वों के आधार पर, जिसमें ऐसी भूमिकाओं और उत्तरदायित्वों में बदलाव शामिल है; और इसके शमन उपाय:

परंतु, दिनप्रतिदिन के संचालन और रखरखाव में लगे कर्मचारियों के लिए या जिनके पास आवश्यक प्रणाली और उनसे जुड़े आस्तियों तक अधिकृत साइबर या भौतिक पहुँच है, उनके रोजगार से समाप्ति, इस्तीफे और सेवा-निवृत्ति के बाद, उनके द्वारा निभाई गई भूमिकाओं और ऐसे सौंपे गए कार्यों में तैनाती की अवधि के आधार पर कार्मिक जोखिम मूल्यांकन किया जाएगा;

(13) यह सुनिश्चित करने के लिए कार्य विधि कि महत्वपूर्ण प्रणाली के सभी पहुँच बिंदु भौतिक रूप से सुरक्षित हैं और लगातार निगरानी किए जाते हैं और साथ ही इन प्रणाली और उनसे जुड़े साइबर आस्तियों की भौतिक सुरक्षा के लिए ऐसे पहुँच को प्रतिबंधित किया जाता है:

परंतु इनमें से किसी भी प्रणाली या उसके आस्तियों को भौतिक नुकसान के किसी भी संभावित खतरे के मामले में, ऐसे प्रणाली या आस्ति के लिए किसी भी व्यक्ति को दिया गया भौतिक पहुँच रद्द किया जा सकता है;

(14) महत्वपूर्ण प्रणाली और उनसे जुड़ी सेवाओं की सप्लाई चेन से जुड़े साइबर सुरक्षा जोखिमों की पहचान करने और उनका आकलन करने के लिए साइबर सप्लाई चेन जोखिम प्रबंधन प्रक्रिया, साथ ही उन्हें कम करने के उपाय;

(15) साइबर आस्तियों तक रिमोट पहुँच के लिए तय प्रक्रिया, साथ ही उनकी महत्ता के आधार पर ऐसे पहुँच के लिए मंज़ूरी देने के प्राधिकृत का विवरण, जिससे ऐसा पहुँच सही नियंत्रण उपायों के माध्यम से सुरक्षित हो, जिसमें कम से कम समय के लिए कम से कम अधिकार, बहु-कारक प्रमाणीकरण और जियो-

फेंसिंग शामिल हैं;

(16) कारबार की अपेक्षा को पूरा करने के लिए, परिचालन तकनीक प्रणाली के रिमोट प्रचालन के लिए ऐसे ऑपरेशन से जुड़े साइबर जोखिमों के आकलन और उन्हें कम करने के उपायों के आधार पर तय प्रक्रिया:

परंतु ऐसी प्रक्रिया की व्यापार की अपेक्षाओं को पूरा करने या किसी भी ज़रूरी बदलाव पर, जो भी पहले हो, की हर साल एक बार समीक्षा और अद्यतन किया जाएगा;

(17) केंद्रीय सरकार द्वारा जारी लागू नियमों और विनियमों के अनुसार डिजिटल डेटा सुरक्षा और गोपनीयता नीति;

(18) यह सुनिश्चित करने के लिए तय बैकअप नीति कि सभी महत्वपूर्ण प्रणाली का ऑनलाइन या ऑफलाइन बैकअप डेटा या दोनों, जैसा भी लागू हो, अद्यतित हो, किन्तु एक महीने से ज़्यादा पुराना न हो, और डेटा प्रतिधारण नीति में तय अवधि के लिए एक पृथक और सुरक्षित माहौल में रखा जाए:

परंतु बैकअप नीति की हर वित्तीय वर्ष में कम से कम एक बार समीक्षा और अद्यतन किया जाएगा और यह सुनिश्चित किया जाएगा कि बैकअप डेटा की अखंडता और उसकी बहाली का परीक्षण किया जाए जिससे वह व्यापार निरंतरता योजना की अपेक्षाओं को पूरा करे;

(19) तय प्रणाली जिससे संवेदनशील डेटा और उसके बैकअप के स्टोरेज, साथ ही समर्पित संपर्क चैनल या इंटरनेट पर इसके संचरण, को कोडीकृत किया जाए जिससे इसकी गोपनीयता, अखंडता और उपलब्धता सुनिश्चित हो सके:

परंतु यदि व्यापार की अपेक्षाओं के कारण कुछ संवेदनशील डेटा का कोडीकरण संभव नहीं है, तो उसे बिना कोडीकृत किए हुए रूप में एक समर्पित संपर्क चैनल पर अनुमति दी जा सकती है;

(20) सभी कर्मियों के क्षमता विकास के लिए वार्षिक साइबर सुरक्षा प्रशिक्षण कार्यक्रम जिनके पास महत्वपूर्ण प्रणाली और उनसे जुड़े आस्तियों तक अधिकृत साइबर या भौतिक पहुँच या दोनों हैं;

(21) इंटरनेट ट्रैफिक की निगरानी और उसे प्रतिबंधित करने के लिए इंटरनेट पहुँच नीति जिससे केवल परिभाषित और अधिकृत उपयोग सुनिश्चित हो सके;

(22) पुराने साइबर आस्तियों के साथ-साथ उन आस्तियों के लिए चरणबद्ध रीति से हटाने की योजना जो उपयोगी जीवन के अंत के करीब हैं और उनका प्रबंधन, साथ ही उनका सुरक्षित निपटान;

(23) साइबर सुरक्षा के क्षेत्र में अनुसंधान एवं विकास क्रियाकलापों को बढ़ावा देने के लिए उद्योग, अनुसंधान संस्थानों, पणधारकों और शिक्षाविदों के साथ सहयोग की योजना:

परंतु ऐसे सहयोग के लिए दायरा और आस्तियों की पहचान विस्तृत जोखिम मूल्यांकन करने के बाद की जा सकती है और ऐसा सहयोग गैर प्रकटीकरण समझौते पर हस्ताक्षर करने के बाद ही प्रभावी होगा;

(24) महत्वपूर्ण प्रणालियों में सॉफ्टवेयर अद्यतन, जिसमें पैच भी शामिल हैं, को दो श्रेणियों में वर्गीकृत करने के लिए मानदंड परिभाषित करें-

(क) एक सॉफ्टवेयर अद्यतन जो इसके परिनियोजन से पहले पूर्व साइबर सुरक्षा अंकेक्षण की अपेक्षा को पूरा करता है, और

(ख) एक सॉफ्टवेयर अद्यतन जिसके परिनियोजन से पहले पूर्व साइबर सुरक्षा अंकेक्षण की अपेक्षा नहीं होती है, लेकिन अगले साइबर सुरक्षा अंकेक्षण में ऐसे मूल्यांकन की अपेक्षा होती है।

इसके अतिरिक्त, सॉफ्टवेयर अद्यतन की सुझावात्मक सूची, जिसके लिए पूर्व साइबर सुरक्षा अंकेक्षण की अपेक्षा होती है, दूसरी अनुसूची में प्रदान की गई है:

परंतु कंप्यूटर सुरक्षा घटना मोचन दल-विद्युत, प्राधिकरण की मंजूरी से, इस सूची को समय-समय पर संशोधित कर सकता है;

(25) सभी महत्वपूर्ण प्रणालियों में लागू किए गए परिवर्तनों को अभिलिखित करने और यह सुनिश्चित करने के लिए कि ऐसी प्रणालियों और उनसे जुड़ी साइबर आस्तियों पर नियोजित परिवर्तन नियंत्रित हैं, एक परिभाषित परिवर्तन प्रबंधन प्रक्रिया:

परंतु ऐसी प्रक्रिया यह सुनिश्चित करेगी कि सॉफ्टवेयर अद्यतन, जिसमें पैच भी शामिल हैं, जो पूर्व साइबर सुरक्षा अंकेक्षण की अपेक्षा के लिए अर्हित हैं, वापिस लेने के उपबंध के साथ संस्करण नियंत्रित होंगे:

परंतु इसके अलावा परिचालन तकनीक प्रणाली में अद्यतन, जिसमें पैच भी शामिल हैं, मूल उपकरण निर्माता द्वारा डिजिटल रूप से हस्ताक्षरित होंगे और ऐसे अद्यतन को उनके जोखिम मूल्यांकन और अनुकरणीय वातावरण में सफल परीक्षण के बाद, ऑफ़लाइन मोड में परिनियोजित किया जा सकता है। तथापि, यदि किसी पैच के लिए मूल उपकरण निर्माता का डिजिटल हस्ताक्षर उपलब्ध नहीं है, तो ऐसे पैच की वैधता और प्रामाणिकता सत्यापित की जाएगी;

(26) डेटा प्रतिधारण नीति में अनिवार्य रूप से लॉग और फोरेंसिक रिकॉर्ड को एक सुरक्षित और संरक्षित वातावरण में संग्रहीत करने की सुविधा के लिए एक तंत्र;

(27) सूचना प्रौद्योगिकी और परिचालन तकनीक पर्यावरण की सभी प्रसंस्करण प्रणालियों को ऐसे स्रोत के साथ तुल्यकालन करने के लिए, उससे जुड़े साइबर जोखिमों का आकलन करने के बाद, संदर्भ समय स्रोत का चयन करने की एक प्रक्रिया:

परंतु परिचालन तकनीक प्रणाली के लिए चयनित संदर्भ समय स्रोत, या तो स्थलीय या भारत विशिष्ट उपग्रह आधारित और इंटरनेट से स्वतंत्र होगा;

(28) सूचना प्रौद्योगिकी प्रणाली के साथ-साथ परिचालन तकनीक प्रणाली के सुरक्षित ऑपरेशन को सुनिश्चित करने के लिए परिचालन तकनीक प्रणाली को सूचना प्रौद्योगिकी प्रणाली से तार्किक रूप से पृथक करने के लिए प्रक्रिया तय की गई है:

परंतु सूचना प्रौद्योगिकी से परिचालन तकनीक और परिचालन तकनीक से सूचना प्रौद्योगिकी तक पहचाना गया डेटा और जानकारी पृथक संपर्क चैनल और एकदिशीय प्रवाह गेटवे के माध्यम से प्रवाहित होगी;

