लेक्चर संख्या	"CEDCLPCSMS100- साइबर सुरक्षा प्रबंधन और अनुपालन" प्रशिक्षण पाठ्यक्रम विषय-वस्तु	अवधि/ कुल घंटे
विषय	**साइबर स्पेस, साइबर सुरक्षा, साइबर अपराध एवं साइबर क़ानून**	
	परिचय : i. साइबर स्पेस एवं शिष्टाचार। ii. साइबर सुरक्षा अवधारणा, परिभाषा (आईटी अधिनियम के अनुसार) और सिद्धांतों को समझे। iii. साइबर सुरक्षा का महत्व एवं आवश्यकता। **साइबर कानून के बारे में संक्षिप्त जानकारी:** i. सूचना प्रौद्योगिकी अधिनियम, 2000 पर परिचय एवं महत्त्वपूर्ण प्रावधान। ii. डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023 पर परिचय एवं महत्त्वपूर्ण प्रावधान। **साइबर अपराध और इसकी रोकथामः** i. साइबर अपराध का परिचय एवं श्रेणी। ii. सूचना प्रौद्योगिकी अधिनियम, 2000 में परिभाषित अपराध। iii. साइबर अपराध के प्रकार। iv. महिलाओं के खिलाफ ऑनलाइन साइबर अपराध और प्रतिरूपण घोटाले। v. कार्यस्थल पर साइबर अपराध।	02 घंटा
	ऑनलाइन वित्तीय धोखाधडी और इसकी रोकथाम: i. विभिन्न ऑनलाइन गतिविधियों से जुड़े साइबर जोखिम और संबंधित सुरक्षा उपाय। ii. कियोस्क बैंकिंग, एटीएम एवं आधार कार्ड आधारित फ्रॉड। iii. पहचान चोरी एवं दस्तावेज का दुरुपयोग कर अवैध लोन, ओटीपी एवं अन्य SMS आधारित फ्रॉड, अज्ञात / असत्यापित मोबाइल ऐप फ्रॉड - लोन, शेयर मार्केट, ई केवाईसी, रिमोट एक्सेस इत्यादि,मोबाइल रिचार्ज शॉप फ्रॉड। iv. मनी म्यूल एकाउंट्सः नये/फ़र्जी खाते खोलने एवं बैंक खातों का ऑनलाइन फ्रॉड में दुरुपयोग। v. फिशिंग लिंक, विशिंग कॉल, एटीएम कार्ड स्किमिंग, ऑनलाइन सेलिंग प्लेटफॉर्म का उपयोग कर धोखाधड़ी, लॉटरी स्कैम, फर्जी इन्वेस्टमेंट स्कैम, ऑनलाइन जॉब फ्रॉड, क्यूआर कोड स्कैन फ्रॉड, सर्च इंजन फ्रॉड, सोशल मीडिया के माध्यम से प्रतिरुपण द्वारा छल, ई-बैंकिंग सेवा (आरटीजीएस/ आईएमपीएस / एनईएफटी) आधारित धोखाधड़ी, ई सिम फ्रॉड, सिम स्वैप / सिम क्लोनिंग, एसएमएस/ ईमेल / इंस्टेंट मैसेजिंग / कॉल स्कैम, ऑनलाइन शॉपिंग फ्रॉड। **शिकायत दर्ज करने हेतु प्रक्रिया:** i. साइबर अपराध सम्बन्धी शिकायत, मध्य प्रदेश साइबर सेल, ऑनलाइन साइबर क्राइम एवं बैंक फ्रॉड की शिकायत, यू पी आई संबंधी शिकायत। ii. आरबीआई बैंक लोकपाल को शिकायत, बैंक एवं हेल्प लाइन नंबर में शिकायत। iii. सोशल मीडिया एवं ऑनलाइन सेवा प्रदाताओं को शिकायत। iv. साइबर अपराध की शिकायत के लिए आवश्यक दस्तावेज क्या हैं? v. न्याय निर्णायक अधिकारी।	
विषय	**ई-गवर्नेंस एवं शासकीय कंप्यूटर संसाधनों से संबंधित नीति, नियम एवं सुरक्षा**	03 घंटा
	इलेक्ट्रॉनिक रिकॉर्ड एवं डिजिटल सिग्नेचर सर्टिफिकेटः i. इलेक्ट्रॉनिक रिकॉर्ड एवं इलेक्ट्रॉनिक रिकॉर्ड की प्रामाणिकता।	

