सत्यमेव जयते

Department of Information Technology & Communication, Rajasthan

SecLAN / RajSWAN / RajNET - नेटवर्क पर संचालित होने वाले आधिकारिक कंप्यूटर सिस्टम के लिए

साइबर सुरक्षा की गाइडलाइन

*V.**1.0** दिनांक: 24-04-2026*

***संपर्क करें**: साइबर सुरक्षा संचालन केंद्र (SOC),*

सूचना प्रौद्योगिकी एवं संचार विभाग
राजस्थान सरकार
राजस्थान स्टेट डाटा सेंटर (RSDC-P4), जयपुर

*ईमेल: **fms.soc@rajasthan.gov.in***

विषय सूची

क्र. सं.	अनुभाग	पृष्ठ संख्या
1	**अनुभाग 1: सभी आंतरिक सिस्टम पर एंटीवायरस सॉफ्टवेयर की स्थापना (अनिवार्य - सबसे पहले करें)**	03
2	**अनुभाग 2: डेस्कटॉप हार्डनिंग एवं सिस्टम सुरक्षा (अनिवार्य दैनिक अभ्यास)**	06
3	**अनुभाग 3: ईमेल सुरक्षा (सबसे सामान्य अटैक माध्यम)**	09
4	**अनुभाग 4: इंटरनेट एवं ब्राउज़र सुरक्षा**	12
5	**अनुभाग 5: पासवर्ड एवं एक्सेस प्रबंधन**	15
6	**अनुभाग 6: USB, फाइल एवं डेटा प्रबंधन**	17
7	**अनुभाग 7: सुधार के बाद निगरानी (Post-Remediation Monitoring)**	19
8	**अनुभाग 8: महत्वपूर्ण सहायता एवं संदर्भ**	21

दस्तावेज़ नियंत्रण और योगदान

संस्करण	तिथि	परिवर्तन का विवरण	तैयार किया	समीक्षा (L1)	समीक्षा (L2/CISO)	अनुमोदन
0.1	18-02-2026	प्रारंभिक ड्राफ्ट	श्री चारु अग्रवाल	श्री पवन कुमार जांगिड़	—	—
0.2	19-02-2026	आंतरिक समीक्षा के बाद अद्यतन	श्री चारु अग्रवाल	श्री पवन कुमार जांगिड़	श्री अनिल कुमार सिंह	—
0.3	***27-02-2026***	***विस्तृत समीक्षा के बाद अद्यतन***	***श्री चारु अग्रवाल, ACP (DD)SOC***	***श्री पवन कुमार जांगिड़, AD, OIC (SOC)***	***श्री अनिल कुमार सिंह, निदेशक (तकनीकी) एवं CISO***	***श्री हिमांशु गुप्ता, आयुक्त एवं विशिष्ट शासन सचिव***
1.0	***24-04-2026***	***अंतिम संस्करण***	***श्री चारु अग्रवाल, ACP (DD)SOC***	***श्री पवन कुमार जांगिड़, AD, OIC (SOC)***	***श्री अनिल कुमार सिंह, निदेशक (तकनीकी) एवं CISO***	***श्रीमती अर्चना सिंह, शासन सचिव***

अनुभाग 1: सभी आंतरिक सिस्टम पर एंटीवायरस सॉफ़्टवेयर की स्थापना

(अनिवार्य - सबसे पहले करें)

1.1 सरकार द्वारा अनुमोदित Advanced AV / EDR स्थापित करें (सर्वोच्च प्राथमिकता)

- हर SecLAN/RajSWAN/RajNET कंप्यूटर में एक **अनुमोदित एंटीवायरस** या Endpoint Detection & Response (EDR) सॉल्यूशन होना ज़रूरी है।
- SecLAN/RajSWAN/RajNET कंप्यूटर सिस्टम, राजस्थान सरकार के आधिकारिक internal नेटवर्क पर काम करते हैं; इन नेटवर्क का इस्तेमाल पूरे राज्य में मौजूद अलग-अलग सरकारी विभागों और दफ़्तरों (जिनमें ज़िले, ब्लॉक और ग्राम पंचायत भी शामिल हैं) के बीच सुरक्षित संचार और डेटा के लेन-देन के लिए किया जाता है।
- **इन नेटवर्क से जुड़े कंप्यूटर संवेदनशील सरकारी डेटा को संभालते हैं, इसलिए उन पर सुरक्षा के कड़े नियम लागू होते हैं।**

आपको क्या करना है

- **इसे केवल LAN के लिंक** से ही डाउनलोड और इंस्टॉल करें:

64-bit सिस्टम:

https://172.21.77.106:4343/officescan/download/agent_cloud_x64.msi

32-bit सिस्टम:

https://172.21.77.106:4343/officescan/download/agent_cloud_x86.msi

- स्क्रीन पर दिए गए निर्देशों का पालन करें और इंस्टॉलेशन को बीच में **रद्द न करें**।
- यदि संकेत दिया जाए, तो अपने कंप्यूटर को रीस्टार्ट (पुनः प्रारंभ) करें।

नोट: यदि आप उपरोक्त चरणों को पूरा करने में असमर्थ हैं, तो

1.2 CSK Bot Removal Tool का उपयोग करके पूर्ण सिस्टम स्कैन करें (किसी इंस्टॉलेशन की आवश्यकता नहीं)

यह चरण सुनिश्चित करता है कि छिपे हुए मैलवेयर या बॉट संक्रमण हटा दिए गए हैं।

आपको क्या करना है

- एक ब्राउज़र खोलें और **Cyber Swachhta Kendra (CERT-In की एक पहल)** पर जाएँ:

  https://www.csk.gov.in/security-tools.html

- **अपने सिस्टम के लिए उपयुक्त CSK Bot Removal Tool डाउनलोड करें।**

  https://www.k7computing.com/in/k7-bot-removal-tool अथवा

  https://www.quickheal.co.in/bot-removal-tool

- टूल चलाएँ और **'Full System Scan'** चुनें।
- स्कैन को पूरी तरह से पूर्ण होने दें (इसमें समय लग सकता है)।
- यदि कोई इन्फेक्शन (संक्रमण) पाया जाता है, तो टूल को उन्हें **साफ/हटाने** की अनुमति दें।
- किसी भी थर्ड-पार्टी क्लीनिंग टूल या क्रैक किए गए सॉफ्टवेयर का उपयोग न करें।

<u>महत्वपूर्ण नोट:</u>

1. **ऊपर पॉइंट नंबर 1.2 में बताया गया टूल, एंटीवायरस / EDR समाधानों का विकल्प नहीं है।** सभी उपयोगकर्ताओं को सरकारी डिजिटल संपत्तियों की व्यापक सुरक्षा सुनिश्चित करने के लिए, सेक्शन 1.1 में दिए गए लिंक के माध्यम से उपलब्ध कराए गए,सरकार द्वारा अनुमोदित 'Advanced Antivirus / EDR solution' (Trend Micro Apex One Agent) को अपने महत्वपूर्ण कार्यालय कम्प्यूटर सिस्टम पर बनाए रखना जारी रखना चाहिए।

2. यदि आपके डेस्कटॉप पर किसी अधिकृत चैनल के माध्यम से पहले से ही कोई **असली और पूरी तरह से अपडेटेड एंटीवायरस (AV) समाधान** इंस्टॉल है (**ऊपर पॉइंट 1.1 और 1.2** में बताए गए समाधानों के अलावा), तो यह सुनिश्चित करें कि वह समाधान **नियमित रूप से अपडेट** होता रहे और उसके **सभी सुरक्षा मॉड्यूल चालू (enabled)** हों, ताकि विभिन्न प्रकार के साइबर खतरों से व्यापक सुरक्षा मिल सके।