(29) सीमा पार संस्थाओं द्वारा जोखिम मूल्यांकन और व्यावसायिक अपेक्षाओं के आधार पर, राष्ट्रीय सीमाओं से परे संचारित करने की अनुमति वाले डेटा और जानकारी, जिसमें रीयल टाइम डेटा शामिल है, को पहचानने और वर्गीकृत करने के लिए प्रक्रिया तय की गई है:

परंतु कंप्यूटर सुरक्षा घटना मोचन दल-विद्युत अपेक्षानुसार ऐसी प्रक्रिया, डेटा और संबंधित जानकारी की समीक्षा और मूल्यांकन कर सकता है;

(30) वेब एप्लीकेशन की पहचान करने के लिए तय प्रक्रिया, साथ ही व्यापार प्रचालन और निरंतरता पर उनके असर के आधार पर ऐसे एप्लीकेशन को आवश्यक वेब एप्लीकेशन के तौर पर वर्गीकृत करने का मानदंड;

(31) सर्विस से बाहर या पुरानी साइबर आस्ति और उनमें भंडारित डेटा को सुरक्षित रीति से निपटान करने के लिए तय प्रक्रिया;

(32) संवेदनशील डेटा और संवेदनशील जानकारी को सुरक्षित रीति से निपटान करने के लिए तय प्रक्रिया;

(33) डेटा प्रतिधारण नीति जिसमें पृथक-पृथक दस्तावेज़ और रिकॉर्ड के साथ-साथ डेटा और जानकारी को रखने कि रीति और प्रकार बताया गया है, जिसमें शामिल हैं-

(क) महत्वपूर्ण प्रणाली के डेटा का बैकअप;

(ख) महत्वपूर्ण प्रणाली तक रिमोट पहुँच की हर अनुमति के लिए लॉग, जोखिम आंकलन और उसकी

मंज़ूरी का रिकॉर्ड;

(ग) परिचालन तकनीक प्रणाली को सूचना प्रौद्योगिकी प्रणाली से जोड़ने से जुड़े लॉग और मंज़ूरी;

(घ) साइबर सुरक्षा दस्तावेज़, जिसमें साइबर सुरक्षा परीक्षण के प्रमाणपत्र, फ़ैक्टरी स्वीकृति परीक्षण और साइट स्वीकृति परीक्षण के परिणाम, साइबर सुरक्षा अंकेक्षण रिपोर्ट और केंद्रीय सरकार द्वारा ज़रूरी अन्य दस्तावेज़ शामिल हैं;

(ङ) महत्वपूर्ण प्रणाली में क्रियान्वित किए गए बदलावों का रिकॉर्ड, जिसमें सॉफ़्टवेयर अद्यतन और पैच शामिल हैं:

परंतु डेटा प्रतिधारण नीति की हर वित्त वर्ष में कम से कम एक बार समीक्षा और अद्यतन किया जाएगा और डेटा, जानकारी और दस्तावेज़ को यह सुनिश्चित करने के लिए रखा जाएगा कि-

(क) कम से कम पिछले दो कार्य संबंधी डेटा बैकअप उपलब्ध हों;

(ख) महत्वपूर्ण प्रणाली तक हर रिमोट पहुँच के संबंध में जोखिम आंकलन, मंज़ूरी देने का भौतिक रिकॉर्ड और लॉग कम से कम एक वर्ष के लिए उपलब्ध हों;

(ग) फ़ैक्टरी स्वीकृति परीक्षण और साइट स्वीकृति परीक्षण की रिपोर्ट, जिसमे सायबर सुरक्षा अपेक्षाओं का परीक्षण शामिल हो, साइबर आस्ति के पूरे जीवनकाल के दौरान उपलब्ध हों;

(घ) परिचालन तकनीक वातावरण में रिमोट ऑपरेशन के लिए जोखिम आंकलन का रिकॉर्ड और उसके लिए मिली मंज़ूरी कम से कम एक वर्ष के लिए उपलब्ध हों;

(ङ) पिछले तीन वर्षों की साइबर सुरक्षा अंकेक्षण रिपोर्ट उपलब्ध हों;

(च) पिछले चार वर्षों की प्रमाणीकरण अंकेक्षण रिपोर्ट उपलब्ध हों;

(छ) पिछले तीन वर्षों की स्वयं-अंकेक्षण रिपोर्टें उपलब्ध हों;

(ज) सभी सूचना और संचार प्रौद्योगिकी प्रणालियों के लॉग, परिचालन तकनीक प्रणाली का सूचना प्रौद्योगिकी प्रणाली, के साथ परस्पर संबंध और फोरेंसिक रिकॉर्ड 180 दिनों की अवधि के लिए उपलब्ध हों;

(झ) किसी घटना से जुड़े लॉग, जिसमें ऐसी घटना से एक सौ अस्सी दिन पहले और बाद के लॉग शामिल हैं, ऐसी घटना होने के कम से कम तीन सौ पैंसठ दिनों तक उपलब्ध रहेंगे:

परंतु ऐसी जानकारी, डेटा और दस्तावेज़ों तक पहुंच केवल अधिकृत व्यक्तियों तक ही सीमित हो सकती है, जो पहुँच कंट्रोल क्रियाविधि के अधीन परिभाषित प्रक्रिया पर आधारित होगा:

परंतु यह और कि प्राधिकरण, पृथक-पृथक आदेशों के माध्यम से, किसी अन्य दस्तावेज़ को शामिल कर सकता है और डेटा प्रतिधारण नीति के अधीन दस्तावेज़ों को बनाए रखने के लिए कोई अन्य रीति, माध्यम और अवधि निर्दिष्ट कर सकता है।

अध्याय 7

साइबर संकट प्रबंधन योजना

9. साइबर संकट प्रबंधन योजना में-

(1) सभी घटनाओं का पता लगाने और पहचान करने के लिए विस्तृत मानक संचालन प्रक्रिया, किसी घटना को संकट के रूप में वर्गीकृत करने के मानदंड और सभी संभावित संकट परिदृश्यों की सूची शामिल करें;

(2) सभी संभावित संकटों के लिए पणधारकों की पहचान उनकी भूमिकाओं और उत्तरदायित्वों के साथ

करें तथा ऐसी भूमिकाओं के साथ-साथ उनकी उत्तरदायित्वों का संचार करें;

(3) संकट के दौरान करीबी तालमेल के लिए आंतरिक और बाहरी पणधारकों के साथ बातचीत की रीति और माध्यम शामिल करें;

(4) प्रभाव को कम करने और जल्द से जल्द संकट से उबरने के लिए निवारक उपाय शामिल करें।

10. **संस्थाओं की उत्तरदायित्व-** संस्था -

(1) साइबर संकट के दौरान संबंधित आंतरिक और बाहरी पणधारकों के साथ सभी आवश्यक संचार की उपलब्धता सुनिश्चित करे;

(2) साइबर संकट प्रबंधन योजना की प्रभावशीलता को प्रत्येक वर्ष कम से कम एक बार, उस वर्ष के लिए चयनित परिदृश्यों के लिए अभ्यास और मॉक ड्रिल के माध्यम से परीक्षणकरें, जो इसमें बताए गए सभी पहचाने गए संकट परिदृश्यों में से चुने गए हों:

परंतु किसी भी वर्ष में परिदृश्यों का चयन पहले से परीक्षण और सत्यापित किए गए परिदृश्यों के साथ अधिव्यापित नहीं होगा, जब तक कि सभी सूचीबद्ध परिदृश्यों का परीक्षण और सत्यापित का चक्र पूरा न हो जाए;

(3) हर वास्तविक संकट से निपटने और उससे उबरने की एक विस्तृत रिपोर्ट तैयार करें , साथ ही मिले अनुभव, सीखे गए सबक, मिली प्रतिक्रिया, देखी गई कमियां और उनके लिए सुझाए गए उपायों के बारे में भी बताए:

परंतु सुसंगत जानकारी, जिसमें वास्तविक संकट, उसके प्रबंधन और मुख्य निष्कर्ष के बारे में संक्षिप्त जानकारी शामिल है, को विद्युत क्षेत्र के साइबर सुरक्षा पारिस्थितिकी तंत्र के सामूहिक सुधार के लिए कंप्यूटर सुरक्षा घटना मोचन दल-विद्युत और अन्य पणधारकों के साथ साझा किया जाएगा:

परंतु यह और कि साइबर सुरक्षा की स्थिति को बेहतर बनाने के लिए, साइबर संकट प्रबंधन योजना को अपने और अन्य पणधारकों के महत्वपूर्ण सुझावों को शामिल करके अद्यतन किया जाएगा।

अध्याय 8

वेडर के लिए साइबर सुरक्षा अपेक्षाएँ

11. वेंडर के लिए साइबर सुरक्षा अपेक्षाएँ- वेंडर -

(1) संस्था को दस्तावेजीकृत और टेस्टेड प्रक्रिया के साथ-साथ पुनर्प्राप्ति योजना भी प्रदान करें, जिससे उनके द्वारा सप्लाई किए गए प्रणाली को संभावित साइबर संकट की स्थितियों से बहाल किया जा सके;

(2) यह सुनिश्चित करे कि सभी प्रणाली और उनके घटकों के लिए डिजिटल रूप से साइन किए गए या मान्य और प्रमाणित किए गए सुरक्षा पैच और अद्यतन, अनुबंध की अवधि या ऐसे प्रणाली की उपयोगी लाइफ, जो भी बाद में हो, उस दौरान संस्था को उपलब्ध हों;

(3) उस संस्था को एक विस्तृत दस्तावेज़ प्रदान करे, जिसमें सभी अपेक्षाएं और प्रक्रिया शामिल हों, जिसमें सुरक्षा पैच और थर्ड-पार्टी घटकों पर इंस्टॉल किए जाने वाले अद्यतन भी शामिल हों, जिससे उनके द्वारा सप्लाई किए गए घटकों या सब-प्रणाली को इंटीग्रेट किया जा सके;

(4) संस्था को उनके द्वारा आपूर्ति किए गए सॉफ़्टवेयर, हार्डवेयर, और प्रणाली के समर्थन की समाप्ति या जीवन की समाप्ति का विवरण प्रदान करे, जैसा भी लागू हो, जिसमें तृतीय पक्ष से प्राप्त किए गए उत्पाद भी शामिल हैं;