	ii. डिजिटल सिग्नेचर क्या है, कौन जारी करता है तथा कितने प्रकार के होते है। iii. कानूनी मान्यता एवं प्रावधान। iv. डिजिटल हस्ताक्षर का उपयोग कर इलेक्ट्रॉनिक रिकॉर्ड का प्रमाणीकरण। v. डिजिटल हस्ताक्षरः तकनीकी एवं कानूनी मुद्दे।	
	शासकीय कंप्यूटर एवं कंप्यूटर संसाधनों से संबंधित नियम एवं प्रावधान i. आईटी अधिनियम 2000 के तहत संरक्षित प्रणाली एवं महत्व। ii. कंप्यूटर एवं कंप्यूटर संसाधनों से संबंधित नियम तथा उपयोगकर्ता/अधिकारी की जिम्मेदारी। iii. इलेक्ट्रॉनिक रिकॉर्ड और सूचना की गोपनीयता और सुरक्षा। iv. मध्य प्रदेश ईमेल नीति 2014 का अवलोकन। **साइबर अपराध जांचः हैंडिलिंग और घटना प्रबंधन** i. साइबर अपराध की प्रकृति को समझे। ii. साइबर अपराध बनाम पारंपरिक अपराध। iii. साइबर अपराध जांच प्रक्रिया एवं मानक संचालन प्रक्रिया। iv. इलेक्ट्रॉनिक साक्ष्य और उपकरणों की हैंडिलिंग एवं सुरक्षा प्रक्रिया। v. जांच करने में जांच अधिकारी/प्रस्तुतकर्ता अधिकारी की भूमिका।	
विषय	**ई-भुगतान और ई-टेंडरिंग (E-Payment and E-tendering) सुरक्षा**	**01 घंटा**
	ई-टेंडरिंगः संबंधित साइबर खतरे, सुरक्षा उपाय, आई टी नियम-निर्देश एवं केस अध्ययन	
	इलेक्ट्रॉनिक आहरण एवं संवितरण प्रक्रियाः संबंधित जोखिम एवं सुरक्षा उपाय: i. IFMS (/PIMS) ऑपरेशन एवं भुगतान प्रक्रियाः जोखिम एवं सावधानियाँ। ii. इलेक्ट्रॉनिक पेमेंट ऑर्डर में डिजिटल सिग्नेचर सर्टिफिकेट की भूमिका एवं सुरक्षित प्रबंधन। iii. ईपीओ के संचालन के अंतर्गत इलेक्ट्रॉनिक भुगतान से जुड़े जोखिम। iv. ईपीओ से संबंधित संभावित साइबर धोखाधड़ी। v. सुरक्षित ईपीओ लेनदेन: सुरक्षा उपाय। vi. वन टाइम पासवर्ड का महत्व और इसका सुरक्षित प्रबंधन। vii. ईपीओ करते समय ध्यान रखने योग्य सावधानियां। viii. वन टाइम पासवर्ड का महत्व और इसका सुरक्षित प्रबंधन।	
	शिकायत एवं नुकसान की भरपाई के लिए विशेष प्रावधान: i. सूचना प्रौद्योगिकी अधिनियम के अंतर्गत इलेक्ट्रॉनिक भुगतान में हुए अनाधिकृत ट्रांजैक्शन/फ्रॉड की शिकायत। ii. अनाधिकृत अवैध ट्रांजैक्शन से शासकीय कोषालय को क्षतिपूर्ति के लिए विशेष न्यायालय एवं आवेदन प्रक्रिया।	
विषय	**साइबर सुरक्षा प्रबंधन: कार्यान्वयन, अनुपालन और मूल्यांकन**	**06 घंटा**
	परिचय- साइबर सुरक्षा प्रबंधन समाधानः कार्यान्वयन, अनुपालन और मूल्यांकन:	
	• Computer Emergency Reponses Team- Indian (Ministry of Electronics and Information Technology) द्वारा निर्धारित Guidelines on Information Security Practices for Government Entities " साइबर सुरक्षा नियंत्रण • MPCERT-Advisory dated 12.08.2024 • मध्यप्रदेश वित्त मंत्रालय- a. पत्र क्रमांक 927/आर-504/2019/ब-1/04, भोपाल, 28.07.2022 b. पत्र क्रमांक 564/आर-504/2019/ब-1/04, भोपाल, 19.04.2023	

	• मध्यप्रदेश ईमेल नीति, 2014 • मध्यप्रदेश कोषालय, 2020	
	Section II - Guidelines on Information Security Practices for Government Entities	
	पासवर्ड सुरक्षा प्रबंधन	
1.	सुरक्षित एवं कठिन पासवर्ड सेट करें। जिसके लिये निम्नलिखित नियमों का पालन करें।	
	a. कम से कम 10 अल्फान्यूमेरिक [अक्षर (A-Z, a-z) या अंक (0-9)]अक्षरों वाला हो।	
	b. इसमें कैपिटल (ABC…..Z) और स्मॉल (abc…. z) दोनों अक्षर हों।	
	c. इसमें कम से कम एक संख्या (उदाहरण के लिए, 0-9) हो।	
	d. इसमें कम से कम एक विशेष वर्ण (उदाहरण के लिए: $, %, ^, &, *, (,), +, |, ~, -, =, \,`, {, }, [,], :, ", ;, ', <, >, ?, /,,) हो।	
	e. सुरक्षित एवं कठिन पासवर्ड का उदाहरण: ^%Pl@Y! NiCE2024, !nsideMy#C4stle0fC0des	
2.	आसान एवं कमजोर पासवर्ड सेट न करें, कमजोर पासवर्ड की निम्नलिखित विशेषताएं होती हैं:	
	i. इसमें 10 अक्षरों से कम हों।	
	ii. ऐसे शब्द जो शब्दकोश में पाया जा सके। जैसे एक शब्द, नंबर, जगह का नाम, जानवरों के नाम अथवा नाम न हो ।	
	iii. इसमें व्यक्तिगत जानकारी जैसे जन्मतिथि, पते, फोन नंबर, या परिवार के सदस्यों, पालतू जानवरों, दोस्तों और काल्पनिक पात्रों के नाम शामिल हों।	
	iv. इसमें कार्य-संबंधी जानकारी जैसे भवनों के नाम, सिस्टम कमांड, साइट्स, कंपनियां, हार्डवेयर या सॉफ़्टवेयर शामिल हों।	
	v. इसमें संख्या पैटर्न जैसे aaabbb, qwerty, zyxwvuts, या 123321 शामिल हों।	
	vi. इसमें सामान्य शब्दों को उल्टा लिखना, या नंबर के साथ लिखना (उदाहरण के लिए: terces, secret1 या 1secret) शामिल हों।	
3.	अलग-अलग यूजर अकाउंट के लिये एक ही या एक जैसे पासवर्ड का उपयोग न करें।	
4.	पासवर्ड को नियमित रूप से 30 दिन में बदलें।	
5.	पासवर्ड को किसी के साथ साझा न करें। जिसमें प्रशासनिक सहायक, सचिव, प्रबंधक, सहकर्मी और परिवार के सदस्य भी शामिल हैं। क्योंकि सभी पासवर्ड संवेदनशील, गोपनीय जानकारी होती है एवं व्यक्तिगत उपयोग के लिये जारी किये गये है।	
6.	पासवर्ड को ईमेल मैसेज या अन्य इलेक्ट्रॉनिक संचार (जैसे: वाट्सएप चैट) में Save न करें।	
7.	फोन पर पासवर्ड या वन टाइम पासवर्ड (OTP) न बतायें।	
8.	पासवर्ड को कार्यालय में कहीं भी लिख कर न रखें। पासवर्ड को किसी कंप्यूटर सिस्टम या मोबाइल उपकरणों (फोन, टैबलेट) पर बिना एन्क्रिप्शन के Store न करें।	
9.	एप्लिकेशन (उदाहरण के लिए, वेब ब्राउज़र) की "Remember Password" सुविधा का उपयोग न करें।	
10.	किसी भी यूजर को संदेह होने पर कि उसका पासवर्ड असुरक्षित हो गया है जैसे पासवर्ड चोरी, हैक या किसी को शेयर कर दिया है तो उस घटना की रिपोर्ट करें एवं शीघ्र सभी पासवर्ड बदले।	
11.	नया पासवर्ड अंतिम तीन पासवर्ड की तरह न हो।	
	इंटरनेट ब्राउज़िंग सुरक्षा प्रबंधन	
12.	शासकीय एप्लिकेशन, ईमेल, बैंकिंग/भुगतान संबंधी सेवाओं या किसी अन्य महत्वपूर्ण एप्लिकेशन को एक्सेस करते समय ब्राउज़र में निजी/गुप्त मोड (Private/Incognito Mode-Ctrl+Shift+N) का उपयोग करें।	