3. इसके अलावा, यदि आपको कोई SOC सुरक्षा अलर्ट मिलता है, या यदि आपको संदेह है कि आपका सिस्टम किसी तरह से प्रभावित (compromised) या संक्रमित हो गया है, तो तुरंत 'Full System Scan' करें।

1.3 अपने सिस्टम को तुरंत अपडेट करें

बिना पैच वाले सिस्टम सुरक्षा के लिए सबसे बड़ा खतरा होते हैं।

बिना पैच वाले सिस्टम का **मतलब है कि कंप्यूटर** में सुरक्षा से जुड़ी ऐसी ज्ञात कमियाँ (vulnerabilities) मौजूद हैं, जिन्हें अभी तक ठीक नहीं किया गया है। **हैकर्स अक्सर इन कमजोरियों का फायदा उठाकर निम्नलिखित कार्य करते हैं:**

- मालवेयर या रैंसमवेयर इंस्टॉल करना
- सिस्टम तक अनधिकृत पहुँच प्राप्त करना
- संवेदनशील जानकारी चुराना
- पूरे नेटवर्क में इन्फेक्शन फैलाना

- ✓ **सॉफ्टवेयर कंपनियाँ इन कमजोरियों को ठीक करने के लिए नियमित रूप** से सुरक्षा पैच और अपडेट जारी करती हैं।
- ✓ अपडेट इंस्टॉल करने से यह सुनिश्चित होता है कि आपका सिस्टम नए खोजे गए सुरक्षा-संबंधी खतरों से सुरक्षित रहे।
- ✓ Microsoft Windows पर **चलने वाले कंप्यूटरों** के लिए, **ये अपडेट 'Windows Update' के माध्यम से वितरित** किए जाते हैं, **यह Microsoft द्वारा प्रदान की गई एक इन-बिल्ट सेवा है।**

आपको क्या करना है

- **Windows Update** खोलें।
- **सभी पेंडिंग** अपडेट (Security updates) इंस्टॉल करें।
- अपडेट के बाद सिस्टम को रीस्टार्ट करें।

रीस्टार्ट करना क्यों ज़रूरी है

- ✓ **कुछ अपडेट** कोर सिस्टम फ़ाइलों और सिक्योरिटी कंपोनेंट्स में बदलाव करते हैं, **जो सिस्टम के चलते समय** एक्टिव रहते हैं। रीस्टार्ट करने से सिस्टम को ये फ़ायदे होते हैं:
  - अपडेट पूरी तरह से लागू हो जाते हैं
  - पुरानी सिस्टम फ़ाइलें पैच किए गए वर्शन से बदल जाती हैं
  - **नई सिक्योरिटी सुरक्षाएँ एक्टिव हो जाती हैं**
  - **रीस्टार्ट किए बिना, कुछ अपडेट लागू नहीं हो पाते, जिससे सिस्टम कुछ हद तक असुरक्षित रह जाता है।**

नियमित सिस्टम अपडेट के फ़ायदे

सिस्टम को नियमित रूप से अपडेट करने के कई फ़ायदे हैं:

1. नई खोजी गई साइबर कमज़ोरियों से सुरक्षा मिलती है
2. सिस्टम की स्थिरता और परफ़ॉर्मेंस बेहतर होती है
3. नए एप्लिकेशन और हार्डवेयर के साथ कम्पैटिबिलिटी पक्की होती है
4. नेटवर्क की कुल मिलाकर साइबर सिक्योरिटी मज़बूत होती है

सरकारी या ऑफ़िस सिस्टम के लिए, समय पर अपडेट बहुत ज़रूरी हैं, क्योंकि वे संवेदनशील डिजिटल संपत्तियों की सुरक्षा करने और साइबर घटनाओं को रोकने में मदद करते हैं।

नोट: Trend Micro Apex Agent (जो LAN End Points पर डिप्लॉय किया गया है) को अनइंस्टॉल करने का काम केवल संबंधित डिपार्टमेंट के CISO/Dy. CISO या वहाँ तैनात सबसे सीनियर DoIT/NIC अधिकारी से मंज़ूरी मिलने के बाद ही किया जा सकता है, और वह भी केवल सही और उचित कारणों से।

ऐसे मामलों में, कृपया LAN IP को **fms.soc@rajasthan.gov.in** और **seclanfms@rajasthan.gov.in** पर शेयर करें, ताकि अनइंस्टॉलेशन की प्रक्रिया शुरू की जा सके।

हालाँकि, ऐसा करने की सलाह केवल बहुत ज़रूरी हालात में ही दी जाती है, जब कोई वैध ऑफ़िशियल एप्लिकेशन, इस एडवांस्ड एंटीवायरस सुरक्षा की वजह से ठीक से काम नहीं कर पा रहा हो ।

अनुभाग 2: डेस्कटॉप हार्डनिंग और सिस्टम सुरक्षा (अनिवार्य दैनिक अभ्यास)

डेस्कटॉप हार्डनिंग का मतलब है अपने कंप्यूटर को सुरक्षित करना, ताकि अगर कोई उस पर हमला करने की कोशिश भी करे, तो भी उसका गलत इस्तेमाल न किया जा सके। इसका मतलब है **डेस्कटॉप कंप्यूटर की सुरक्षा को मज़बूत करने की प्रक्रिया, जिसमें कमज़ोरियों को कम किया जाता है और हमले के संभावित बिंदुओं को सीमित किया जाता है।** इसका लक्ष्य सिस्टम को इतना सुरक्षित बनाना है कि **उसका आसानी से गलत इस्तेमाल न हो सके, बिना अनुमति के उस तक पहुँचा न जा सके, या साइबर हमलावर उसे नुकसान न पहुँचा सकें।**

आसान शब्दों में, इसका मतलब है **कंप्यूटर को पूरी तरह से सुरक्षित (लॉक डाउन) करना, ताकि उसका गलत इस्तेमाल या साइबर हमले न हो सकें।**

डेस्कटॉप हार्डनिंग के उद्देश्य

मुख्य उद्देश्य ये हैं:

- कंप्यूटर पर स्टोर किए गए **संवेदनशील डेटा की सुरक्षा** करना।
- सिस्टम तक **बिना अनुमति के पहुँच** को रोकना।
- **सिस्टम की उन कमज़ोरियों** को कम करना, जिनका फ़ायदा हमलावर उठा सकते हैं।
- **मालवेयर संक्रमणों,** जैसे वायरस या रैंसमवेयर को रोकना।
- **सिस्टम की विश्वसनीयता बनाए रखना।**

2.1 केवल Original/Genuine और स्वीकृत सॉफ़्टवेयर का उपयोग करें

- सुनिश्चित करें कि आपके सिस्टम पर **Original/Genuine ऑपरेटिंग सिस्टम** चल रहा हो।
- **केवल ऑफ़िस से संबंधित सॉफ़्टवेयर** ही इंस्टॉल करें।
- यदि आधिकारिक काम के लिए किसी सॉफ़्टवेयर की आवश्यकता है, तो **उसे केवल किसी भरोसेमंद स्रोत (repository) से ही डाउनलोड करें।**
- कभी भी अनौपचारिक, अविश्वसनीय, या बिना अनुमति वाले स्रोतों से एप्लिकेशन या सॉफ़्टवेयर इंस्टॉल न करें।
- **इन्हें इंस्टॉल या उपयोग न करें**:
    - क्रैक किया हुआ या पायरेटेड सॉफ़्टवेयर।
    - अज्ञात वेबसाइटों से मिलने वाले मुफ़्त टूल।
    - टॉरेंट, VPN, एनोनिमाइज़र, या स्क्रीन-शेयरिंग टूल।