(5) भारतीय कंप्यूटर आपात मोचन दल द्वारा समय-समय पर जारी दिशानिर्देशों के अनुसार, संस्था को 'सामानों का बिल' उपलब्ध कराए, जिसमें महत्वपूर्ण प्रणाली में प्रयुक्त होने वाले सभी घटक, फर्मवेयर

सहित की विस्तृत सूची शामिल होगी;

(6) यह सुनिश्चित करे कि संस्था को सप्लाई करने से पहले, हार्डवेयर और सॉफ्टवेयर को सभी अंतर्निहित सुरक्षा क्षमताओं, सुरक्षित कॉन्फ़िगरेशन, और नियंत्रण को चालू करके मज़बूत बनाया गया है;

(7) संस्थाओं के लिए उत्पाद और सेवा में कमियों की रिपोर्ट करने के लिए एक औपचारिक संरचित प्रक्रिया बनाए । इसके अतिरिक्त, वेंडर अपनी दोषपूर्ण प्रकटन और प्रबंध कार्यक्रम के माध्यम से ऐसी कमियों की जानकारी कंप्यूटर सुरक्षा घटना मोचन दल-विद्युत को देगा।

12. वेंडर्स का उत्तरदायित्व -प्रोज्यूमर के वितरित उत्पादन संसाधन के मामले में, वेंडर –

(1) यह सुनिश्चित करे कि कोई भी आवेदन, संबंधित निगरानी और नियंत्रण सर्वर और ऐसे प्रणाली का वास्तविक समय का डेटा, जिसमें क्लाउड प्लेटफॉर्म पर होस्ट किया गया कोई भी डेटा या सूचना और साथ ही संबंधित ऐतिहासिक डेटा या सूचना शामिल है, एक एन्क्रिप्टेड, सुरक्षित और संरक्षित वातावरण में संग्रहीत किया जाए और केवल भारत में ही रहे;

(2) यह सुनिश्चित करे कि ग्रिड से जुड़े डिवाइस का रिमोट एक्सेस और रिमोट ऑपरेशन, साथ ही रिमोट एप्लीकेशन, एग्रीगेटर और वितरण लाइसेंसधारी के साथ उनके रियल टाइम डेटा और जानकारी का आदान-प्रदान, आपसी प्रमाणीकरण के बाद, सुरक्षित चैनल के माध्यम से किया जाएगा और ऐसा संचार कोडीकृत होगा;

(3) केंद्रीय सरकार द्वारा समय-समय पर जारी किए गए आदेशों, निर्देशों या दिशानिर्देशों के अनुसार, किसी विश्वसनीय स्रोत के सत्यापन के लिए आवश्यक सूचना उपलब्ध कराए:

परंतु प्रोज्यूमरों के विद्यमान वितरित उत्पादन संसाधन के लिए यह विनियमन उस तिथि को लागू होगा, जिसे प्राधिकरण द्वारा पृथक आदेश के माध्यम से निर्दिष्ट किया जाएगा।

अध्याय 9

साइबर सुरक्षा अंकेक्षण

13. साइबर सुरक्षा अंकेक्षण - संस्था यह सुनिश्चित करेगी कि-

(1) साइबर सुरक्षा ऑडिट, साइबर सुरक्षा अंकेक्षणदिशा-निर्देशों और कंप्यूटर सुरक्षा घटना मोचन दल-विद्युत और केंद्रीय सरकार द्वारा नामित अन्य साइबर सुरक्षा अभिकरणों द्वारा जारी निर्देशों में दिए गए विस्तृत दायरे के अनुसार आयोजित किया जाएगा;

(2) साइबर सुरक्षा अंकेक्षण के दायरे में पिछले साइबर सुरक्षा अंकेक्षणमें पहचाने गए सभी अंकेक्षणनिष्कर्षों के समापन का सत्यापन भी शामिल होगा;

(3) अंकेक्षक अपनी साइबर सुरक्षा अंकेक्षणरिपोर्ट इसके शुरू होने के छह सप्ताह के भीतर प्रस्तुत करेगा, और सभी महत्वपूर्ण और उच्च जोखिम वाली कमियों को एक महीने की अवधि के भीतर और मध्यम और साथ ही कम जोखिम वाली कमियों को अंकेक्षक द्वारा साइबर सुरक्षा अंकेक्षणरिपोर्ट प्रस्तुत करने की तारीख से तीन महीने की अवधि के भीतर संबोधित किया जाएगा:

परंतु गंभीर और उच्च जोखिम वाली कमजोरियों को नियंत्रित करने के लिए उचित प्रतिपूरक नियंत्रण लागू किए जाएंगे, जब तक कि ऐसी कमियों की अंकेक्षणमंजूरी न हो जाए।

14. मुख्य सूचना सुरक्षा अधिकारी का उत्तरदायित्व –

(1) मुख्य सूचना सुरक्षा अधिकारी अंकेक्षणअनुपालन की समीक्षा करेगा और यह सुनिश्चित करेगा कि अंकेक्षक साइबर सुरक्षा अंकेक्षणशुरू होने से छह महीने के भीतर अपनी साइबर सुरक्षा अंकेक्षणसमापन रिपोर्ट प्रस्तुत करे।

(2) मुख्य सूचना सुरक्षा अधिकारी, साइबर सुरक्षा अंकेक्षणकी समापन रिपोर्ट में पाई गई अहम अंकेक्षण जानकारियों, जिनमें महत्वपूर्ण और उच्च जोखिम वाली कमियां शामिल हैं और महत्वपूर्ण प्रणालियों से जुड़े नियमों का पालन न करने के मामलों की जानकारी, संस्था के प्रमुख या बोर्ड को, जैसा भी सन्दर्भ हो, देगा:

परंतु विद्युत मंत्रालय के मुख्य सूचना सुरक्षा अधिकारी किसी भी समय जांच के लिए किसी भी संस्था की अंकेक्षणसमापन रिपोर्ट मांग सकता है और यदि आवश्यक हो, तो लिखित स्पष्टीकरण मांगने के बाद, प्राधिकरण की पूर्व स्वीकृति और ऐसी संस्था को पूर्व सूचना के साथ, अंकेक्षणअनुपालन के सत्यापन के लिए तृतीय पक्ष के अंकेक्षक को नियुक्त कर सकता है, जिसकी लागत संस्था द्वारा वहन की जाएगी:

परंतु यह और कि यदि तृतीय पक्ष अंकेक्षण के परिणाम साइबर सुरक्षा अंकेक्षणसमापन रिपोर्ट की टिप्पणियों से भिन्न हों, तो विद्युत मंत्रालय के मुख्य सूचना सुरक्षा अधिकारी आगे आवश्यक कार्रवाई कर सकता है।

अध्याय 10

प्रकीर्ण

15. स्व-अंकेक्षण- इकाई हर वित्तीय वर्ष में इन नियमों के पालन का आकलन करने के लिए स्व-अंकेक्षण करेगी:

परंतु साइबर सुरक्षा और इन नियमों का अनुपालन सुनिश्चित करने के लिए, इकाई बोर्ड या वरिष्ठ प्रबंधन के किसी सदस्य को, जैसा भी सन्दर्भ हो, इस अनुपालन के लिए उत्तरदायी अभिहित कर सकती है:

परंतु यह और कि संस्था समयबद्ध तरीके से गैर-अनुपालन को ठीक करेगी और यह सुनिश्चित करेगी कि अगले वित्तीय वर्ष में होने वाले स्व-अंकेक्षणसे पहले ऐसे सभी गैर-अनुपालन को ठीक कर लिया जाए:

परंतु यह और भी कि विद्युत मंत्रालय के मुख्य सूचना सुरक्षा अधिकारी, उपलब्ध तथ्यों या किसी व्यक्ति द्वारा दी गई जानकारी के आधार पर, किसी भी संस्था की अनुपालन रिपोर्ट की जांच कर सकते हैं। लिखित स्पष्टीकरण मांगने के बाद, और प्राधिकरण की पूर्व मंजूरी तथा संबंधित संस्था को पूर्व सूचना देने के बाद, वे संस्था के दावे की पुष्टि के लिए किसी तीसरे पक्ष के अंकेक्षक को नियुक्त कर सकते हैं; इस प्रक्रिया की लागत संबंधित संस्था द्वारा वहन की जाएगी।

16. कुछ विनिर्दिष्ट मामलों में, लिखित स्पष्टीकरण मांगने और उसकी जांच करने के बाद, विद्युत मंत्रालय के मुख्य सूचना सुरक्षा अधिकारी, केंद्रीय सरकार को 'सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21)' के संबंधित उपबंधों के अधीन उचित कार्यवाही शुरू करने की सिफारिश कर सकते हैं, या अधिनियम की धारा 142 के अधीन कार्यवाही के लिए उचित आयोग के समक्ष याचिका दायर कर सकते हैं।

17. शिथिल करने की शक्ति- प्राधिकरण एक आदेश के माध्यम से, लिखित रूप में दर्ज किए जाने वाले कारणों के लिए, इन विनियमों के किसी भी उपबंध में अपने स्वयं के प्रस्ताव पर या किसी इच्छुक व्यक्ति द्वारा उसके समक्ष किए गए आवेदन पर शिथिलता प्रदान कर सकता है इनमें से किसी भी विनियम के संचालन से उत्पन्न होने वाली कठिनाई को दूर किया जा सके, जो व्यक्तियों के एक वर्ग पर लागू होती है।

पहली अनुसूची

[विनियम 7 का खंड 3 (झ) देखें]

निम्नलिखित दस्तावेज़ और जानकारी सुरक्षित रखी जाएगी-

1. साइबर सुरक्षा नीति और उसमें दिए गए दस्तावेज़ और प्रक्रिया।
2. साइबर संकट प्रबंधन योजना।

3. डेटा प्रतिधारण नीति और उसमें दिए गए सभी दस्तावेज़ और जानकारी।
4. आईएसओ/आईईसी 27001 प्रमाणपत्र या तकनीकी मानदंड प्रमाणपत्र।
5. साइबर आस्तियों और महत्वपूर्ण प्रणालियों के लिए आस्ति रजिस्टर।
6. साइबर जोखिम आकलन और शमन योजना।
7. घटना मोचन और पुनर्प्राप्ति योजना।
8. साइबर सुरक्षा घटना रिपोर्टिंग रजिस्टर।
9. सामानों का बिल।
10. व्यवसाय निरंतरता योजना।
11. दूरस्थ प्रचालन प्रक्रिया।
12. रिमोट एक्सेस प्रक्रिया।