13.	यदि सीधे वेब लिंक पर क्लिक/एक्सेस करते समय, यूज़र लॉगिन की आवश्यकता हो, तो लिंक पर क्लिक न करें, हमेशा साइट का डोमेन नाम/URL ब्राउजर में टाइप करें।	
14.	इंटरनेट ब्राउज़र के latest version का उपयोग करें ।	
15.	ब्राउज़र नवीनतम पैच के साथ अपडेट रखें।	
16.	इंटरनेट ब्राउज़र पर कोई भी Username, पासवर्ड या ऑनलाइन भुगतान संबंधी जानकारी save न करें।	
17.	इंटरनेट ब्राउज़र पर अनजान सेवाएं Third party टूल बार Nord VPN, Express VPN, Tor, Proxy/download manager, weather tool bar, ask me tool bar etc.) का उपयोग प्रतिबंधित करें।	
18.	कार्यालयीन कम्प्यूटर में कोई भी गेम इंस्टॉल न करें और न ही गेम खेलने के लिये उपयोग करें।	
19.	किसी भी Shorten URL (जैसे: tinyurl.com/ab534/) पर सीधे क्लिक न करें, यह फ़िशिंग/मैलवेयर वेब पेज पर ले जा सकता है या रेंसमवेयर जैसे हानिकारक प्रोग्राम सिस्टम में इंस्टॉल कर सकता है।	
20.	प्राइवेसी एवं सिक्योरिटी सेटिंग [जैसे: ब्राउजर एक्सेस के लिये सुरक्षित एवं कठिन पासवर्ड सेट करें, कुकीज़ डिलीट करें एवं मल्टी फैक्टर ऑथेंटिकेशन इत्यादि सक्रिय करें] कन्फिगर (Configure) करें।	
	डेस्कटॉप सुरक्षा प्रबंधन	
21.	कार्यालय के कंप्यूटर/लैपटॉप एक्सेस (Access) करने के लिए सभी अधिकारी/कर्मचारी के लिये Non-Administrator Account Create करें एवं उपयोग करें।	
22.	सिस्टम बूटिंग के लिए बायोस (BIOS) लेवल पासवर्ड सेट करें। नोट:	
23.	**ऑपरेटिंग सिस्टम को ट्रस्टेड सोर्स से ऑटो अपडेट के लिये सेट करें।**	
24.	नवीनतम एवं लाइसेंस एंटी वायरस कम्प्यूटर/लैपटॉप पर इंस्टॉल करें एवं ऑटो अपडेट के लिये सेट करें।	
25.	केवल अधिकृत एवं लाइसेंस्ड एप्लिकेशन/ सॉफ्टवेयर उपयोग किये जायें।	
26.	यूजर अकाउंट एवं आवश्यकतानुसार अन्य एप्लीकेशनों में सुरक्षित एवं कठिन पासवर्ड सेट करें।	
27.	ऐडमिन अकाउंट (Admin Account) को अन्य कर्मचारी या गेस्ट (Guest) यूजर को उपयोग करने की अनुमति न दें।	
28.	कार्यालय या वर्कस्टेशन छोड़ते समय या उपयोग नहीं करने पर कम्प्यूटर लॉक (Window+L), logoff या shutdown करें।	
29.	संस्थान/कार्यालय के कंप्यूटर संसाधनों एवं सिस्टम की Vulnerability Assessment/Penetration Testing सुरक्षा ऑडिट करें। * प्रत्येक 06 माह में इंटर्नल सिक्योरिटी ऑडिट एवं वार्षिक रूप से CERT-In से पैनल बद्ध एजेंसी से Third party सुरक्षा ऑडिट करायें।	
30.	सक्षम अधिकारी की विशिष्ट अनुमोदन के अलावा कार्यालय एवं कंप्यूटर संसाधनों पर रिमोट एक्सेस (Remote Access) अक्षम (disable) रखें एवं उपयोग न करें। नोट: यदि विशिष्ट कार्यों के लिये प्राधिकारी द्वारा स्वीकृति दी जाती है तो उसका रिकार्ड सुरक्षित करें। किसी भी रिमोट डेस्कटॉप एप्लिकेशन जैसे कि एनीडेस्क, टीमव्यूअर, एमी एडमिन आदि के उपयोग को प्रतिबंधित करें।	
31.	कार्यालय के डेस्कटॉप/लैपटॉप पर USB/CD तक पहुंच सीमित करें। नोट: उपयोग न होने पर USB/CD पोर्ट डिसेबल करें।	
	डाटा सुरक्षा प्रबंधन	
32.	संस्थान/ कार्यालय के एंडपॉइंट्स (जैसे:यूएसबी पोर्ट, ईमेल या अन्य डेटा ट्रांसफर माध्यम) को डेटा के अनाधिकृत निष्कासन (exfiltration) एवं चोरी से सुरक्षित रखें ।	