2.2 केवल एक सामान्य उपयोगकर्ता (Normal User) के रूप में काम करें

- **दैनिक कार्यों के लिए Administrator खाते का उपयोग न करें।**
- Administrator पहुँच (access) केवल विशिष्ट कार्यों के लिए होती है। सुनिश्चित करें कि सिस्टम पर सॉफ़्टवेयर इंस्टॉल करने या उसमें बदलाव करने के लिए Administrator क्रेडेंशियल की आवश्यकता हो।
- Guest उपयोगकर्ता खाता **हमेशा बंद (disabled)** रहना चाहिए।

2.3 सिस्टम फ़ायरवॉल हमेशा चालू रखें

फ़ायरवॉल कंप्यूटर और बाहरी नेटवर्क, जैसे इंटरनेट के बीच एक सुरक्षा कवच (barrier) का काम करता है। यह सिस्टम में आने वाले या बाहर जाने वाले डेटा पैकेट की जाँच करता है और किसी भी संदिग्ध या बिना अनुमति वाले कनेक्शन को रोक देता है।

Microsoft Windows पर चलने वाले ज़्यादातर कंप्यूटरों में एक इन-बिल्ट फ़ायरवॉल होता है, जिसे Windows Defender Firewall कहा जाता है।

- **Windows Firewall हमेशा चालू (ON)** रहना चाहिए।
- स्पीड बढ़ाने, सॉफ़्टवेयर इंस्टॉल करने, या किसी समस्या को ठीक करने (troubleshooting) के लिए फ़ायरवॉल को बंद न करें।
- यदि कोई **सॉफ़्टवेयर फ़ायरवॉल बंद** करने के लिए कहता है, तो **'Cancel'** (रद्द करें) चुनें।

2.4. BIOS और Firmware सुरक्षा

BIOS/UEFI सुरक्षा **डेस्कटॉप हार्डनिंग** का एक महत्वपूर्ण हिस्सा है, क्योंकि यह **ऑपरेटिंग सिस्टम शुरू होने से पहले ही हार्डवेयर स्तर पर कंप्यूटर** की सुरक्षा करता है।

- यह पक्का करें कि BIOS/UEFI पासवर्ड चालू हो, ताकि कोई बिना इजाज़त के बूट न कर सके। **(पासवर्ड याद रखें, क्योंकि अगर आप इसे भूल गए, तो आपको OS फिर से इंस्टॉल करना पड़ सकता है)**

चूंकि BIOS/UEFI बूट प्रोसेस को कंट्रोल करता है, इसलिए जो हमलावर इस तक पहुंच बना लेते हैं, वे ये काम कर सकते हैं:

1. बूट सेटिंग्स बदल सकते हैं
2. सिस्टम को बाहरी डिवाइस (USB/DVD) से बूट कर सकते हैं
3. ऑपरेटिंग सिस्टम की सुरक्षा को तोड़ सकते हैं
4. खतरनाक सॉफ्टवेयर इंस्टॉल कर सकते हैं

2.5 सिस्टम की गैर-ज़रूरी सुविधाएं बंद करें

- रिमोट डेस्कटॉप (RDP) - **बंद रखें**
- ब्लूटूथ, NFC - **बंद रखें, जब तक कि आधिकारिक तौर पर ज़रूरत न हो**
- Wi-Fi / हॉटस्पॉट - **सिर्फ़ अनुमोदित Wi-Fi नेटवर्क का इस्तेमाल करें**

ऑफिस के कंप्यूटर को इनसे न जोड़ें:

- निजी मोबाइल हॉटस्पॉट
- स्मार्ट TV
- घर के IoT डिवाइस

2.6 अपने डेस्कटॉप को भौतिक रूप से सुरक्षित करें

डेस्कटॉप कंप्यूटर की भौतिक सुरक्षा उतनी ही ज़रूरी है जितनी कि डिजिटल सुरक्षा। भले ही किसी सिस्टम में मज़बूत पासवर्ड, एंटीवायरस और फ़ायरवॉल सुरक्षा हो, फिर भी **अगर कोई कंप्यूटर तक भौतिक रूप से पहुंच बना** ले, तो उसका गलत इस्तेमाल किया जा सकता है। इसलिए, उपयोगकर्ताओं को बिना इजाज़त के इस्तेमाल को रोकने के लिए कुछ तरीकों का पालन करना चाहिए।

2.6.1. अपनी डेस्क छोड़ते समय कंप्यूटर लॉक करें

जब भी आप अपनी वर्कस्टेशन छोड़ें, भले ही थोड़े समय के लिए ही क्यों न हो, आपको अपनी **कंप्यूटर स्क्रीन लॉक कर देनी** चाहिए।

Microsoft Windows पर चलने वाले कंप्यूटर पर आप Windows + L दबाकर सिस्टम को जल्दी से लॉक कर सकते हैं।

कंप्यूटर लॉक करने से यह पक्का होता है कि:

- कोई भी आपकी फ़ाइलों या एप्लिकेशन तक पहुंच न बना सके।
- आपका ईमेल या आधिकारिक दस्तावेज़ सुरक्षित रहें।
- आपके नाम पर कोई भी बिना इजाज़त के काम न कर सके।

जब सिस्टम लॉक होता है, तो उसे फिर से इस्तेमाल करने के लिए आपके **लॉगिन पासवर्ड** की ज़रूरत होती है।

2.6.2. दिन के आखिर में सिस्टम बंद करें

कामकाज के दिन के आखिर में, उपयोगकर्ताओं को कंप्यूटर को चालू छोड़ने के बजाय उसे ठीक से बंद कर देना चाहिए।

सिस्टम बंद करने से इन कामों में मदद मिलती है:

- ऑफिस बंद होने पर बिना इजाज़त के इस्तेमाल को रोकना।
- मालवेयर या रिमोट हमलों का खतरा कम करना।
- बिजली बचाना और सिस्टम की परफ़ॉर्मेंस बेहतर करना।

अगले दिन सिस्टम को फिर से चालू करने से सिस्टम को अपडेट और सुरक्षा सेटिंग्स ठीक से लोड करने में भी मदद मिलती है।

2.6.3. किसी और को अपने लॉग-इन किए हुए सिस्टम का इस्तेमाल न करने दें

जब आप लॉग-इन हों, तो आपको कभी भी किसी दूसरे व्यक्ति को अपने कंप्यूटर का इस्तेमाल करने की अनुमति नहीं देनी चाहिए।

इसके कारण ये हैं:

- **सिस्टम पर किए गए काम आपके यूज़र अकाउंट के तहत रिकॉर्ड होंगे।**
- संवेदनशील जानकारी तक पहुँच बनाई जा सकती है या उसे कॉपी किया जा सकता है।
- आपकी जानकारी के बिना कोई अनधिकृत सॉफ़्टवेयर इंस्टॉल किया जा सकता है।

यदि किसी को कंप्यूटर का इस्तेमाल करने की ज़रूरत है, तो **उन्हें अपने खुद के अधिकृत अकाउंट का इस्तेमाल करके लॉग-इन** करना चाहिए।