दूसरी अनुसूची

[विनियम 8 का खंड 24 देखें]

सॉफ़्टवेयर अद्यतन के लिए सुझाए गए मानदंड जिनके लिए पहले साइबर सुरक्षा अंकेक्षणकी अपेक्षा होती है

एप्लिकेशन, वेबसाइट, वेब पोर्टल और संबंधित प्रणालियों में संशोधन और संवर्द्धन सहित सॉफ़्टवेयर अद्यतन के लिए निम्नलिखित मानदंडों में से किसी एक को पूरा करने से पहले अनिवार्य रूप से एक सफल साइबर सुरक्षा अंकेक्षणकी अपेक्षा होगी:-

1. **महत्वपूर्ण प्रणाली प्रभाव**: ऐसे अद्यतन जो मुख्य परिचालन प्रक्रियाओं को प्रभावित करते हैं, जैसे ऊर्जा उत्पादन, संचरण, वितरण या लोड प्रबंधन, जिसमें कमियां महत्वपूर्ण बुनियादी ढांचे की कार्यक्षमता या विश्वसनीयता से समझौता कर सकती हैं।
2. **पहुँच नियंत्रण संशोधन**: ऐसे अद्यतन जो उपयोगकर्ता प्रमाणीकरण, प्राधिकरण तंत्र, या प्रशासनिक विशेषाधिकार को बदलते हैं, जिसमें पहचान प्रबंधन प्रणाली या पहुँच नियंत्रण नीतियां शामिल हैं।
3. **तृतीय पक्ष प्रणाली के साथ एकीकरण:** बाहरी प्रणाली, एप्लिकेशन या तृतीय पक्ष सर्विस के साथ एकीकरण से जुड़े अद्यतन, खासकर वे जो संवेदनशील डेटा का आदान-प्रदान करते हैं या क्रॉस-प्लेटफ़ॉर्म संचार को सक्षम बनाते हैं।
4. **सुरक्षा प्रोटोकॉल में बदलाव:** एन्क्रिप्शन मानक, डेटा ट्रांसमिशन प्रोटोकॉल, या दूसरे सुरक्षा-संबंधी कॉन्फ़िगरेशन में बदलाव लाने वाले अद्यतन, जो संवेदनशील जानकारी की सुरक्षा पर प्रभाव डाल सकते हैं।
5. **नए फीचर्स या इंटरफेस का परिचय:** ऐसे अपडेट्स जो ज़रूरी नए फंक्शन, यूज़र इंटरफेस, या एपीआई जोड़ते हैं, जिनसे संभावित अटैक सरफेस मिल सकते हैं।
6. **सुरक्षा कमियों का समाधान:** पहले से पहचानी गई गंभीर और उच्च प्रभाव वाली कमियों को ठीक करने वाले अद्यतन, जहाँ अधूरा या अनुचित कार्यान्वयन सुरक्षा जोखिमों को और बढ़ा सकता है।
7. **घटना मोचन और निगरानी प्रणाली**: साइबर सुरक्षा निगरानी, घटना मोचन, या लॉग मैनेजमेंट से जुड़े प्रणाली या टूल्स को प्रभावित करने वाले अद्यतन, जिसमें कोई भी रुकावट खतरों का पता लगाने या उन पर असरदार रीति से मोचन करने की क्षमता में रुकावट डाल सकती है।
8. **सुधार या विनियामक अनिवार्य प्रणालियाँ:** विनियमों के अधीन या समुचित सरकार के सुधार

कार्यक्रमों के अनुसार प्रणालियों को प्रभावित करने वाले अद्यतन।

श्रवण कुमार, सचिव

[विज्ञापन-III/4/असा./253/2026-27]

CENTRAL ELECTRICITY AUTHORITY

NOTIFICATION

New Delhi, the 31th July, 2026

F. No. CEA-HY-91-19/8/2024-Cyber Security Division.—Whereas public notices advertising the draft of the Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2025 were published in six newspaper dailies, as required by sub-section (3) of section 177 of the Electricity Act, 2003 (36 of 2003) read with sub-rule (2) of rule 3 of the Electricity (Procedure for Previous Publication) Rules, 2005 for inviting objections and suggestions from all persons likely to be affected thereby, before the expiry of the period of thirty days, from the date on which the copies of the said draft regulations were made available to the public;

And whereas copies of the said newspapers containing the public notices and the said draft regulations on the website of the Central Electricity Authority were made available to the public on 07th October 2025;

And whereas the objections and suggestions received from the public on the said draft regulations were considered by the Central Electricity Authority;

And whereas Ministry of Electronics and Information Technology has accorded its concurrence to make these regulations in respect of the Cyber Security for power sector.

Now, therefore, in exercise of the powers conferred by sub-section (1) of section 177 read with clause (c) of section 73 of the Electricity Act, 2003(36 of 2003), the Central Electricity Authority hereby makes the following regulations relating to Cyber Security in power sector for ensuring safe and secure operation and maintenance of electrical plants and electrical lines, namely**:** –

Chapter I

Preliminary

1. **Short title and commencement -** (1) These regulations may be called the Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2026.

(2) These regulations shall come into force with effect from 1st April 2027:

Provided that the Regulations 5(9), 5(24), 5(33), 5(39), 6(2) and 6(7) shall come into force on such dates, as may be specified by the Authority through separate orders with prior approval of the Central Government.

2. **Scope and extent of applicability -** (1) These Regulations shall apply to -

(a) all the entities which own, operate, or manage Operational Technology infrastructure associated with the interconnected power system and their Information Technology infrastructure that is physically or logically connected to such Operational Technology infrastructure, for their existing as well as upcoming infrastructure:

Provided that in respect of generating companies, captive generating plants, and organisations having Energy Storage System, these regulations shall be applicable only where such entities have an installed capacity of 50 MW or more:

Provided further that the entities having an installed capacity of less than 50 MW are encouraged to implement the minimum baseline cyber security controls outlined in the "15 Elemental Cyber Defense Controls for Micro, Small and Medium Enterprises" issued by Indian Computer Emergency Response Team;

(b) power exchanges and over the counter platforms, except regulations 6, 11, and 12.

(2) The vendor shall comply with the regulations 11 and 12 of these regulations as applicable.

3. **Definitions** - (1) In these regulations, unless the context otherwise requires -

(a) **“Act”** means the Electricity Act, 2003 (36 of 2003);

(b) **“Bill of materials”** means a comprehensive list and structured inventories of components, sub-components, material, libraries, and modules used in product or system to facilitate a comprehensive visibility and transparency into composition of such product or system;

(c) **“Business continuity plan”** means documented procedures that guide an organisation to maintain a defined level of continued business operations;

(d) **“Chief Information Security Officer”** means the designated employee of senior management level of an entity, having knowledge of cyber security and matters related thereto and who is responsible for cyber security efforts and initiatives;

(e) “**Chief Information Security Officer – Ministry of Power**” means Chief Information Security Officer of Ministry of Power;

(f) **“communication system”** means a collection of individual communication networks, communication media, relaying stations, tributary stations, terminal equipment usually capable of inter-connection and inter-operation to form an integrated communication for power sector;

(g) **“Computer Security Incident Response Team – Power”** means an organisation established by the Ministry of Power as an extended arm of Indian Computer Emergency Response Team (CERT-In) for coordinating, reporting, and responding to cyber security incidents in power sector;

(h) **“critical Information Technology system”** means Information Technology system of an organisation whose unavailability or degradation would adversely impact its business operations;

(i) **“critical Operational Technology system”** means Operational Technology system of an organisation whose unavailability or degradation would adversely impact its business operations;

(j) **“critical system”** means critical Operational Technology system or critical Information Technology system or both, including Critical Information Infrastructure, as applicable, of an entity;

(k) **“Critical Information Infrastructure”** means Critical Information Infrastructure as defined in explanation of sub-section (1) of section 70 of the Information Technology Act, 2000 (21 of 2000);

(l) **“cyber asset”** means the programmable electronic device, with or without computing capabilities including its hardware, software, sub-components and data thereof that are connected over a network;

(m) **“cyber asset register”** means a record that contains list of all cyber assets and description thereof;

(n) **“cyber crisis management plan”** means cyber crisis management plan as defined in clause (d) of sub-rule (1) of rule 2 of the Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018;

(o) **“cyber resilience”** means the ability to anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks or compromises on cyber asset;

(p) **“cyber security audit”** means an audit to assess the cyber security posture by a CERT-In empanelled auditor or any other auditor, as may be designated by the Ministry of Power, Government of India through a separate order;

(q) **“Cyber security breach”** means cyber security breach as defined in clause (i) of sub-rule (1) of rule 2 of the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013;

(r) **“Cyber security incident”** means cyber security incident as defined in clause(h) of sub-rule (1) of rule 2 of the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013;

(s) **“Cyber security policy”** means procedure and processes for protecting information, computer resources, networks, devices, industrial control systems and Operational Technology resources and to improve the cyber security posture thereof;

(t) **“Cyber sabotage”** means deliberate action to disrupt, damage or destroy the information systems, networks or data processed therein for malicious purpose;

(u) **“Distributed Generation Resource”** means a generating station feeding electricity into the electricity system at voltage level of below 33 kV and includes grid-connected rooftop solar systems and Energy Storage System;

(v) **"Electronic Security Perimeter"** means the logical border surrounding Information Technology system or Operational Technology system or both that are electronically connected within which the access is monitored and controlled for protection of such system;

(w) **"entity"** includes generating companies, Captive generating plants, organisations having Energy Storage System; transmission licensees; distribution licensees; National Load Dispatch Centre; Regional Load Dispatch Centres; State Load Dispatch Centres; Power Exchanges and Over the Counter Platforms;

(x) **"Factory Acceptance Test"** means structured and documented testing process carried out by the vendor in the presence of the representative of the entity to verify functional, performance, contractual and safety requirements of system or equipment or major component thereof before dispatch;