	नोट: सुरक्षा सोल्यूशन जैसे डेटा लॉस प्रिवेंशन (DLP), फायरवॉल, बायोमेट्रिक सुरक्षा, USB/Wi-Fi को डिसैबल करना, पैच मैनेजमेन्ट आदि का उपयोग करें। 1. यूएसबी पोर्ट/सीडी रोम ड्राइव डिसेबल रखे। 2. External user को ऑफिस कंप्युटर एक्सेस करने के लिए 'guest user account' बनाए एवं आवश्यकतानुसार डाटा/ फाइल ट्रांसफर के लिए ऐड्मिन से अनुमति प्रदान करें। 3. अनौपचारिक वेबसाइट/मेल ब्लॉक करे। 4. कम्प्यूटर सिस्टम में "व्हाट्सएप" को इंस्टॉल न करे फाइल/डाटा ट्रांसफर के लिये ईमेल सर्विस का उपयोग करें। विशेष परिस्थतियों मे "व्हाट्सएप" उपयोग करने पर केवल डाटा/फाइल प्राप्त करने की अनुमति दे जबकि फाइल ट्रांसफर/सेंड की अनुमति न दे। 5. कार्यालीन डाटा/ फाइल ट्रांसफर के लिए आधिकारिक मोबाइल फोन का उपयोग करे। 6. कर्मचारी द्वारा कार्यालय छोड़ने पर तत्काल रूप से उसके दिए गये अकाउंट एवं क्रेडेंटियल्स जैसे आई डी पासवर्ड डीऐक्टिवेट करे तथा 180 दिन तक उपयोग न होने पर अकाउंट को डिलीट किया जा सकता है।	
33.	अधिकारी/कर्मचारी कार्यालय की जानकारी या डेटा को गोपनीय रखें।	
34.	किसी भी परिस्थिति में सक्षम अधिकारी की अनुमति के बिना संस्थान/कार्यालय के संवेदनशील (Sensitive) या गोपनीय डाटा को किसी भी बाहरी व्यक्ति या एजेंसी के साथ शेयर न करे।	
35.	संस्थान/कार्यालय में मुख्य कंप्यूटर सिस्टम का निर्धारित समयान्तराल पर नियमित रूप से डाटा बैकअप लें।	
36.	e-Waste management: कम्प्यूटर संसाधनों (जैसे: स्टोरेज डिवाइस, प्रिंटर) का निपटान या विक्रय करते समय स्टोर डाटा को Wipe करें। नोट: डेटा वाइपिंग टूल का उपयोग करें।	
37.	जब कोई कर्मचारी अपनी नौकरी छोड़ता है या प्रोजेक्ट पूरा करता है या उसकी भूमिका परिवर्तित होती है, तो उस स्थिति में कार्यालय से जुड़ी जानकारी (Data) को वापस लें। नोट: यूजर अकाउंट और एक्सेस अधिकारों को निष्क्रिय या ब्लॉक कर सुरक्षित करें। Employee Exit Form का उपयोग किया जा सकता है।	
	ई-भुगतान सुरक्षा प्रबंधन	
38.	ब्राउज़र में अपने PFMS के लॉगिन Credentials को सेव न करे। *ई-भुगतान यूजर अकाउंट का पासवर्ड ईमेल आई डी का पासवर्ड न रखें।	
39.	सभी अकाउंट के डिफॉल्ट पिन, लॉगिन पासवर्ड नियमित रूप से पासवर्ड सुरक्षा प्रबंधन के क्लॉज़ 01 के अनुसार बदलते रहे।	
40.	कम्प्यूटर सिस्टम में "व्हाट्सएप" को इंस्टॉल न करे फाइल/डाटा ट्रांसफर के लिये ईमेल सर्विस का उपयोग करें।	
41.	ई-भुगतान अकाउंट का एक्सेस किसी अन्य को न दें और ना ही Credentials शेयर करें।	
42.	कमरों की सफाई और हाउसकीपिंग स्टाफ द्वारा कागज़ के कचरे को हटाने का काम केयरटेकर स्टाफ़ की देखरेख में करवायें।	
43.	संदिग्ध ईमेल या किसी भी सुरक्षा घटना की रिपोर्ट event@cert-in.org.in और event@nic-cert.nic.in पर करें। नोट: NIC-CERT (https://nic-cert.nic.in/advisories.jsp) और CERT-In (https://www.cert-in.org.in) द्वारा प्रकाशित सुरक्षा सलाह का पालन करें।	
44.	किसी भी भुगतान से पहले निर्धारित प्रक्रिया के अनुसार सभी बिलों की पूर्व जांच करें।	
45.	संवेदनशील सीटों पर संविदा कर्मचारियों को नियुक्त न करें।	