अनुभाग 3: ईमेल सुरक्षा (हमलों का सबसे आम ज़रिया)

ईमेल, दफ़्तरों और संगठनों में इस्तेमाल होने वाले संचार के सबसे ज़्यादा इस्तेमाल किए जाने वाले साधनों में से एक है। हालाँकि, यह साइबर हमलावरों द्वारा साइबर हमले शुरू करने के लिए इस्तेमाल किया जाने वाला सबसे आम तरीका भी है। क्योंकि कर्मचारियों को अक्सर बाहरी स्रोतों से ईमेल मिलते रहते हैं, इसलिए हमलावर अक्सर इस माध्यम का फ़ायदा उठाकर सिस्टम और संवेदनशील जानकारी तक बिना अनुमति के पहुँच बनाने की कोशिश करते हैं।

साइबर अपराधी ईमेल का इस्तेमाल करके कई तरह के ख़तरे पहुँचाते हैं, क्योंकि ऐसे नुकसान पहुँचाने वाले संदेश भेजना आसान होता है जो देखने में असली लगते हैं। **कई हमले, उपयोगकर्ताओं को धोखा देकर नुकसान पहुँचाने वाले लिंक पर क्लिक करवाने या संक्रमित अटैचमेंट खोलने पर निर्भर करते हैं।**

ईमेल सुरक्षा बहुत ज़रूरी है, क्योंकि ईमेल ही साइबर हमलों के लिए प्रवेश का सबसे आम ज़रिया है**। हमलावर सिस्टम को नुकसान पहुँचाने के लिए फ़िशिंग, नुकसान पहुँचाने वाले लिंक और संक्रमित अटैचमेंट का इस्तेमाल करते हैं।** ईमेल सुरक्षा के सही तरीकों का पालन करने से व्यक्तिगत सिस्टम और संगठन के डिजिटल बुनियादी ढाँचे, दोनों को सुरक्षित रखने में मदद मिलती है।

ईमेल के ज़रिए पहुँचाए जाने वाले आम ख़तरों में शामिल हैं:

- फ़िशिंग ईमेल, जो पासवर्ड या गोपनीय जानकारी चुराने की कोशिश करते हैं।
- मालवेयर अटैचमेंट, जो खोलने पर सिस्टम को संक्रमित कर देते हैं।
- रैंसमवेयर लिंक, जो नुकसान पहुँचाने वाला सॉफ़्टवेयर डाउनलोड कर लेते हैं।
- नकली संदेश, जो अधिकारियों या सरकारी संस्थाओं का स्वरूप अपनाकर सामने आते हैं।

ईमेल सुरक्षा का महत्व:

ईमेल सुरक्षा के मज़बूत तरीके इन कामों में मदद करते हैं:

- संगठन के संवेदनशील डेटा को **सुरक्षित** रखना।
- मालवेयर संक्रमण को **रोकना**।
- सिस्टम तक बिना **अनुमति के पहुँच** को रोकना।
- पैसे या डेटा के नुकसान के **जोखिम को कम** करना।

3.1 केवल आधिकारिक सरकारी ईमेल का इस्तेमाल करें

- केवल अपनी आधिकारिक ईमेल ID का इस्तेमाल करें (**जो rajasthan.gov.in/rajpolice.gov.in...**आदि पर खत्म होती हो)।
- आधिकारिक दस्तावेज़ों को कभी भी इन जगहों पर फ़ॉरवर्ड न करें:
    - निजी क्लाउड खाते।

आधिकारिक **ईमेल ID को इन जगहों पर रजिस्टर न** करें:

- सोशल मीडिया
- ई-कॉमर्स पोर्टल
- थर्ड पार्टी टूल या वेबसाइटें

3.2 फ़िशिंग ईमेल की पहचान करें

अगर कोई ईमेल ऐसा हो, तो सावधान रहें:

- जो पासवर्ड, OTP या पैसे की माँग करता हो
- जो जल्दबाज़ी करने को कहता हो ("खाता बंद कर दिया जाएगा")
- जिसमें **ग्रामर की ग़लतियाँ** हों या भेजने वाले का पता अजीब हो
- जिसमें कोई अनजान अटैचमेंट या छोटा किया हुआ लिंक हो

ज़रूरी: क्लिक न करें। जवाब न दें। तुरंत fms.soc@rajasthan.gov.in पर रिपोर्ट करें।

3.3. URL और डोमेन का सत्यापन:

क्लिक करने से पहले, खासकर ईमेल और संदेशों में, डोमेन नाम, URL और ईमेल अटैचमेंट को ध्यान से जाँचने की आदत डालें। (आप सार्वजनिक रूप से उपलब्ध Threat Intel संसाधनों, जैसे VirusTotal आदि का संदर्भ ले सकते हैं।)

URL और Domain Verification का मतलब है कि **वेबसाइट का पता (URL), डोमेन नाम, या ईमेल/संदेशों** में दिए गए लिंक पर क्लिक करने से पहले उन्हें ध्यान से जाँचें। **फ़िशिंग, मैलवेयर फैलाना और क्रेडेंशियल चोरी** जैसे कई साइबर हमले, यूज़र्स को नकली या नुकसान पहुँचाने वाले लिंक पर क्लिक करने के लिए धोखा देने पर निर्भर करते हैं। **इन चीज़ों को जाँचने की आदत डालने से कई सुरक्षा घटनाओं को रोका जा सकता है।**

1. डोमेन नाम को ध्यान से जाँचें
2. क्लिक करने से पहले लिंक पर माउस ले जाएँ (Hover करें)
3. पूरे URL Structure को Verify करें
4. Threat Intelligence Tools (**जैसे VirusTotal आदि का संदर्भ ले सकते हैं**) का इस्तेमाल करें
5. ईमेल Attachments के मामले में सावधान रहें
6. HTTPS देखें, लेकिन उस पर पूरी तरह भरोसा न करें

3.4 सुरक्षित ईमेल के तरीके

सुरक्षित ईमेल के तरीके फ़िशिंग हमलों, अकाउंट के Compromise होने और मैलवेयर संक्रमण के जोखिम को कम करने में मदद करते हैं। ईमेल का इस्तेमाल करते समय कुछ अनुशासित तरीकों का पालन करने से व्यक्तिगत और संगठनात्मक साइबर सुरक्षा में काफ़ी सुधार हो सकता है।

3.4.1. Browser में "Save Password" को Disable करें

कई Browser ईमेल लॉगिन पासवर्ड को अपने आप Save करने का विकल्प देते हैं। यह सुविधाजनक तो है, लेकिन इसमें जोखिम भी हो सकता है।

यह जोखिम भरा क्यों है:

- जिस किसी के पास भी आपके डिवाइस का एक्सेस है, वह आपका ईमेल अकाउंट खोल सकता है।
- **मैलवेयर या Browser की कमज़ोरियाँ Save किए गए क्रेडेंशियल निकाल सकती हैं।**
- Shared या Office के कंप्यूटर पर Unauthorized Access का जोखिम बढ़ जाता है।

सबसे अच्छा तरीका:

- **Browser में ईमेल पासवर्ड Save करने से बचें।**
- किसी भरोसेमंद Password Manager का इस्तेमाल करें।
- **ईमेल अकाउंट के लिए हमेशा Multi-Factor Authentication (MFA) चालू रखें।**

3.4.2. Attachments को अपने आप Download न होने दें

कुछ ईमेल एप्लिकेशन, जब कोई ईमेल खोला जाता है, तो Attachments को अपने आप Download कर लेते हैं। इससे सिस्टम मैलवेयर या नुकसान पहुँचाने वाली Scripts के संपर्क में आ सकता है।