(y) **"Information Technology system"** means the Information Technology system consisting of user endpoints, network resources, applications, servers, and communication components deployed therein;

(z) **"obsolete asset"** means an asset declared by original equipment manufacturer or original equipment supplier whose production and services have discontinued, and its support is no longer available, and that asset is not suitable for its intended purpose due to technological advancement, operational changes and may pose security or operational risk;

(aa) **"Operational Technology"** means programmable hardware or system that detects or causes changes through the direct monitoring or control of physical devices, processes, and events;

(bb) **"prosumer"** means a person who consumes electricity from the grid and can also inject electricity into the grid for distribution licensee, using same point of supply;

(cc) **"protected system"** means protected system as defined in clause (k) of sub-rule (1) of rules 2 of the Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018;

(dd) **"remote access"** means an access to any cyber asset of an organisation through an external network;

(ee) **"remote operation"** means day-to-day operation and control of Information Technology or Operational Technology system of an entity performed from a distant location from such system;

(ff) **"self-audit"** means an audit by an entity in a financial year to assess its compliance with all applicable regulations specified in these regulations;

(gg) **"sensitive information"** means data or information that, if disclosed, modified, or destroyed, could negatively impact the privacy, integrity, security or operations of an organisation or an individual;

(hh) **"Site Acceptance Test"** means structured and documented testing conducted to verify functional, performance, contractual and safety requirements, at the site of installation and ensure that a system or equipment and its major components operate as intended in its final operational environment, before its commissioning;

(ii) **"Sub-Sectoral Computer Security Incident Response Team"** means an entity designated by the Authority to assist Computer Security Incident Response Team - Power in cyber security related matters;

(jj) **"Technical Criteria Certificate"** means a certificate issued to an organisation by a designated certification body accredited for ensuring conformance to cyber security standards specified by the Central Government;

(kk) **"threat"** means any circumstance or event having the potential to exploit a deficiency and negatively impact the confidentiality, integrity or availability of a cyber asset or Information Technology system or Operational Technology system;

(ll) **"trusted source"** means a mechanism designed to mitigate specific security requirements particularly cyber security supply chain risks by ensuring that equipment, services, manufacturer and service providers, associated with power sector meet an established criteria;

(mm) **"Vulnerability"** means vulnerability as defined in clause (p) of sub-rule (1) of rule 2 of the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013;

(nn) **"vendor"** means original equipment manufacturer, original equipment supplier, system integrator, supplier of hardware or software associated with original equipment, contractor or service provider including cloud service provider; and manufacturer and supplier of hardware, firmware, or software

associated with the original equipment or control systems, including but not limited to inverters, communication modules, monitoring systems, and related control or energy management software, of a Distributed Generation Resource owned by a prosumer.

(2) Words and expressions used but not defined in these regulations shall have their respective meanings assigned to them in the Act, Rules and other regulations made thereunder.

CHAPTER II

COMPUTER SECURITY INCIDENT RESPONSE TEAM - POWER

4. (1) **The Computer Security Incident Response Team – Power shall** -

(a) be the coordinating agency for reporting and responding to cyber security incidents associated with power sector;

(b) be the nodal agency of power sector for analysis, prediction and prevention of cyber security incidents and dissemination of information thereof;

(c) collect data and information pertaining to any cyber security incident from an entity including network architecture, details of assets, logs, cyber forensic records, forensic image, policies and procedures or any other relevant information, in the form, manner and mode as specified by it:

Provided that sensitive data as well as sensitive information collected shall be protected against breaches and shall only be used for cyber security purpose by designated government agencies but not be disclosed to any third party without explicit communication to the concerned entity.

(2) **The roles and responsibilities of Computer Security Incident Response Team - Power in** Power **Sector include the following, namely** -

(a) collect and analyze cyber incidents, vulnerabilities and threats related to power sector;

(b) predict cyber security incidents, threats and vulnerabilities related to power sector;

(c) coordinate and collaborate with Indian Computer Emergency Response Team, National Critical Information Infrastructure Protection Centre and other agencies designated by the Central Government in the area of cyber security, to resolve the cyber security incidents related to power sector;

(d) issue alerts, advisories, and guidelines as well as threat intelligence in coordination with Indian Computer Emergency Response Team, National Critical Information Infrastructure Protection Centre and any other agencies designated by the Central Government in the area of cyber security;

(e) create or develop Standard Operating Procedures, security policies, sub-sector specific benchmarks, security controls, and best practices for incident response activities in consultation with Indian Computer Emergency Response Team, National Critical Information Infrastructure Protection Centre, sub-sectoral Computer Security Incident Response Teams, Electricity Regulatory Commissions, entities, and other agencies designated by the Central Government in the area of cyber security;

(f) undertake proactive measures to increase the cyber security awareness through capacity building initiatives and interventions;

(g) ensure the improvement of cyber security posture of the power sector through cyber security assessments, cyber security audits, certification audits, self-audits, third party audits and exercises including mock-drills and simulations;

(h) coordinate for laying down the sub-sector specific cyber security framework, protocols, and rules;

(i) advise the entities in preparation of their Cyber Crisis Management Plan;

(j) coordinate with entity for ensuring the implementation of their Cyber Crisis Management Plan during actual cyber crisis;

(k) facilitate and promote Research and Development in the domain of cyber security through collaboration with Industry, Research Institutes and Academia;

(l) formulate and implement of measures to ensure cyber security of supply chain of cyber assets specified by the Central Government or the Authority;

(m) establish central cyber security coordination forum and regional cyber security coordination forums of power sector to support Computer Security Incident Response Team - Power, in accordance with a separate order issued by the Authority, for periodic review of cyber security posture, deliberate upon cyber security challenges, information sharing, coordinated response planning and improve the overall posture of sector;

(n) Any other functions associated with cyber security related matters in the power sector, as directed by the Central Government or the Authority.

(3) The directions and guidelines of Computer Security Incident Response Team - Power, in the matters related to cyber security of power sector, shall be complied with by entities and vendors, as applicable.

(4) The Authority through a separate order may designate sub-sectoral Computer Security Incident Response Teams in power sector for generation, transmission, distribution, grid operation, and any other sub-sector, along with their roles and responsibilities to assist Computer Security Incident Response Team - Power.

CHAPTER III

General Cyber Security requirements

5. **The entity shall -**

(1) designate regular employees of senior management level as Chief Information Security Officer and alternate Chief Information Security Officer;

(2) ensure that the positions of Chief Information Security Officer and alternate Chief Information Security Officer shall not remain vacant at the same time;

(3) define roles and responsibilities of Chief Information Security Officer and alternate Chief Information Security Officer in accordance with the Central Government's regulatory framework and relevant guidelines;

(4) ensure that the Chief Information Security Officer reports to the head of the entity:

Provided that in case any entity such as the State Load Dispatch Centre is not an independent entity but part of a holding company or parent company, such entity shall have a separate Chief Information Security Officer, who shall report to head of such holding company or parent company, as applicable and shall also have Alternate Chief Information Security Officer;

(5) ensure an employee is designated as Chief Information Security Officer, for a minimum period of three years;

(6) ensure that role of the Chief Information Security Officer is ring fenced to the tasks of cyber security related matters only;

(7) provide contact details of the Chief Information Security Officer and alternate Chief Information Security Officer and updation thereof in public domain and communicate such details to Computer Security Incident Response Team - Power as well as all internal and external stakeholders;

(8) ensure that Chief Information Security Officer attends cyber security training courses for at least five man-days in each financial year;

(9) establish a dedicated Information Security Division headed by Chief Information Security Officer, within India, for dealing with all cyber security related matters and the same shall remain operational round the clock. Further-

(a) the Information Security Division shall be deployed with sufficient staffing;

(b) the staff deployed in Information Security Division shall have valid certificate of successful completion of domain specific cyber security course;

(c) the staff deployed in Information Security Division shall attend cyber security training courses associated with power sector for at least five man-days in each financial year;

(d) the staff shall be deployed in Information Security Division for a minimum tenure of three years;

(10) have a defined and documented Cyber Security Policy, which is approved and reviewed annually by the head or board of the entity, as the case may be;

(11) prepare a Cyber Crisis Management Plan in consultation with Computer Security Incident Response Team - Power, to manage and recover from all possible cyber crisis situations in shortest possible time with minimum impact on business operations:

Provided that the Cyber Crisis Management Plan shall be vetted by Indian Computer Emergency Response Team, approved and reviewed annually by the head or board of the entity, as the case may be;

(12) ensure separation of Information Technology networks containing Critical Information Infrastructure from Internet as well as rest of the Information Technology networks:

Provided that in case internet is required for Information Technology networks containing Critical Information Infrastructure, the same shall be sourced securely with suitable hardening measures as specified by designated agencies of the Central Government;

(13) ensure deployment of all required security devices including firewalls at Electronic Security Perimeter, such that the deployed security system meets the requirements of, inter-alia, packet filtering; deep packet inspection; content, user and application based filtering; detection and inspection of encrypted traffic; intrusion detection and prevention; geo-fencing; facility for automatic signature and behaviour updates; user controlled updates; detection, inspection and filtering based on signature and behavioural anomalies;

(14) ensure that any web service or web-based application including website, web portal, and Application Programming Interfaces, having public access, shall be deployed only after cyber security audit clearance:

Provided that any software update, including patch, in web applications and web services shall be deployed only after successful testing and confirmation, such that the subject update is free from any cyber security vulnerability, and after ensuring that such update is free from any cyber risk:

Provided further that any software update qualified for prior requirement of cyber security audit, as specified in Cyber Security Policy, shall be deployed only after its cyber security audit clearance:

Provided also that all software updates, those not necessitated for prior cyber security audit, shall be assessed during next cyber security audit;

(15) ensure deployment of all required security devices for all critical web applications, identified as per the procedure detailed under Cyber Security Policy, such that the deployed security system meets the requirements of, inter alia, application layer filtering including detection and filtering of web based encrypted traffic; ensuring bidirectional protection; facility for automatic signature and behavioural updates; intrusion detection and prevention, user controlled update mechanism; content, user and application based filtering; geo-fencing; detection, inspection and filtering of encrypted traffic based on signature and behavioural anomalies;

(16) identify and segregate systems as critical and non – critical systems, as per the procedure detailed in Cyber Security Policy;