46.	पंजीकृत मोबाइल नंबर पर प्राप्त मैसेज, जानकारी या वन टाइम पासवर्ड (OTP) किसी के साथ शेयर न करें।	
47.	**बैंक रिकॉन्सिलिएशन एवं इन्टर्नल चेक/ऑडिट**	
	एजेंसी एडमिन को साप्ताहिक निम्नानुसार इन्टर्नल चेक/ऑडिट करना चाहिए।	
	i. पेमेंट असफलता एवं इसके कारण का पता लगाएं।	
	ii. सभी सफल भुगतान ट्रांसफर होने पर वेरीफाई करें एवं बेनिफिशरी खाते की जांच करें।	
	iii. बैंक अकाउंट बैलन्स को actual पासबुक बैलेंस से मैच करें।	
48.	**डिजिटल सिग्नेचर सर्टिफिकेट सुरक्षा प्रबंधन**	
	i. अधिकृत डीएससी उपयोगकर्ता/स्वामी अपने डीएससी का स्वयं उपयोग करें एवं किसी भी अन्य व्यक्ति को डीएससी शेयर न करें यदि डीएससी के अनधिकृत उपयोग से संबंधित कोई कानूनी मुद्दा होता है तो इसकी जिम्मेदारी डीएससी स्वामी की होगी।	
	ii. डीएससी चोरी या गुमने पर तत्काल रूप से संबंधित प्रमाणन प्राधिकारी या अधिकारी को शिकायत करें।	
	iii. डीएससी के पासवर्ड की सुरक्षा का प्रबंधन पासवर्ड सुरक्षा प्रबंधन के क्लॉज़ 01 के अनुसार सुनिश्चित करें।	
	iv. डीएससी की वैधता चेक करें यदि वैधता समाप्त हो जाती है तो डीएससी का उपयोग न करें।	
	v. किसी भी गैर कानूनी कार्यों मे डीएससी का उपयोग न करें।	
	vi. बैच में भुगतान करते समय डीएससी साइन/उपयोग करने से पहले प्रत्येक फिज़िकल बिल को चेक करें।	
	vii. कार्यालय के अतिरिक्त बाहिरी कम्प्यूटर का उपयोग करके भुगतान करने में डीएससी का उपयोग न करें।	
	viii. ऑनलाइन भुगतान एवं फिज़िकल डॉक्यूमेंट सत्यापन करने में शासन द्वारा जारी दिशा-निर्देश व प्रक्रिया का पालन करें जब तक की विशेष दिशा-निर्देश जारी न किए गए हो।	
49.	**घटना प्रबंधन:** किसी भी स्थिति में ई-भुगतान अकाउंट के अनाधिकृत एक्सेस और/या अवैध राशि ट्रांसफर, पासवर्ड चोरी होने पर सक्षम अधिकारी को सूचित करें एवं सूचना प्रौद्योगिकी अधिनियम, 2000 के अनुसार आपराधिक जांच व क्षतिपूर्ति के लिये वैधानिक कार्यवाही करें।	
	ई-मेल सुरक्षा प्रबंधन	
50.	नियमानुसार सुरक्षित एवं कठिन पासवर्ड सेट करें।	
51.	म प्र ई-मेल नीति, 2014 के समस्त प्रावधानों का अनुपालन करें।	
52.	ईमेल द्वारा किये गये किसी मेल एवं सूचना की जिम्मेदारी अधिकृत उपयोगकर्ता/मालिक की होगी। अत: केवल वैध एवं कार्यालयीन कार्यों में ही ई मेल सेवा का उपयोग करें।	
53.	ई मेल अकाउंट किसी अन्य व्यक्ति को उपयोग करने न दें।	
54.	आधिकारिक संचार के लिए कभी भी किसी अनधिकृत/बाहरी ईमेल सेवा का उपयोग न करें। जैसा कि मध्य प्रदेश ईमेल नीति के clause 1.2.3 में उल्लिखित है।	
55.	अटैचमेंट डाउनलोड करने से पहले Sender का ईमेल पता Verify करें।	
56.	"Login history" टैब पर क्लिक करके नियमित रूप से पिछले login गतिविधियों की समीक्षा करें।	
57.	ई मेल अकाउंट पर Two-Factor Authentication enable करें।	
58.	संवेदनशील दस्तावेज सार्वजनिक नेटवर्क में डाउनलोड न करें।	
59.	ई-मेल के माध्यम से फ़ाइल transfer में एन्क्रिप्शन या गोपनीय मोड इनैबल करें। नोट: Confidential Toggle Mode का उपयोग किया जा सकता है।	