Attachments के अपने आप Download होने के जोखिम:

- **Documents या Archives के अंदर छिपा मैलवेयर अपने आप Download हो सकता है।**
- हमलावर अक्सर नुकसान पहुँचाने वाली फ़ाइलों को Invoices, Reports या Delivery Notices के रूप में छिपाकर भेजते हैं।
- कुछ फ़ाइलें Download होते ही तुरंत सिस्टम की कमज़ोरियों का फ़ायदा उठा सकती हैं।

सबसे अच्छा तरीका:

- **अपने ईमेल Settings में Attachments को अपने आप Download होने से रोकें (Disable करें)।**
- केवल भरोसेमंद और Verify किए गए भेजने वालों से ही Attachments Download करें।
- संदिग्ध फ़ाइलों को Tools का इस्तेमाल करके Scan करें।

3.4.3. ईमेल केवल तभी Forward करें जब ज़रूरी हो और पूरी बातचीत (Trail) को सुरक्षित रखें

ईमेल को बिना किसी ज़रूरत के **Forward** करने से संवेदनशील जानकारी, अंदरूनी बातचीत और संपर्क विवरण (Contact Details) सबके सामने आ सकते हैं।

लापरवाही से फ़ॉरवर्ड करने के जोखिम:

- गोपनीय जानकारी ऐसे लोगों तक पहुँच सकती है जिनके लिए वह नहीं थी।
- हमलावर सोशल इंजीनियरिंग हमलों के लिए ईमेल चेन से जानकारी इकट्ठा कर सकते हैं।
- ईमेल के कुछ हिस्सों को हटाने से गलतफ़हमी हो सकती है या संदर्भ खो सकता है।

सबसे अच्छा तरीका:

- ईमेल तभी फ़ॉरवर्ड करें **जब काम या बातचीत के लिए ज़रूरी** हो।
- **पूरा ईमेल थ्रेड (ट्रेल)** बनाए रखें, ताकि पाने वाले को संदर्भ समझ में आ जाए।
- अगर कोई संवेदनशील जानकारी पाने वाले के लिए प्रासंगिक नहीं है, तो उसे हटा दें।

अनुभाग 4: इंटरनेट और ब्राउज़र सुरक्षा

वेब ब्राउज़र बहुत सारी जानकारी स्टोर करते हैं, जैसे लॉगिन सेशन, कुकीज़ और ब्राउज़िंग डेटा। अगर इन सेटिंग्स को सुरक्षित तरीके से कॉन्फ़िगर नहीं किया जाता है, तो हमलावर इनका फ़ायदा उठाकर **क्रेडेंशियल चुरा सकते हैं, यूज़र की गतिविधि को ट्रैक कर सकते हैं, या खातों तक बिना अनुमति** के पहुँच बना सकते हैं। सुरक्षित ब्राउज़र सेटिंग्स कॉन्फ़िगर करने से व्यक्तिगत और संगठनात्मक डेटा को सुरक्षित रखने में मदद मिलती है।

4.1 सुरक्षित ब्राउज़र सेटिंग्स का उपयोग करें

सुनिश्चित करें:

- **'Enhanced Security Mode'** (बेहतर सुरक्षा मोड) चालू है।
- ज़्यादातर आधुनिक ब्राउज़र एक इन-बिल्ट बेहतर सुरक्षा या प्रोटेक्शन मोड देते हैं, जो नुकसान पहुँचाने वाली वेबसाइटों और डाउनलोड से सुरक्षा को बेहतर बनाता है।
- ब्राउज़र बंद होने पर, यह अपने आप साफ़ कर देता है:
    - कुकीज़
    - Cache (कैश)
    - ब्राउज़िंग इतिहास
    - स्टोर किए गए पासवर्ड

'Enhanced Security Mode' चालू करने के फ़ायदे:

- **फ़िशिंग वेबसाइटों का पता लगाता है और उन्हें ब्लॉक करता है**
- **खतरनाक या संदिग्ध साइटों पर जाने से पहले यूज़र्स को चेतावनी देता है**
- नुकसान पहुँचाने वाले डाउनलोड के ख़िलाफ़ मज़बूत सुरक्षा प्रदान करता है
- **हानिकारक URL की पहचान करने के लिए 'Real-time Security Checks' (रीयल-टाइम सुरक्षा जाँच) का उपयोग करता है**

4.2 इंटरनेट उपयोग के नियम

संगठनात्मक सुरक्षा, उत्पादकता और साइबर खतरों से सुरक्षा बनाए रखने के लिए इंटरनेट के ज़िम्मेदार उपयोग के तरीकों का पालन करना महत्वपूर्ण है।

कई वेबसाइटें जो पायरेटेड सामग्री या मुफ़्त डाउनलोड प्रदान करती हैं, उनका उपयोग अक्सर हमलावरों द्वारा मैलवेयर, स्पाइवेयर और फ़िशिंग लिंक फैलाने के लिए किया जाता है।

इसलिए, कर्मचारियों को अपनी ब्राउज़िंग केवल काम से संबंधित और विश्वसनीय वेबसाइटों तक ही सीमित रखनी चाहिए।

इन पर न जाएँ:

- **Torrent sites (टॉरेंट साइटें):**टॉरेंट वेबसाइटें यूज़र्स को *Peer-to-peer sharing* (पीयर-टू-पीयर शेयरिंग) के माध्यम से फ़ाइलें डाउनलोड करने की अनुमति देती हैं। हालाँकि कुछ टॉरेंट में वैध सामग्री हो सकती है, लेकिन कई का उपयोग पायरेटेड सॉफ़्टवेयर, फ़िल्में या गेम वितरित करने के लिए किया जाता है।

- **Streaming sites (स्ट्रीमिंग साइटें):**बिना पुष्टि वाली स्ट्रीमिंग वेबसाइटें, जो मुफ़्त फ़िल्में, टीवी शो या खेल प्रसारण प्रदान करती हैं, अक्सर अवैध रूप से संचालित होती हैं और उनमें हानिकारक सामग्री हो सकती है।

- **Free movie / software & crack sites (मुफ़्त वीडियो / सॉफ़्टवेयर और क्रैकसाइटें):**ऐसी वेबसाइटें, जो मुफ़्त प्रीमियम सॉफ़्टवेयर, क्रैक या पायरेटेड एप्लिकेशन प्रदान करती हैं, साइबर खतरों का एक आम स्रोत होती हैं।

केवल **काम से संबंधित वेबसाइटों** का ही उपयोग करें।

4.3 सार्वजनिक Wi-Fi से बचें

सार्वजनिक Wi-Fi नेटवर्क अक्सर असुरक्षित या कम सुरक्षित होते हैं, जिससे वे साइबर हमलावरों के लिए एक आसान निशाना बन जाते हैं। जब यूज़र्स ऐसे नेटवर्क से जुड़ते हैं, तो संवेदनशील डेटा, जैसे लॉगिन क्रेडेंशियल, आधिकारिक दस्तावेज़ या सेशन की जानकारी को बीच में ही पकड़ा जा सकता है। इसलिए, सरकारी प्रणालियों और महत्वपूर्ण आधिकारिक पोर्टलों तक सार्वजनिक या खुले Wi-Fi नेटवर्क से कभी भी पहुँच नहीं बनाई जानी चाहिए।

सरकारी सिस्टम और ज़रूरी सरकारी पोर्टल्स को कभी भी इन जगहों से एक्सेस न करें:

- **रेलवे Wi-Fi** - रेलवे स्टेशनों पर मिलने वाली मुफ़्त Wi-Fi सेवाएँ ओपन नेटवर्क होती हैं, जिनका इस्तेमाल बड़ी संख्या मेंलोग करते हैं।
- **कैफ़े Wi-Fi -** कैफ़े या रेस्टोरेंट में मिलने वाला पब्लिक Wi-Fi आम तौर पर कई अनजान यूज़र्स के साथ शेयर होता है
- **एयरपोर्ट पब्लिक नेटवर्क** - एयरपोर्ट आम तौर पर यात्रियों को मुफ़्त इंटरनेट की सुविधा देते हैं, लेकिन ज़्यादा यूज़र्स होने की वजह से साइबर अपराधी अक्सर इन नेटवर्क्स को निशाना बनाते हैं।

4.4 सोशल मीडिया और मैसेजिंग प्लेटफ़ॉर्म

- **सोशल मीडिया या गैर-सरकारी प्लेटफ़ॉर्म पर रजिस्टर करने के लिए अपनी ऑफ़िशियल ईमेल ID का इस्तेमाल न करें।**
- सोशल मीडिया पर ऑफ़िशियल जानकारी, फ़ोटो, स्क्रीनशॉट या दस्तावेज़ शेयर न करें।
- मैसेजिंग प्लेटफ़ॉर्म पर मिले लिंक्स पर क्लिक करने या फ़ाइलें डाउनलोड करने से बचें।
- **प्राइवेसी सेटिंग्स को सबसे ऊँचे लेवल पर रखें और अपनी प्रोफ़ाइल को पब्लिक के लिए विज़िबल न रखें।**

4.5. संवेदनशील एक्सेस के लिए सुरक्षित ब्राउज़र का इस्तेमाल

सरकारी एप्लीकेशन्स, ऑफ़िशियल ईमेल सेवाओं या अन्य संवेदनशील ऑनलाइन पोर्टल्स को एक्सेस करते समय, सुरक्षित ब्राउज़िंग तरीकों का इस्तेमाल करना ज़रूरी है। एक सुझाया गया तरीका यह है कि ज़्यादातर आधुनिक ब्राउज़र्स में उपलब्ध 'प्राइवेट' या 'इनकॉग्निटो' ब्राउज़िंग मोड का इस्तेमाल किया जाए।

उदाहरण के लिए, Google Chrome, Mozilla Firefox और Microsoft Edge जैसे ब्राउज़र्स में **'प्राइवेट/इनकॉग्निटो' मोड** होता है, जो डिवाइस पर स्टोर होने वाले ब्राउज़िंग डेटा की मात्रा को कम करने में मदद करता है।

'प्राइवेट' या 'इनकॉग्निटो' मोड ब्राउज़र का एक ऐसा फ़ीचर है, जो यूज़र्स को अपनी ब्राउज़िंग एक्टिविटी को लोकल डिवाइस पर सेव किए बिना इंटरनेट ब्राउज़ करने की सुविधा देता है। जैसे ही ब्राउज़िंग सेशन खत्म होता है, उस सेशन के दौरान बना ज़्यादातर टेम्पररी डेटा अपने आप डिलीट हो जाता है।

4.6. ब्राउज़र एक्सटेंशन्स और टूलबार कंट्रोल

ब्राउज़र एक्सटेंशन्स, टूलबार और ऐड-ऑन्स ब्राउज़र की कार्यक्षमता को बढ़ा सकते हैं, लेकिन अगर उन्हें किसी **अविश्वसनीय सोर्स से इंस्टॉल** किया जाए, तो वे सुरक्षा से जुड़े गंभीर खतरे भी पैदा कर सकते हैं।

कई नुकसान पहुँचाने वाले **एक्सटेंशन्स यूज़र का डेटा इकट्ठा करने, ब्राउज़िंग एक्टिविटी पर नज़र रखने, विज्ञापन दिखाने या लॉगिन क्रेडेंशियल्स चुराने** के लिए डिज़ाइन किए जाते हैं।

इसलिए, **यूज़र्स को किसी भी थर्ड-पार्टी ब्राउज़र टूलबार, डाउनलोड मैनेजर या ऐड-ऑन्स को तब तक इंस्टॉल नहीं करना चाहिए, जब तक कि उन्हें संगठन की IT या सुरक्षा टीम** से साफ़ तौर पर मंज़ूरी न मिल गई हो।

4.6.1. बिना मंज़ूरी वाले ब्राउज़र एक्सटेंशन्स के खतरे

बिना वेरिफ़िकेशन वाले ब्राउज़र एक्सटेंशन्स में छिपा हुआ नुकसान पहुँचाने वाला कोड हो सकता है।

4.6.2. ब्राउज़र टूलबार के खतरे

थर्ड-पार्टी ब्राउज़र टूलबार अक्सर ब्राउज़र के अंदर बहुत **ज़्यादा अनुमतियों (permissions)** की माँग करते हैं।

4.6.3. डाउनलोड मैनेजर और ऐड-ऑन के जोखिम

ऑनलाइन उपलब्ध कई डाउनलोड मैनेजर और ऐड-ऑन के साथ एडवेयर या स्पाइवेयर भी जुड़े होते हैं।

अनुभाग 5: पासवर्ड और एक्सेस प्रबंधन

5.1 मज़बूत पासवर्ड बनाएँ

पासवर्ड, उपयोगकर्ता खातों, सरकारी प्रणालियों और संवेदनशील डेटा की सुरक्षा के लिए रक्षा की पहली पंक्ति होते हैं। कमज़ोर या आसानी से अंदाज़ा लगाए जा सकने वाले पासवर्ड, हमलावरों के लिए ब्रूट-फ़ोर्स हमलों, पासवर्ड का अंदाज़ा लगाने, या क्रेडेंशियल स्टफ़िंग जैसे तरीकों से अनधिकृत पहुँच प्राप्त करना आसान बना देते हैं। इसलिए, उपयोगकर्ताओं को हमेशा मज़बूत और सुरक्षित पासवर्ड बनाने चाहिए।

आपका पासवर्ड ऐसा होना चाहिए जिसमें:

- कम से कम **8 अक्षर हों**
- शामिल हों:
    - बड़े अक्षर (Capital letters)
    - छोटे अक्षर (Small letters)
    - संख्याएँ
    - विशेष अक्षर (Special characters)

इनका उपयोग न करें:

- नाम, जन्म तिथि (DOB), मोबाइल नंबर
- कई प्रणालियों के लिए एक ही पासवर्ड
- **नेटवर्क प्रणालियों और अनुप्रयोगों के लिए नियमित रूप से पासवर्ड बदलते रहें और कई खातों में एक ही पासवर्ड का दोबारा उपयोग करने से सख्ती से बचें।**
- **कई वेबसाइटों या प्रणालियों में एक ही पासवर्ड का उपयोग करने से जोखिम बढ़ जाता है। यदि कोई एक खाता खतरे में पड़ जाता है, तो हमलावर उसी पासवर्ड का उपयोग करके अन्य सेवाओं या आधिकारिक पोर्टलों तक पहुँचने का प्रयास कर सकते हैं।**
- प्रत्येक महत्वपूर्ण खाते का एक अद्वितीय **(unique) पासवर्ड** होना चाहिए।