(17) ensure that remote access to cyber assets, if necessary, may be permitted only for troubleshooting and emergency requirements, as per the procedure specified under Cyber Security Policy:

Provided that such access for the cyber assets associated with non – critical system may be permitted with approval of Chief Information Security Officer for troubleshooting and emergency requirements only along with suitable security control measures:

Provided further that approval for such access to critical systems or cyber assets thereof may be granted after a comprehensive risk assessment is conducted along with identification of effective measures thereof and such access shall be continuously monitored to detect any anomaly or attempts of unauthorised use:

Provided also that record of risk assessment, physical document of approval and logs with respect to each such access to critical system shall be maintained for a period as specified in data retention policy;

(18) conduct cyber security awareness program and cyber security exercises including mock-drills and tabletop exercises, at least once in every six months;

(19) ensure that sensitive information and sensitive data including such data and information hosted on cloud as well as such historical data and information, is stored in an encrypted, secured, and protected environment and resides within India only;

(20) include all cyber security requirements as well as applicable cyber security rules, regulations issued by the Central Government and Non - Disclosure Agreement in Service Level Agreement with the vendors, as specified under Cyber Security Policy, to ensure the confidentiality, integrity and availability of sensitive information during their contract period as well as after completion of such contract period:

Provided that vendor having cyber or physical access or both to the critical systems including staff of vendor engaged for operation or maintenance or both of such systems, may be permitted after carrying out personnel risk assessment and mitigative measures taken thereof along with an undertaking complying with Service Level Agreement:

Provided further that in case of any cyber security breach, the entity shall enquire into the matter and initiate action against such vendors including cloud service provider committing cyber security breach;

(21) ensure online and offline backups of all critical systems in a separate, safe and secure environment as specified in cyber security policy;

(22) facilitate a comprehensive cyber security audit encompassing all critical systems, as specified under regulation 13, at least once in every financial year but with a minimum and maximum gap of nine months and fifteen months, respectively, between two consecutive cyber security audits:

Provided that the cyber security auditing agency engaged by entity shall deploy its qualified personnel but exclusive of any staff deployed for such entity, if any:

Provided further that no three consecutive audits shall be carried out by the same auditing agency or personnel;

(23) ensure that all Information Technology products procured comply with and tested in adherence with the orders issued by the Central Government;

(24) ensure compliance with and acquire ISO / IEC 27001 certificate or Technical Criteria Certificate encompassing all critical systems:

Provided that no four consecutive audits for the certification of ISO 27001 or Technical Criteria Certificate shall be carried out by the same auditing agency or personnel;

(25) maintain asset register-

(a) for all cyber assets along with the requisite details including ownership, hardware, firmware, software, and patch as per the procedure defined in Cyber Security Policy;

(b) recording the details of all critical systems along with the requisite details including its configuration, hardware, software, network architecture depicting data flows and communication protocols used therein:

Provided that such register shall be reviewed and updated at least once in every financial year or upon commissioning of any new cyber asset or critical system including replacements thereof, whichever is earlier;

(26) maintain Cyber Risk Assessment and Mitigation Plan for all assets detailed in cyber asset register, as per the procedure defined in Cyber Security Policy:

Provided that Cyber Risk Assessment and Mitigation Plan shall be updated at least once in every six months and reviewed at least once in every financial year and such Cyber Risk Assessment and Mitigation Plan shall be implemented to manage the vulnerabilities, threats and risks associated thereof;

(27) ensure that the cyber security audit including vulnerability assessment and penetration testing is carried out prior to the commissioning of any new critical system including replacement of such system and manage vulnerabilities and risks for critical system as per the mechanism defined in Cyber Security Policy;

(28) furnish relevant information including system details and functionality, of all new critical systems commissioned including those replaced, as per asset register associated with critical systems to the Computer Security Incident Response Team - Power within thirty days of such commissioning or replacement;

(29) provide the relevant information to National Critical Information Infrastructure Protection Centre for identification of Critical Information Infrastructure. Further, within sixty days of an asset being identified as a Critical Information Infrastructure by National Critical Information Infrastructure Protection Centre, entity shall approach the Appropriate Government for notifying such asset as a Protected System;

(30) ensure that Critical Information Infrastructure and Protected System are not discoverable on public platforms unless approved by the head or board of the entity, as applicable, on the basis of business requirements, criticality, and risk assessment of such system;

(31) ensure that the procurement process mandates inclusion of Factory Acceptance Test and Site Acceptance Test including testing of cyber security requirements;

(32) ensure that the clocks of all relevant information processing systems within Information Technology and Operational Technology systems, as applicable, are synchronised to a reference time source as provided in the Cyber Security Policy:

Provided that prior to selection of such reference time source detailed cyber risk assessment shall be carried out;

(33) ensure that all personnel including personnel engaged by vendors in day-to-day operation and

maintenance of all critical systems, have mandatorily undergone designated cyber security courses pertaining to power sector;

(34) ensure that the systems, networks, and applications associated with physical security of critical systems are physically separated from the network of such critical systems:

Provided that in case of such physical separation is not feasible, with approval of head of the entity, subject systems, networks, and applications shall be logically separated from the networks of such critical systems;

(35) maintain Incident Response and Recovery Plan, as specified in Cyber Security Policy, to recover from cyber incidents and resume normal operations at the earliest:

Provided that such plan shall be reviewed and updated at least once in every six months;

(36) have surveillance and continuous monitoring of Information Technology systems and Operational Technology systems, as applicable, for identification of threats as well as vulnerabilities and provide incident response and remediation support thereof;

(37) ensure that logs of all security devices deployed at Electronic Security Perimeter are enabled to record exchange of data and information flowing through such devices;

(38) ensure regular, at least once in every year, review and updation of rules and policies of perimeter security devices;

(39) ensure that the Information Technology equipment and services are procured from trusted sources, in accordance with orders, directions or guidelines issued by the Central Government from time to time;

(40) comply with the directions and requirements issued under the Information Technology Act, 2000 (21 of 2000) and with all rules and regulations made thereunder, in addition to these regulations;

(41) have structured vulnerability disclosure and management programs with vendors and Computer Security Incident Response Team – Power;

(42) maintain a register to record all cyber security incidents along with relevant details, as per the format prescribed by Computer Security Incident Response Team - Power.

CHAPTER IV

Additional Cyber Security requirements of Entities related to Operational Technology Systems.

6. **In addition to requirements mandated for entities under the regulation 5, the entity shall** – (1) ensure physical isolation of Operational Technology system from internet as well as Information Technology system:

Provided that in case such isolation from Information Technology system is not possible due to business requirements, such Information Technology and Operational Technology interconnection may be permitted, as per the procedure defined in Cyber Security Policy, with suitable hardened logical separation between Operational Technology system and Information Technology system, on the basis of risk assessment of such interconnection and approval of head or board of the entity, as applicable:

Provided further that such inter-connection is continuously monitored for detection of malicious activities and corrective measures thereof:

Provided also that such approval and logs associated with such inter-connection shall be retained for a period as specified in data retention policy;

(2) ensure deployment of suitable perimeter level cyber security devices including firewall at point of inter-connection of Operational Technology system with communication system of power system such that the deployed security system meets the requirements of, amongst other requirements, the detection and filtering of Operational Technology related protocols as well as traffic; content, user and application based filtering; deep packet inspection, intrusion detection; geo-fencing; user controlled updates; detection based on signature and behavioural anomalies and filtering thereof:

Provided that the updates including signatures for devices forming part of such security system shall be carried out in offline mode, as specified in Cyber Security Policy;

(3) ensure that control and operation of power system elements and exchange of information thereof including real time data shall be over a dedicated communication channel isolated from the internet through perimeter level cyber security devices and shall be confined to national boundaries only:

Provided that for entities having business requirements or cross border power system elements, the exchange of information and real time data, as identified under Cyber Security Policy, may be permitted beyond the national boundaries only through dedicated separate communication system and unidirectional gateway, isolated from internet and along with cyber security devices, to transmit and receive subject to the condition that such information and data are monitored continuously to detect any anomaly or unauthorised attempt:

Provided further that in case of exchange of real time information and data associated with end consumers, the same may be permitted through secured connection, isolated from public access, subject to the condition that exchange of sensitive information and data thereof over such connection shall be encrypted to ensure its confidentiality, integrity, and privacy;

(4) ensure that if remote operation is necessary for business requirements, the same shall be, within India, with the prior approval of head or board of the entity, as applicable, as per the procedure specified in the Cyber Security Policy, through a dedicated communication channel, isolated from internet, having cyber security system mandated under the regulation 6(3);

(5) ensure that all Operational Technology equipment, components, and parts thereof deployed for control and operation of power system shall comply with orders issued by the Central Government;

(6) ensure that the communication system of Operational Technology system is isolated from that of Information Technology system;

(7) ensure that the Operational Technology equipment and services are procured from trusted sources, in accordance with orders, directions, or guidelines issued by the Central Government from time to time;

(8) ensure that the Operational Technology environment is segmented into different trust levels on the basis of criticality, security requirements, and risk assessment;

(9) ensure that the communication system particularly channel, catering the Operational Technology data and information between the two entities is protected by owner of such system against cyber security threats.

CHAPTER V

Functions of Chief Information Security Officer and Information Security Division

7. (1) The Chief Information Security Officer and Alternate Chief Information Security Officer shall be citizens as well as residents of India and shall possess a degree in engineering or equivalent from a recognised institute, with at least fifteen years of experience in domain of power sector or Information Technology:

Notwithstanding anything contained in these regulations, the Authority may specify additional qualifications for Chief Information Security Officer of entity, through separate orders:

Provided that in absence of Chief Information Security Officer the roles and responsibilities of the Chief Information Security Officer shall be performed and executed by Alternate Chief Information Security Officer.

(2) The Chief Information Security Officer shall -

(a) be the nodal officer for all cyber security related matters;

(b) coordinate with all concerned stakeholders associated with the cyber security related matters.