	रिमूवेबल (Removable) मीडिया सुरक्षा प्रबंधन	
60.	केवल कार्यालय के रिमूवेबल मीडिया (Pen drive, Memory Card, portable Hard disk, etc.) उपकरणों का ही उपयोग करें।	
61.	कर्मचारियों को निर्देश दें कि वे सभी रिमूवेबल मीडिया पर अपना नाम, तारीख, और उपयोग का उद्देश्य लिखें।	
62.	उपयोग से पहले रिमूवेबल मीडिया की किसी भी प्रकार की भौतिक क्षति की जाँच करें एक्सेस करने से पहले उसे एंटीवायरस सॉफ़्टवेयर से स्कैन करें।	
63.	रिमूवेबल मीडिया को उपयोग न होने पर लॉकर या दराज में लॉक करें।	
64.	रिमूवेबल मीडिया को बिना देखरेख के या आसानी से पहुंच योग्य जगहों में न छोड़ें।	
65.	पहली बार उपयोग करने से पहले रिमूवेबल मीडिया को फॉर्मेट करें।	
66.	रिमूवेबल मीडिया का उपयोग केवल कार्यालयीन कार्यों में करें।	
67.	किसी भी उद्देश्य के लिए रिमूवेबल मीडिया का उपयोग करने से पहले आवश्यक अनुमति प्राप्त करें।	
68.	मैलवेयर या अनधिकृत पहुंच के जोखिम को कम करने के लिए सार्वजनिक या अविश्वसनीय कंप्यूटरों पर रिमूवेबल मीडिया का उपयोग करने से बचें।	
69.	रिमूवेबल मीडिया में स्टोर दस्तावेज़ों को हमेशा सुरक्षित एवं कठिन पासवर्ड से सुरक्षित रखें।	
70.	कभी भी रिमूवेबल मीडिया को अनधिकृत व्यक्तियों या संगठनों के साथ शेयर न करें।	
	मोबाइल एवं सिम सुरक्षा प्रबंधन	
71.	फोन में सुरक्षित एवं कठिन पासवर्ड सेट करें। एवं अपना फोन किसी अन्य व्यक्ति को उपयोग करने न दें।	
72.	फोन में एप्लीकेशन परमिशन प्रबंधित करें। जैसे: आवश्यकतानुसार किसी भी एप्लीकेशन को कैमरा, माइक, लोकेशन या कॉन्टेक्ट लिस्ट इत्यादि एक्सेस करने की अनुमति दें।	
73.	Google (एंड्रॉइड के लिए) और ऐप्पल (iOS के लिए) के आधिकारिक ऐप स्टोर से ऐप डाउनलोड करें।	
74.	फोन में अवांछित एप्लीकेशन या अनजान व्यक्ति द्वारा वाट्सएप्प पर भेजी गई '.apk' एप्लीकेशन फाइल इंस्टॉल न करें।	
75.	फोन में शासन द्वारा अधिकृत एंटी वायरस एप्लीकेशन जैसे: M-Kavach 2.0 (C-DAC द्वारा जारी) इत्यादि इंस्टॉल करें। एवं नियमित रूप से स्केन करें।	
76.	शासकीय सेवाओं एवं ऑनलाइन अकाउंट में पंजीकृत मोबाइल नंबर की सिम बंद होने पर शीघ्र शिकायत करें एवं तत्काल रूप से सक्रिय करावें।	
77.	पंजीकृत मोबाइल नंबर पर प्राप्त मैसेज, जानकारी या वन टाइम पासवर्ड (OTP) किसी के साथ शेयर न करें।	
78.	मोबाइल आपरेटिंग सिस्टम एवं एप्लीकेशन को नियमित रूप से अपडेट करें।	
79.	मोबाइल फोन पर वाई-फाई, जीपीएस, ब्लूटूथ, एनएफसी और अन्य सेंसर को बंद रखें। इन्हें केवल आवश्यकता पड़ने पर ही चालू करें।	
80.	अपने फोन में ऑटो डाउनलोड को बंद करें।	
81.	कार्यालय मे काम करते समय आधिकारिक मोबाइल फोन एवं मोबाईल नंबर का उपयोग करे।	
82.	कोई भी applications बिना अप्रूवल के कार्यालीन मोबाईल फोन मे इंस्टॉल न करे।	
83.	कार्यालीन मोबाईल फोन मे केवल कार्यालीन ईमेल आई डी का उपयोग करे।	
84.	कार्यालीन मोबाईल फोन मे public Wi-Fi का उपयोग न करे।	
	सोशल मीडिया सुरक्षा प्रबंधन	
85.	सुरक्षित एवं कठिन पासवर्ड सेट करें।	
86.	सोशल मीडिया और नेटवर्किंग साइट्स पर जाते समय व्यक्तिगत जानकारी के उपयोग/एक्सपोज़र को	