5.2 मल्टी-फ़ैक्टर आथेंटिकेशन (MFA) सक्षम करें

मल्टी-फ़ैक्टर आथेंटिकेशन (MFA), पहुँच प्रदान करने से पहले सत्यापन के एक से अधिक तरीकों की आवश्यकता द्वारा उपयोगकर्ता खातों में सुरक्षा की एक अतिरिक्त परत जोड़ता है।

यदि पासवर्ड किसी अन्य व्यक्ति को मिल भी जाए तो , MFA अनधिकृत उपयोगकर्ता को खाते तक पहुँचने से रोकने में मदद करता है।

इसलिए, जहाँ भी MFA उपलब्ध हो, उसे हमेशा सक्षम किया जाना चाहिए - विशेष रूप से सरकारी प्रणालियों, आधिकारिक ईमेल खातों और संवेदनशील पोर्टलों के लिए।

- **जहाँ भी उपलब्ध हो, हमेशा MFA सक्षम करें।**
- **किसी के साथ भी OTP साझा न करें।**
- कई प्लेटफ़ॉर्म MFA का समर्थन करते हैं, जिनमें Google Authenticator और Microsoft Authenticator जैसी सेवाएँ शामिल हैं, जो सुरक्षित, एक-बार उपयोग होने वाले सत्यापन कोड उत्पन्न करती हैं।
- साइबर अपराधी अक्सर फ़िशिंग ईमेल, नकली कॉल या धोखाधड़ी वाले संदेशों के माध्यम से उपयोगकर्ताओं को धोखा देकर OTP बताने के लिए प्रेरित करने का प्रयास करते हैं।
- हमलावर तकनीकी सहायता कर्मचारियों, बैंक अधिकारियों, या सिस्टम प्रशासकों होने का दिखावा कर सकते हैं और सत्यापन के लिए OTP का अनुरोध कर सकते हैं।

5.3. पासवर्ड प्रबंधन में अनुशासन

पासवर्ड और अन्य संवेदनशील जानकारी के प्रबंधन में उचित **अनुशासन बनाए रखना, संगठनात्मक प्रणालियों, नेटवर्कों और गोपनीय डेटा** की सुरक्षा के लिए अनिवार्य है। पासवर्ड या सिस्टम विवरण को दिखाई देने वाली जगहों पर लिखकर रखने से वे अनधिकृत व्यक्तियों की नज़र में आ सकते हैं, **जिससे सुरक्षा उल्लंघनों या अनधिकृत पहुँच का जोखिम** काफी बढ़ जाता है।

- **पासवर्ड, IP पते, या संवेदनशील जानकारी को कागज़, चिपकाने वाले नोट (sticky notes), या दिखाई देने वाली सतहों पर न लिखें।**
- क्रेडेंशियल्स को सुरक्षित रखने के लिए सुरक्षित तरीकों का उपयोग करें।
- अपनी डेस्क को साफ-सुथरा रखने की आदत बनाए रखें।

अनुभाग 6: USB, फ़ाइलें और डेटा हैंडलिंग

6.1 बाहरी डिवाइस

USB ड्राइव, बाहरी हार्ड डिस्क और अन्य रिमूवेबल मीडिया जैसे बाहरी स्टोरेज डिवाइस डेटा ट्रांसफर करने के लिए सुविधाजनक हो सकते हैं, लेकिन इनसे साइबर सुरक्षा के भी बड़े जोखिम होते हैं। इन डिवाइस में मैलवेयर, वायरस या अनधिकृत सॉफ़्टवेयर हो सकते हैं, जो ऑफ़िस के सिस्टम और नेटवर्क को नुकसान पहुँचा सकते हैं। इसलिए, काम की जगह पर बाहरी स्टोरेज डिवाइस का इस्तेमाल करते समय कड़ी सावधानियों का पालन करना ज़रूरी है।

- काम की जगह पर निजी USB और हार्ड डिस्क का इस्तेमाल नहीं करना चाहिए।
- बाहरी डिवाइस का इस्तेमाल केवल ठीक से सैनिटाइज़ करने के बाद ही करें।
- **रिमूवेबल मीडिया के लिए ऑटोरन (autoruns) को बंद कर दें।**
- कभी भी प्रमोशनल या अनजान USB डिवाइस का इस्तेमाल न करें।
- **ऑफिस के कंप्यूटरों में कभी भी सीधे कोई USB स्टोरेज डिवाइस न लगाएं, क्योंकि अनजान USBs में मैलवेयर हो सकता है। ऐसी स्टोरेज को खोलने और उसके अंदर की फ़ाइलों का इस्तेमाल करने से पहले, उन्हें पहले स्कैन करें।**

6.2 फ़ाइल सुरक्षा

- **संवेदनशील फ़ाइलों को पासवर्ड से सुरक्षित रखें और उन्हें कंप्रेस्ड फ़ॉर्मेट में रखें:**

  महत्वपूर्ण या गोपनीय फ़ाइलों को अनधिकृत पहुँच से बचाने के लिए उन्हें मज़बूत पासवर्ड से सुरक्षित किया जाना चाहिए। ZIP या RAR जैसे टूल्स का उपयोग करके फ़ाइलों को पासवर्ड सुरक्षा के साथ कंप्रेस करने से सुरक्षा की एक अतिरिक्त परत जुड़ जाती है, और फ़ाइलों को सुरक्षित रूप से स्टोर करना या साझा करना आसान हो जाता है।

- **आधिकारिक डेटा केवल ऑफ़िस के PC पर ही स्टोर करें:**

  सभी आधिकारिक दस्तावेज़ और काम से संबंधित डेटा केवल अधिकृत ऑफ़िस कंप्यूटर या स्वीकृत सिस्टम पर ही सेव किए जाने चाहिए। इससे डेटा सुरक्षा बनाए रखने में मदद मिलती है, उचित बैकअप सुनिश्चित होता है, और डेटा खोने यालीक होने का जोखिम कम होता है, जो फ़ाइलों को निजी डिवाइस पर स्टोर करने से हो सकता है।

6.3. प्रिंटर और पेरिफेरल सुरक्षा

6.3.1 सुनिश्चित करें कि प्रिंटर के फ़र्मवेयर और सॉफ़्टवेयर नियमित रूप से अपडेट किए जाते हैं:

प्रिंटर और अन्य पेरिफेरल को अक्सर निर्माताओं से फ़र्मवेयर और सॉफ़्टवेयर अपडेट मिलते रहते हैं, ताकि सुरक्षा से जुड़ी कमियों को ठीक किया जा सके और परफ़ॉर्मेंस को बेहतर बनाया जा सके। इन अपडेट को नियमित रूप से इंस्टॉल करने से डिवाइस को संभावित साइबर खतरों से बचाने में मदद मिलती है और यह सुनिश्चित होता है कि डिवाइस संगठन के नेटवर्क के भीतर सुरक्षित रूप से काम करे।

6.3.2 साझा प्रिंटर के लिए एक अनोखा PIN/पासवर्ड सेट करें:

साझा प्रिंटर को एक अनोखे PIN या पासवर्ड से सुरक्षित किया जाना चाहिए, ताकि अनधिकृत उपयोगकर्ता उन तक पहुँच न बना सकें। इससे यह सुनिश्चित करने में मदद मिलती है कि केवल अधिकृत कर्मचारी ही प्रिंट कर सकें, सेटिंग्स में बदलाव कर सकें, या प्रिंटर से संवेदनशील दस्तावेज़ प्राप्त कर सकें।

6.3.3 प्रिंटर पर सीधे इंटरनेट पहुँच को बंद कर दें:

प्रिंटर को इंटरनेट तक असीमित पहुँच नहीं होनी चाहिए। सीधे इंटरनेट कनेक्टिविटी को बंद करने से बाहरी हमलों, मैलवेयर या अनधिकृत रिमोट पहुँच का जोखिम कम हो जाता है। प्रिंटर्स को केवल सुरक्षित ऑफिस नेटवर्क के माध्यम से ही कम्युनिकेट करना चाहिए।

6.3.4 प्रिंटर्स को इस तरह कॉन्फ़िगर करें कि वे प्रिंट हिस्ट्री या डॉक्यूमेंट्स को स्टोर न करें:

कुछ प्रिंटर्स प्रिंट किए गए डॉक्यूमेंट्स की कॉपीज़ को स्टोर करते हैं या अपनी इंटरनल मेमोरी में प्रिंट हिस्ट्री बनाए रखते हैं। इन सेटिंग्स को डिसेबल कर देना चाहिए या नियमित रूप से क्लियर करते रहना चाहिए, ताकि संवेदनशील जानकारी को स्टोर होने से रोका जा सके और यह सुनिश्चित किया जा सके कि अनधिकृत उपयोगकर्ता (unauthorized users) इस जानकारी तक पहुँच न बना सकें।

अनुभाग 7: सुधार के बाद की निगरानी

7.1 सिस्टम के व्यवहार पर नज़र रखें (अगले 24-48 घंटे)

किसी संभावित समस्या या सुरक्षा घटना को हल करने के बाद, सिस्टम की अगले 24-48 घंटों तक सावधानीपूर्वक निगरानी की जानी चाहिए ताकि यह सुनिश्चित हो सके कि कोई छिपा हुआ खतरा या समस्या बाकी न रह जाए। निम्नलिखित चेतावनी संकेतों पर ध्यान दें:

- **असामान्य धीमापन:**
  यदि कंप्यूटर अचानक सामान्य से धीमा हो जाता है, एप्लिकेशन खोलने में अधिक समय लेता है, या बार-बार अटक (फ्रीज़) जाता है, तो यह संकेत हो सकता है कि कोई दुर्भावनापूर्ण प्रोग्राम या बैकग्राउंड प्रक्रिया सिस्टम के संसाधनों का उपभोग कर रही है।

- **स्वचालित पॉप-अप:**
  अचानक खुलने वाले पॉप-अप, विज्ञापन, या ब्राउज़र विंडो का अपने आप खुलना इस बात का संकेत हो सकता है कि सिस्टम पर कोई एडवेयर, मैलवेयर, या अनधिकृत सॉफ़्टवेयर इंस्टॉल है।

- **अज्ञात प्रक्रियाएँ:**
  बैकग्राउंड में चल रही किसी भी अपरिचित या संदिग्ध प्रक्रिया के लिए सिस्टम के टास्क मैनेजर की जाँच करें। ऐसे अज्ञात प्रोग्राम जो उच्च CPU, मेमोरी, या डिस्क उपयोग कर रहे हों, वे दुर्भावनापूर्ण गतिविधि का संकेत हो सकते हैं।

- **बार-बार आने वाले एंटीवायरस अलर्ट:**
  बार-बार आने वाली एंटीवायरस चेतावनियाँ या पहचान इस बात का संकेत हो सकती हैं कि सिस्टम पर अभी भी कोई खतरा मौजूद है, या नई संदिग्ध फ़ाइलें लगातार बनाई जा रही हैं।

यदि कोई समस्या दिखाई दे तो क्या करें:

यदि उपरोक्त में से कोई भी संकेत दिखाई देता है, तो तुरंत महत्वपूर्ण डेटा का पूरा बैकअप लें और PC को फिर से बनाने (ऑपरेटिंग सिस्टम और आवश्यक सॉफ़्टवेयर को फिर से इंस्टॉल करने) पर विचार करें, ताकि यह सुनिश्चित हो सके कि सिस्टम पूरी तरह से साफ और सुरक्षित है। यह किसी भी छिपे हुए मैलवेयर को हटाने में मदद करता है, जो शायद पहले न हटाया गया हो।

7.2 रिपोर्टिंग और समापन

सिस्टम जाँच और सुधार के चरण पूरे करने के बाद, घटना या सुरक्षा समीक्षा को औपचारिक रूप से बंद करने के लिए उचित दस्तावेज़ीकरण और रिपोर्टिंग की जानी चाहिए। निम्नलिखित जानकारी साझा की जानी चाहिए:

- **एंटीवायरस / EDR स्कैन रिपोर्ट:**

  इंस्टॉल किए गए एंटीवायरस या एंडपॉइंट डिटेक्शन एंड रिस्पॉन्स (EDR) समाधान द्वारा तैयार की गई नवीनतम स्कैन रिपोर्ट प्रदान करें। रिपोर्ट में स्पष्ट रूप से यह दर्शाया जाना चाहिए कि क्या सिस्टम से कोई खतरा पहचाना गया, क्वारंटाइन किया गया, या हटाया गया। यह सुरक्षा टीम को यह सत्यापित करने में मदद करता है कि सिस्टम को ठीक से स्कैन किया गया है और वह उपयोग के लिए सुरक्षित है।

- **CSK स्कैन परिणाम:**

  यदि CSK सुरक्षा स्कैन या किसी आंतरिक सुरक्षा स्कैनिंग टूल का उपयोग किया गया था, तो स्कैन के पूरे परिणाम साझा करें। ये परिणाम इस बात की पुष्टि करने में मदद करते हैं कि सिस्टम में कोई भेद्यता (vulnerabilities), दुर्भावनापूर्ण फ़ाइलें, या संदिग्ध कॉन्फ़िगरेशन मौजूद नहीं हैं।

- **औपचारिक रूप से बंद करने के लिए SecLAN / RSWAN / RajNET / SOC टीम को विवरण जमा करें:**

  सभी रिपोर्ट और संबंधित विवरण समीक्षा के लिए SecLAN, RSWAN, RajNET या SOC (Security Operations Center) टीम को जमा किए जाने चाहिए। सुरक्षा टीम प्रदान की गई रिपोर्टों का विश्लेषण करेगी और पुष्टि करेगी कि समस्या का समाधान हो गया है। एक बार सत्यापित हो जाने पर, वे सुरक्षा निगरानी प्रणाली में मामले या घटना को औपचारिक रूप से बंद कर देंगे।

उचित रिपोर्टिंग जवाबदेही, दस्तावेज़ीकरण और संगठनात्मक सुरक्षा नीतियों के अनुपालन को सुनिश्चित करती है।

अनुभाग 8: महत्वपूर्ण सहायता एवं संदर्भ

क्र. सं.	संसाधन URL	विवरण
1	https://doitc.rajasthan.gov.in/Content/CyberSecurityAdvisory.aspx	DOITC साइबर सुरक्षा परामर्श
2	https://www.cert-in.org.in	सुरक्षा परामर्श, दिशानिर्देश एवं अलर्ट
3	https://www.csk.gov.in	सुरक्षा उपकरण एवं सर्वोत्तम परामर्श
4	https://nic-cert.nic.in	सुरक्षा परामर्श, दिशानिर्देश एवं अलर्ट
5	https://infosecawareness.in/	साइबर सुरक्षा जागरूकता सामग्री
6	https://www.meity.gov.in/cyber-security-division	कानून, नीतियाँ एवं दिशानिर्देश
7	https://guidelines.india.gov.in/	भारतीय सरकारी वेबसाइटों के लिए दिशा निर्देश