(3) The functions of the Chief Information Security Officer, with the assistance of the Information Security Division shall include the following, namely -

(a) reporting of cyber security incidents within six hours to Computer Security Incident Response Team - Power and Indian Computer Emergency Response Team:

Provided that in case any incident is concluded as a cyber sabotage in critical systems, the same shall be reported within twenty-four hours;

(b) quarterly review of compliances as mandated in Cyber Security Policy;

(c) implementation of cyber security control measures for critical systems, as specified in Cyber Security Policy, to firm up their cyber resilience;

(d) in case of Critical Information Infrastructure or Protected System, implementation of validated cyber security control measure as per guidelines of National Critical Information Infrastructure Protection Centre;

(e) acting upon the cyber security related directives, guidelines and advisories issued by the Central

Government, the Authority, Indian Computer Emergency Response Team as well as Computer Security Incident Response Team - Power;

(f) gathering of cyber threat intelligence, its analysis, identification of threat vectors, assessment of cyber security risks and mitigation measures thereof;

(g) sharing of the detailed report of detected cyber security incidents, Action Taken Reports, Root Cause Analysis, and other relevant information with Computer Security Incident Response Team - Power and Indian Computer Emergency Response Team;

(h) retention of all cyber security related data, information and documents in the manner, form and period as specified in data retention policy;

(i) custody of all documents specified in First Schedule of these regulations;

(j) ensuring the updation of firmware and software of all critical systems, with patches as provided in Cyber Security Policy;

(k) ensuring the storage of logs of all Information and Communication Technology systems and logs as well as forensic records pertaining to cyber security incidents for the period, as specified in Cyber Security Policy;

(l) providing required information including allocated, used and unused public IPs to Computer Security Incident Response Team - Power;

(m) ensuring random testing of day-to-day operations of critical systems for being in conformance with its Cyber Security Policy and corrective measures thereof;

(n) prepare a procedure to facilitate remote access to cyber assets associated with non-critical system, for troubleshooting and emergency requirements including suitable security controls required and process to grant approval for such access;

(o) prepare a procedure, as specified in Cyber Security Policy, to facilitate safe and secure remote operation of Operational Technology system and updation thereof;

(p) ensure the development, implementation, review and updation of Cyber Security Policy, Cyber Crisis Management Plan, data retention policy, and backup policy;

(q) ensure the preparation, updation and review of asset register for cyber assets and critical systems as well as Cyber Risk Assessment and Mitigation Plan;

(r) ensure synchronisation of all Information Technology systems and Operational Technology systems to the reference time source, as specified under Cyber Security Policy.

CHAPTER VI

Cyber Security Policy

8. The Cyber Security Policy shall be aligned with the Business Continuity Plan of entity covering Operational Technology as well as Information Technology environment, as applicable, and the same may include -

(1) defined purpose and scope along with all applicable cyber security requirements and compliances thereof;

(2) for Protected Systems, provisions ensuring alignment with National Critical Information Infrastructure Protection Centre guidelines and control requirements;

(3) defined roles and responsibilities of relevant internal and external stakeholders;

(4) defined procedure to prepare cyber asset register, consisting of all cyber assets and classification thereof on the basis of their criticality and risk identified in Cyber Risk Assessment and Mitigation Plan; and update such procedure for detailed visibility and management of all cyber assets;

(5) defined procedure to identify all systems and classify such systems as critical systems, on the basis of a defined criteria considering their impact on the Business Continuity Plan, as well as record details of such systems in a register:

Provided that such procedure shall be reviewed and updated at least once in every financial year;

(6) defined procedure for Cyber Risk Assessment and Mitigation Plan to identify vulnerabilities and threats against each cyber asset and risk associated thereof, control and mitigation measures in commensuration with criticality of such risks and implementation thereof:

Provided that such procedure shall be reviewed and updated at least once in every financial year;

(7) defined mechanism to manage the vulnerabilities and risks in critical systems by timely identifying deficiencies and threats in such systems, including receipt of associated information from internal and external sources, analysis of such information, risk assessment, and management thereof:

Provided that such mechanism shall be reviewed and updated at least once in every financial year or upon commissioning of any new critical system, including replacement thereof, whichever is earlier;

(8) procedure to identify and report cyber sabotages in critical systems including receipt of such information from internal as well as external stakeholders;

(9) defined Incident Response and Recovery Plan detailing list of all type of incidents, risk analysis, and risk-based incident specific response plan for effective and timely restoration of affected system:

Provided that an incident which necessitates entity level strategic recovery plan shall be classified as a crisis;

(10) mechanism for random testing of day-to-day operations of critical system, for being in conformance with applicable policies, rules and regulations issued by Computer Security Incident Response Team - Power and other agencies designated by the Central Government in the area of cyber security:

Provided that such testing shall not interrupt the operations and functionality of such systems and safety thereof;

(11) access control mechanism to critical systems and cyber assets associated thereof, applications having public access, sensitive information and sensitive data, shall be governed by Access Management based on the principles of Authentication, Authorisation and Accounting criteria and criticality thereof:

Provided that a detailed procedure may be laid down to restrict the physical and logical access to documents and records specified under data retention policy;

(12) personnel risk assessment process to identify risks associated with personnel deployed by vendor, having authorised cyber or physical access to critical system and assets associated thereof or engaged for Operation or Maintenance or both of such system, on the basis of their roles and responsibilities including change in such roles and responsibilities and mitigating measures thereof:

Provided that for the employees engaged in day-to-day Operation and Maintenance or having authorised cyber or physical access to critical system and assets associated thereof, personnel risk assessment shall be carried out, on the basis of their roles executed and duration of deployment in such entrusted tasks, after their termination, resignation, and superannuation from their employment;

(13) mechanism to ensure that all access points to critical systems are secured physically and monitored continuously and also such access is restricted for physical protection of these systems and cyber assets associated thereof:

Provided that in case of a perceptible threat of physical damage to any of these systems or assets thereof, the physical access granted to any individual for such system or asset may be revoked;

(14) cyber supply chain risk management process to identify and assess cyber security risks associated with supply chain of critical systems and services thereof along with mitigative measures;

(15) defined procedure for remote access to cyber assets along with the details of authorisation to grant approval for such access on the basis of their criticality, such that such access is safe and secured through suitable control measures including minimum duration with least privileges, multi-factor authentication, and geo-fencing;

(16) defined procedure for remote operation of Operational Technology systems to meet the business requirement, on the basis of assessment of cyber risks associated with such operation and mitigation measures thereof:

Provided that such procedure shall be reviewed and updated once in every year or upon any change necessitated to meet business requirements, whichever is earlier;

(17) digital data protection and privacy policy in line with applicable rules and regulations issued by the Central Government;

(18) defined backup policy to ensure that online or offline backup data or both, as applicable, of all critical systems is up to date, but not older than a month, and retained in a separate and safe environment for the period as specified in the data retention policy:

Provided that the backup policy shall be reviewed and updated at least once in every financial year and ensure that the integrity of backup data and its restoration is tested such that the same meets the requirements of Business Continuity Plan;

(19) defined mechanism to ensure storage of sensitive data and its backup, as well as its transmission over dedicated communication channel or internet, is encrypted to ensure its confidentiality, integrity, and availability:

Provided that in case encryption of certain sensitive data is not feasible due to business requirements, the same, in unencrypted form, may be permitted over a dedicated communication channel;

(20) annual cyber security training program for capacity development of all personnel having authorised cyber or physical access or both to critical system and assets associated thereof;

(21) Internet access policy to monitor and restrict the internet traffic to ensure defined and authorised use only;

(22) phase out plan for obsolete cyber assets as well as those assets nearing end of useful life and management thereof along with their safe and secure disposal;

(23) plan for collaboration with industry, research institutes, stakeholders and academia to promote Research and Development activities in the domain of cyber security:

Provided that scope and assets for such collaboration may be identified after carrying out detailed risk assessment and such collaboration shall be effected after signing of Non-Disclosure Agreement;

(24) define criteria to classify the software updates including patches in critical systems into two categories-

(a) a software update that qualifies for requirement of prior cyber security audit before its deployment, and

(b) a software update that does not require prior cyber security audit before its deployment but necessitates such assessment in next cyber security audit.

Further, the suggestive list of software updates, which requires prior cyber security audit, is specified at the Second Schedule:

Provided that Computer Security Incident Response Team - Power, with the approval of Authority, may revise this list from time to time;

(25) defined change management process to record changes implemented in all critical systems and to ensure that planned changes on such systems and cyber assets associated thereof are controlled:

Provided that such process shall ensure that software updates including patches qualified for prior requirement of cyber security audit shall be version controlled along with provision of roll-back:

Provided further that the updates including patches in Operational Technology system shall be digitally signed by original equipment manufacturer and such updates may be deployed in offline mode, after their risk assessment and successful testing in simulated environment. However, in case the digital signature of original equipment manufacturer is not available for any patch, the validity and authenticity of such patch shall be verified;

(26) a mechanism to facilitate storage of logs and forensic records as mandated in data retention policy in a safe and secured environment;

(27) a procedure to select reference time source, after assessing its associated cyber risks for synchronizing all processing systems of Information Technology and Operational Technology environment to such source:

Provided that the reference time source selected for Operational Technology system shall be, either terrestrial or India specific satellite based and independent of internet;

(28) defined procedure for logical separation of Operational Technology system from Information Technology system to ensure safe and secure operation of both Information Technology systems as well as Operational Technology systems:

Provided that the identified data and information from Information Technology to Operational Technology and that from Operational Technology to Information Technology shall flow through separate communication channel and unidirectional gateway;

(29) defined procedure by cross border entities to identify and classify the data as well as information including real time data permitted to be communicated beyond national boundaries, on the basis of risk assessment and business requirements:

Provided that Computer Security Incident Response Team - Power may review and assess such procedure, data and relevant information, as and when required;

(30) defined procedure to identify web applications along with a criterion to classify such applications as critical web applications, on the basis of their impact on business operations and continuity;

(31) defined procedure for safe and secure disposal of out of service or obsolete cyber asset and data stored therein;

(32) defined procedure for safe and secure disposal of sensitive data and sensitive information;

(33) data retention policy specifying the manner and form of retention of various documents and records as well as data and information including -

(a) backup of data of critical systems;

(b) record of logs, risk assessment, and approval thereof for each grant of remote access to critical systems;

(c) logs and grant of approval associated with interconnection of Operational Technology system with Information Technology system;

(d) cyber security documents including certificates of cyber security tests, Factory Acceptance Test and Site Acceptance Test results, cyber security audit reports and other documents as mandated by the Central Government;

(e) record of changes including software updates and patches implemented in critical systems:

Provided that the data retention policy shall be reviewed and updated at least once in every financial year and the data, information and documents shall be retained to ensure -

(a) at least last two working data backups are available;

(b) risk assessment, physical record of grant of approval and logs with respect to each remote access to critical system are available for at least one year;

(c) reports of Factory Acceptance Test and Site Acceptance Test including test of cyber security requirements are available throughout life of cyber asset;

(d) record of risk assessment for remote operation in Operational Technology environment along with approval received thereof are available for at least one year;

(e) cyber security audit reports of last three years are available;

(f) certification audit reports of last four years are available;

(g) self-audit reports of last three years are available;

(h) logs of all Information and Communication Technology systems, inter-connection of Operational Technology system with Information Technology system and forensic records are available for a period of one hundred and eighty days;

(i) the logs associated with an incident including logs pertaining to one hundred and eighty days prior and post to such incident are available for at least three hundred and sixty-five days from occurrence of such incident:

Provided further that the access to such information, data and documents may be restricted to authorised persons only, on the basis of procedure defined under access control mechanism:

Provided also that the Authority may, through separate orders include any other document and specify any other manner, mode, and period for retention of documents under data retention policy.