	सीमित और नियंत्रित करें।	
87.	किसी friend request को स्वीकार करने से पहले हमेशा व्यक्ति की प्रामाणिकता की जाँच करें।	
88.	सोशल मीडिया अकाउंट को सुरक्षित करने के लिए मल्टी-फैक्टर ऑथेंटिकेशन का उपयोग करें।	
89.	किसी भी अज्ञात संपर्क/उपयोगकर्ता द्वारा भेजे गए लिंक या फ़ाइलों पर क्लिक न करें।	
90.	सोशल मीडिया पर कोई भी आंतरिक सरकारी दस्तावेज़ या जानकारी प्रकाशित, पोस्ट या साझा न करें।	
91.	सोशल मीडिया के माध्यम से कोई भी असत्यापित जानकारी प्रकाशित, पोस्ट या साझा न करें।	
92.	किसी भी सोशल मीडिया प्लेटफ़ॉर्म पर @gov.in/@nic.in ईमेल पता साझा न करें।	
93.	आधिकारिक संचार के लिए किसी तीसरे पक्ष के मैसेजिंग ऐप के बजाय NIC के संदेश ऐप का उपयोग करें।	
	नेटवर्क सुरक्षा प्रबंधन	
94.	नेटवर्क एक्सेस के लिये एक्टिव यूजर डायरेक्टरी बनायें। नेटवर्क एक्सेस लॉग को 180 दिनों तक सुरक्षित रखें। नोट: सर्वर एवं firewall का उपयोग किया जा सकता है ।	
95.	पहली बार इंस्टालेशन के बाद सभी डिफ़ॉल्ट क्रेडेंशियल्स/ पासवर्ड और कॉन्फ़िगरेशन बदलें। नोट: संस्थान/ कार्यालय को यह सुनिश्चित करना होगा कि नेटवर्क उपकरणों और सूचना प्रणालियों के डिफ़ॉल्ट क्रेडेंशियल्स, जैसे उपयोगकर्ता नाम, पासवर्ड और टोकन इत्यादि पहली बार उपयोग से पहले बदल दिए जाएं।	
96.	Bring Your Own Device को प्रतिबंधित करें तथा नेटवर्क एड्मिनिस्ट्रेटर की अनुमति के बिना किसी भी अज्ञात कम्प्यूटर संसाधन को नेटवर्क में Access की अनुमति न दें।	
97.	सुनिश्चित करें कि SSID (Service Set Identifier) और/अथवा वाई-फाई उपयोगकर्ताओं के आधार पर नेटवर्क विभाजन हो। यदि विभाजन नहीं किया गया है तो डिवाइस बाइंडिंग सुरक्षा क्रियान्वित करें।	
98.	सुनिश्चित करें कि आवश्यकतानुसार SSID अथवा प्रोफाइल अथवा डिवाइस बाइंडिंग के अनुसार पहुँच Access Control नीतियां लागू करें।	
99.	संस्थान/ कार्यालय यह सुनिश्चित करें कि एक्सेस पॉइंट्स (APs) या WLAN स्विचों पर सभी सुरक्षा उपाय लागू किए जाएं ताकि उन्हें अनधिकृत पहुंच से सुरक्षित रखा जा सके। नोट: Firewall, पासवर्ड सुरक्षा, एवं नियमानुसार सुरक्षा ऑडिट करें।	
100.	कार्यालय में व्यक्तिगत उपकरणों का उपयोग संस्थान/ कार्यालय के संबंधित नेटवर्क ऐड्मिनिस्ट्रेटर द्वारा अधिकृत होना सुनिश्चित करें। नोट:एक्सेस रिक्वेस्ट फार्म का उपयोंग किया जा सकता है ।	
101.	सुनश्चित करे कि उपयोगकर्ता स्तर पर सभी डिवाइसों में यूजर अकाउंट का उपयोग हो और ऐड्मिन अकाउंट का उपयोग केवल नेटवर्क/सिस्टम एडमिनिस्ट्रेटर तक ही सीमित रहे।	
102.	संस्थान/कार्यालय के नेटवर्क का Vulnerability Assessment/Penetration Testing सुरक्षा ऑडिट करें। * प्रत्येक 06 माह में इंटर्नल सिक्योरिटी ऑडिट एवं वार्षिक रूप से CERT-In से पैनलबद्ध एजेंसी से Third party सुरक्षा ऑडिट करायें।	
	भौतिक सुरक्षा प्रबंधन	
103.	कम्प्यूटर संसाधन एवं आईटी प्रणालियों तक अनधिकृत एक्सेस, भौतिक क्षति और छेड़छाड़ को रोकें ।	
104.	केवल अधिकृत कर्मियों को संवेदनशील क्षेत्रों (जैसे: सर्वर रूम) के एक्सेस की अनुमति दें तथा पहचान पत्र, बायोमेट्रिक, और विज़िटर लॉग रजिस्टर इत्यादि के माध्यम रिकार्ड रखें।	
105.	निगरानी और मॉनिटरिंग:	

i. सीसीटीवी मॉनिटरिंग सिस्टम का उपयोग करें जिसमें 90 दिनों की सीसीटीवी फुटेज को स्टोर करने की क्षमता हो।

106. कार्यालय के सभी कम्प्यूटर संसाधनों का इन्वेन्टरी रिकार्ड/ (Assets Management Record) रखें जिसमें कम्प्यूटर संसाधनों की लेबलिंग और हैंडलिंग तथा अधिकारी/कर्मचारी को आवंटित कम्प्यूटर संसाधन की जानकारी आदि शामिल हो।

107. जब कोई कर्मचारी अपनी नौकरी छोड़ता है या प्रोजेक्ट पूरा करता है या उसकी भूमिका परिवर्तित होती है, तो उस स्थिति में कार्यालय द्वारा प्रदत्त सभी कम्प्यूटर संसाधन , मोबाइल या अन्य उपकरण वापस लें। Employee Exit Form उपयोग किया जा सकता है।

सामान्य सुरक्षा प्रबंधन

108. कार्यालय में आई टी सेवाऐं प्रदान करने वाले एवं कम्प्यूटर संसाधनों को एक्सेस करने वाले किसी भी सेवा प्रदाता/वेंडर के कर्मचारियों के साथ, गोपनीयता समझौते (Non discloser agreement) के साथ एक्सेस रिक्वेस्ट फार्म हस्ताक्षरित करवायें।

109. वेंडर/सर्विस प्रोवाइडर के साथ सर्विस लेवल एग्रीमेंट (SLA) हस्ताक्षरित करें।

110. संविदा/अनुबंधित कर्मचारी द्वारा नियुक्ति पत्र के साथ गोपनीयता समझौता (Non discloser agreement) हस्ताक्षरित करवायें।