CHAPTER VII

Cyber Crisis Management Plan

9. **The cyber crisis management plan shall** – (1) include detailed Standard Operating Procedure to detect and identify all incidents, criteria to classify an incident as a crisis and list of all possible crisis scenarios;

(2) identify stakeholders along with their roles and responsibilities for all possible crises and communication of such roles as well as responsibilities thereof;

(3) include the manner and mode of communication with internal as well as external stakeholders for close coordination during the crisis;

(4) include mitigative measures to minimize the impact and recover from crisis at the earliest.

10. **Responsibilities of the entities** – The entity shall -

(1) ensure availability of all essential communications with relevant internal and external stakeholders during cyber crisis;

(2) test the efficacy of Cyber Crisis Management Plan at least once in every year through exercises and mock drills for scenarios selected for that year out of all identified crisis scenarios specified under it:

Provided that the selection of scenarios in any year shall not overlap with the scenarios tested and verified earlier unless the cycle of all listed scenarios has been completed for testing and verification;

(3) prepare a detailed report of each actual crisis handled and recovered along with experience gained, lessons learnt, feedback received, lapses observed and proposed measures thereof:

Provided that the relevant information including brief about actual crisis, its handling and takeaways shall be shared with Computer Security Incident Response Team - Power and other stakeholders for collective improvement of cyber security ecosystem of power sector:

Provided further that the Cyber Crisis Management Plan shall be updated by incorporating qualified observations of its own and that of other stakeholders to improve its cyber security posture.

CHAPTER VIII

Cyber Security requirements for Vendor

11. **Cyber Security requirements for vendor -** The vendor shall -

(1) provide documented and tested procedures as well as recovery plan to the entity for restoration of systems supplied by them from potential cyber crisis scenarios;

(2) ensure, either digitally signed or validated and authenticated, security patches and updates for all systems as well as components supplied by them are available to the entity throughout their contract period or useful life of such systems, whichever is later;

(3) provide detailed document to the entity consisting of all requirements and processes including security patches as well as updates required to be installed on the third-party components to integrate a component or sub-system supplied by them;

(4) provide details of end of support or end of life of software, hardware and system to the entity, as applicable, supplied by them including those sourced from third parties;

(5) provide Bill of material to the entity, as per Indian Computer Emergency Response Team guidelines issued from time to time, comprising detailed list of all components supplied by them for applications including firmware, deployed in critical systems;

(6) ensure that the hardware and software are hardened by enabling all inherent security capabilities, secured configuration, and controls, before supplying to the entity;

(7) establish a formal structured process for entities to report vulnerabilities in the products and services. Further, the vendor shall furnish such vulnerabilities to the Computer Security Incident Response Team - Power, through its vulnerability disclosure and management program.

12. **Responsibility of vendors** - In the case of Distributed Generation Resource of prosumers, it shall be the responsibility of vendor to -

(1) ensure that any application, associated monitoring and control servers, and the real-time data of such systems including any data or information hosted on cloud platforms as well as associated historical data or information, be stored in an encrypted, secure, and protected environment and shall reside exclusively within India;

(2) ensure that remote access and remote operation of the grid-connected devices as well as exchange of their real time data and information with remote applications, aggregators, and distribution licensees shall be established through secure channel after mutual authentication and such communication shall be encrypted;

(3) provide such information as may be required for the purpose of verification of a trusted source, in accordance with the orders, directions or guidelines issued by the Central Government from time to time:

Provided that this regulation for the existing Distributed Generation Resource of prosumers shall come into force on such date, as may be specified by the Authority through separate order.

Chapter IX

Cyber Security Audit

13. **Cyber Security Audit** - The entity shall ensure that -

(1) cyber security audit shall be conducted, as per scope detailed in cyber security audit guidelines and directions issued by Computer Security Incident Response Team - Power and other cyber security agencies designated by the Central Government;

(2) the scope of cyber security audit shall also include verification of closure of all audit findings identified in the previous cyber security audit;

(3) the auditor submits its cyber security audit report within six weeks of its commencement, and all critical and high-risk vulnerabilities shall be addressed within a period of one month and medium as well as low risks vulnerabilities within a period of three months from the date of submission of cyber security audit report by the auditor:

Provided that appropriate compensatory controls shall be deployed to contain critical and high-risk vulnerabilities, till audit clearance of such vulnerabilities.

14. **Responsibilities of Chief Information Security Officer** -

(1) Chief Information Security Officer shall review the audit compliances and ensure that the auditor shall submit its cyber security audit closure report within six months from commencement of cyber security audit.

(2) Chief Information Security Officer shall report major audit findings including critical and high-risk vulnerabilities observed in cyber security audit closure report along with any non - compliances with respect to critical systems to the head or board of the entity, as the case may be:

Provided that Chief Information Security Officer - Ministry of Power, may ask for audit closure report of any entity at any point of time for examination and, if need be, after seeking written clarification, with prior approval of the Authority and prior notice to such entity, may appoint a third-party auditor for verification of audit compliances, the cost of which shall be borne by entity:

Provided further that in case the findings of the third-party audit are in variance with the observations of cyber security audit closure report, Chief Information Security Officer - Ministry of Power may take further necessary action.

CHAPTER X

MISCELLANEOUS

15. **Self-audit** - The entity shall conduct self - audit to assess its compliance with these regulations every financial year:

Provided that, for cyber security and compliance with these regulations, the entity may designate any member of the board or of senior management, as the case may be, to be responsible for such compliance:

Provided further that the entity shall address the non-compliances in a time bound manner and ensure that all such non-compliances are addressed before self-audit scheduled in next financial year:

Provided also that Chief Information Security Officer - Ministry of Power, based on the facts available or reported by any individual, may examine compliance report of any entity and after seeking written clarification, with prior approval of the Authority and prior notice to such entity, may appoint a third-party auditor to verify claim made by the entity, the cost of which shall be borne by such entity.

16. In specific cases, after seeking written clarifications and examination thereof, Chief Information Security Officer - Ministry of Power may recommend to the Central Government for initiation of appropriate proceedings under relevant provisions of the Information Technology Act, 2000 (21 of 2000) or to file a petition before Appropriate Commission for proceedings under section 142 of the Act.

17. **Power to Relax** - The Authority through an order, for reasons to be recorded in writing, may relax any of the provisions of these regulations on its own motion or on an application made before it by an interested person to remove the hardship arising out of the operation of any of these regulations, applicable to a class of persons.

FIRST SCHEDULE

[see clause 3(i) of regulation 7]

The following documents and information shall be retained -

1. Cyber Security Policy along with documents and procedures listed therein.
2. Cyber Crisis Management Plan.
3. Data Retention Policy and all documents and information listed thereunder.
4. ISO/ IEC 27001 Certificate or Technical Criteria Certificate.
5. Asset register for cyber assets and critical systems.
6. Cyber Risk Assessment and Mitigation Plan.
7. Incident Response and Recovery Plan.
8. Cyber Security Incident Reporting register.
9. Bill of materials.
10. Business Continuity Plan.
11. Remote operation procedure.
12. Remote access procedure.

THE SECOND SCHEDULE

[see clause 24 of regulation 8]

The suggestive criteria for software updates requiring Prior Cyber Security Audit

Software updates including modifications and enhancements to applications, websites, web portals, and associated systems meeting any of the following criteria shall mandatorily require a successful cyber security audit prior to deployment, namely -

1. **Critical system impact**: Updates that affect core operational processes, such as energy generation, transmission, distribution or load management wherein vulnerabilities could compromise the functionality or reliability of critical infrastructure.
2. **Access control modifications**: Updates that alter user authentication, authorisation mechanisms, or administrative privileges including those involving identity management systems or access control policies.
3. **Integration with third-party systems**: Updates involving integration with external systems, applications or third-party services especially those that exchange sensitive data or enable cross-platform communication.
4. **Security protocol changes**: Updates introducing changes to encryption standards, data transmission protocols or other security-related configurations that could impact the protection of sensitive information.
5. **Introduction of new features or interfaces**: Updates adding significant new functionalities, user interfaces or Application Programming Interfaces that could present potential attack surfaces.
6. **Resolution of security vulnerabilities**: Updates addressing previously identified Critical and High impact vulnerabilities where an incomplete or improper implementation could exacerbate security risks.
7. **Incident response and monitoring systems**: Updates affecting systems or tools related to cyber security monitoring, incident response or log management wherein any disruption could hinder the ability to detect or respond to threats effectively.
8. **Reform or regulatory mandated systems**: Updates impacting systems subject to regulations or pursuant to reforms programs of Appropriate Government.

SHARVAN KUMAR, Secy.

[ADVT.-III/4/Exty./253/2026-27]

Uploaded by Dte. of Printing at Government of India Press, Ring Road, Mayapuri, New Delhi-110064
and Published by the Controller of Publications, Delhi-110054.

VINOD KUMAR
Digitally signed by VINOD KUMAR
Date: 2026.08.05 16:30:06 +05'30'