111. एग्रीमेंट को अपडेट रखें जिससे यह समय के साथ प्रभावी बना रहे।
नोट: जो भी अनुबंध संस्थान की तरफ से बनाए गए है वो समय के साथ अपडेट किये जाने चाहिए।

112. कर्मचारियों के लिए नियमित रूप से सुरक्षा जागरूकता प्रशिक्षण आयोजित करावें।

113. कार्यालय में कम्प्यूटर संसाधनों एवं डाटा पर एक्सेस कन्ट्रोल प्रबंधन निम्नानुसार करें।

1. एक्सेस अधिकार प्रबंधन (Access Rights Management):
   i. अधिकारी/कर्मचारियों को एक्सेस देने, संशोधित करने और हटाने के लिए उनकी भूमिकाओं और जिम्मेदारियों को परिभाषित करें।
   ii. केवल अधिकृत कर्मचारियों को उपयोगिता/आवश्यकतानुसार कम्प्यूटर संसाधनों का एक्सेस दें तथा सुरक्षित उपयोग व प्रबंधन के लिये उचित प्रशिक्षण दें।

नोट: रोल कान्फ्लिक्ट मैट्रिक्स (Role Conflict Matrix) के अनुसार एक्सेस राइट्स आवंटित (allocate) किये जा सकते हैं। रोल कान्फ्लिक्ट मैट्रिक्स (Role Conflict Matrix) यह निर्धारित करने में सहायता करता है कि कौन सी भूमिकाएं या जिम्मेदारियां किस कर्मचारी/अधिकारियों को सौंपी जा सकती हैं। उदाहरण के लिए:

भूमिका/जिम्मेदारी	कार्यालय प्रमुख	अकाउंटेंट	अध्यापक	आईटी स्टाफ
छात्रों के ग्रेड रिकार्ड तक एक्सेस	हाँ	नहीं	हाँ	नहीं
वित्तीय रिकार्ड तक एक्सेस	हाँ	हाँ	नहीं	नहीं
आई टी एडमिनिस्ट्रेटर	हाँ	नहीं	नहीं	हाँ

2. उपयोगकर्ता प्रमाणीकरण (User Authentication):
   i. क्लॉज 1 के अनुसार पासवर्ड प्रबंधन करें एवं अन्य प्रावधानों का अनुपालन करें।
   ii. मल्टी-फैक्टर ऑथेंटिकेशन (MFA) का उपयोग करें।

3. एक्सेस समीक्षा और ऑडिट (Access Review and Audits):
   i. नियमित रूप से एक्सेस अधिकारों की समीक्षा और ऑडिट करें।
   ii. भूमिका में बदलाव या नौकरी छोड़ने पर संबंधित यूजर अकाउंट और एक्सेस अधिकारों को निष्क्रिय या ब्लॉक कर सुरक्षित करें।

4. निगरानी और रिपोर्टिंग (Monitoring and Reporting):- महत्वपूर्ण सिस्टम और डेटा के

	एक्सेस की निरंतर निगरानी करें तथा अद्यतन एक्सेस रिपोर्ट तैयार करें।	
114.	साइबर हमला (Cyber Attack) या साइबर अपराध की घटना की शिकायत शासन द्वारा निर्धारित प्लेटफॉर्म जैसे राष्ट्रीय साइबर हेल्प लाइन नंबर 1930/ www.cybercrime.gov.in या विभागीय ISSC (Information Security Steering Committee) या MPCERT पर करें।	
115.	कार्यालय में क्लियर डेस्क (Clear desk) और क्लियर स्क्रीन (Clear Screen) प्रक्रिया निम्नानुसार क्रियान्वित करें। i. कार्यालय में अनुपस्थित रहने पर, हार्डकॉपी या इलेक्ट्रॉनिक रूप में सभी संवेदनशील/गोपनीय जानकारी सुरक्षित रखें। ii. डेस्क को छोड़ते समय कंप्यूटर को लॉक (Window+L) करें। iii. कार्यालय से बाहर जाते समय कंप्यूटर वर्कस्टेशन को पूरी तरह से बंद करें। iv. उपयोग न होने पर लैपटॉप को दराज या लॉकर में सुरक्षित रखें। v. कम्प्यूटर स्क्रीन पर संवेदनशील जानकारी न रखें एवं स्क्रीन को क्लियर रखें।	
116.	जहां भी कोई कार्य थर्ड पार्टी या वेन्डर सर्विस प्रोवाइडर को आउटसोर्स की जाती है और उन्हें कार्य का कान्ट्रैक्ट (work contract) दिया जाता है, यह सुनिश्चित करें कि कान्ट्रैक्ट में सूचना एवं कम्प्यूटर संसाधन सुरक्षा की आवश्यकताएं शामिल हैं। नोट: जैसे यदि छात्रों/कर्मचारियों का प्रशिक्षण या ऑनलाइन परीक्षा किसी बाहरी संस्था से कराई जाती है तो उसके अनुबंध में भारतीय कानून एवं मानक डाटा सुरक्षा उपायों का पालन करनें का प्रावधान होने का सुनिश्चित करे।	
117.	कार्यालय में इन्वर्टर/ पावर बैकअप सिस्टम रखें।	
118.	प्रिंटआउट्स एवं फोटोकॉपी का लॉग (रिकॉर्ड) रखें।	
119.	यदि एक कम्प्यूटर को एक से ज्यादा यूजर द्वारा उपयोग करने की स्थिति में अलग-अलग यूजर अकाउंट का उपयोग करें एवं एक्सेस लॉग रजिस्टर का रखरखाव करें।	
120.	अनौपचारिक एवं अप्पतिजनक वेब कंटेन्ट एवं वेबसाईट को न खोले ।	