CISO

साइबर सुरक्षा निर्देशिका

तकनीकी सेवायें

उत्तर प्रदेश पुलिस

राजीव कृष्ण, IPS
पुलिस महानिदेशक
उत्तर प्रदेश पुलिस
e-Mail: police.up@nic.in
Website: https://uppolice.gov.in

शुभकामना संदेश

प्रिय साथियों,

आज के युग में, जब शासन, संचालन और नागरिक सेवाएं तेजी से डिजिटल हो रही हैं, **साइबर सुरक्षा केवल एक तकनीकी विषय नहीं**, बल्कि एक **रणनीतिक आवश्यकता** बन चुकी है। प्रत्येक संस्था, विशेष रूप से वे जो सार्वजनिक सुरक्षा और संवेदनशील डेटा से जुड़ी हैं, को यह समझना होगा कि उनका **डिजिटल इन्फ्रास्ट्रक्चर उतना ही महत्वपूर्ण है जितना कि फिजिकल इन्फ्रास्ट्रक्चर।**

जैसे-जैसे हम टैक्नोलाजी-आधारित पुलिसिंग और प्रशासन की दिशा में आगे बढ़ रहे हैं, हमारी जिम्मेदारियाँ भी बढ़ी हैं। आज के डिजिटल युग में **पारदर्शिता, जवाबदेही और डिजिटल स्थिरता** अच्छे प्रशासन के आधार बन गए हैं। एक छोटा सा साइबर अपराध भी हमारी सेवाओं को बाधित कर सकता है, हमारे साइबर इन्फ्रास्ट्रक्चर को नुकसान पहुंचा कर हमें अपूर्णनीय क्षति पहुंचा सकता है।

इस परिप्रेक्ष्य में यह हर्ष का विषय है कि तकनीकी सेवायें मुख्यालय द्वारा **"CISO साइबर सुरक्षा निर्देशिका"** का प्रकाशन किया जा रहा है। यह **साइबर सुरक्षा निर्देशिका** केवल एक पुस्तिका नहीं, बल्कि **एक साइबर-जागरूक और जिम्मेदार संगठन की ओर एक कदम** है, जो प्रत्येक स्तर के कार्मिक को साइबर सुरक्षा में अपनी भूमिका को समझने और उसका पालन करने की दिशा में मार्गदर्शन प्रदान करती है।

मैं तकनीकी सेवायें मुख्यालय की साइबर सुरक्षा टीम और हमारे Chief Information Security Officer (CISO) के इस प्रयास की सराहना करता हूँ और सभी अधिकारियों व कर्मचारियों से आग्रह करता हूँ कि वे इस पुस्तिका को ध्यानपूर्वक पढ़ें और इसमें दिए गए सुझावों को अपने दैनिक कार्य में अपनाएं।

साइबर सुरक्षा किसी एक की जिम्मेदारी नहीं है बल्कि यह एक सामूहिक अभ्यास है जिसे हम सभी को मिलकर विकसित करना होगा।

आइए हम एक उदाहरण प्रस्तुत करें और अपने नागरिकों के लिए एक **सुरक्षित, विश्वसनीय और स्थिर डिजिटल वातावरण** तैयार करें।

शुभकामनाओं सहित।

(राजीव कृष्ण)

नवीन अरोरा, IPS
अपर पुलिस महानिदेशक
तकनीकी सेवायें एवं
CISO, उ0प्र0 पुलिस
e-Mail: adgts@up.nic.in
Website: https://uppolice.gov.in

शुभकामना संदेश

प्रिय साथियों,

आज के डिजिटल युग में **साइबर सुरक्षा,** राष्ट्रीय सुरक्षा की एक मजबूत आधारशिला बन चुकी है, विशेष रूप से पुलिस जैसे **कानून प्रवर्तन संगठनों** के लिए। जनता के विश्वास और राष्ट्रीय अखंडता के संरक्षक होने के नाते, हमारा कर्तव्य है कि हम केवल भौतिक सीमाओं की ही नहीं, बल्कि अपने **डिजिटल मोर्चों की भी सुरक्षा** करें। पुलिसिंग के संचालन जैसे रिकॉर्ड प्रबंधन से लेकर खुफिया जानकारी एकत्र करने तक, अब सब कुछ डिजिटल हो रहा है और हमारे सिस्टम तथा डेटा, साइबर अपराधियों व असामाजिक तत्वों के लिए Priority Target बन चुके हैं।

पुलिस विभाग में साइबर सुरक्षा का महत्व अब दिन प्रतिदिन महत्वपूर्ण होता जा रहा है। चल रही जांचों की गोपनीयता बनाए रखने से लेकर नागरिकों और अधिकारियों के डेटा की सुरक्षा तक, किसी भी प्रकार की चूक, गंभीर **Operational, Legal & Reputational Consequences** उत्पन्न कर सकती है। साइबर सुरक्षा सिर्फ एक IT से जुड़ा मुद्दा नहीं है, यह एक **रणनीतिक और सामूहिक जिम्मेदारी** है, जो हर वर्दीधारी और सेवार्थ व्यक्ति से सम्बन्धित है।

भारत सरकार द्वारा अधिनियमित **Digital Personal Data Protection (DPDP) Act, 2023** के अनुसार, हमारी भूमिका केवल कानून प्रवर्तन तक सीमित नहीं है, बल्कि **Data Fiduciary, Significant Data Fiduciary (SDF)** एवं **Data Processor** के रूप में हम एक बहु-आयामी साइबर उत्तरदायित्व भी निभा रहे हैं इसलिए हमारी कानूनी, नैतिक और साइबर सुरक्षा संबंधी ज़िम्मेदारियाँ तीनों ही स्तरों पर अत्यंत महत्वपूर्ण हैं। यह आवश्यक है कि हम डेटा सुरक्षा को केवल एक तकनीकी आवश्यकता न मानें, बल्कि उसे जनविश्वास, न्याय और राष्ट्रीय सुरक्षा की रीढ़ के रूप में स्वीकार करें।

साइबर सुरक्षा तीन स्तंभों **People, Process & Technology** पर आधारित है जिसे प्रभावी रूप से क्रियान्वित करने के लिए इन तीनों स्तंभों को सुदृढ़ करना आवश्यक है। यह **मार्गदर्शक पुस्तिका** प्रत्येक स्तर के पदाधिकारी के लिए एक व्यावहारिक संदर्भ के रूप में तैयार की गई है, जिसे ध्यानपूर्वक पढ़कर पालन करने से लाभ होगा। साइबर स्वच्छता को उसी गंभीरता से लें, जैसे आप भौतिक सुरक्षा को लेते हैं।

आइए, हम सब मिलकर एक **साइबर सुरक्षित पुलिस बल** का निर्माण करें जो न केवल सुरक्षा प्रदान करे, बल्कि जिम्मेदार डिजिटल आचरण भी प्रस्तुत करें।

सतर्क रहें। सुरक्षित रहें। प्रतिबद्ध रहें।

शुभकामनाओं सहित।

(नवीन अरोरा)

अनुक्रमणिका

1. साइबर स्पेस – एक परिचय 2

2. पुलिस सेवाओं में साइबर सुरक्षा का महत्व 3

   2.1 - 2.9 3-4

3. पुलिस सेवाओं के सम्बन्ध में सम्भावित साइबर खतरे 5

   3.1 - 3.23 5-11

4. उभरते साइबर खतरे 12

   4.1 - 4.10 12-15

5. साइबर स्पेस में उपयोगकर्ता के लिए स्वीकार्य व्यवहार और दिशानिर्देश 16

   5.1 - 5.9 16-21

6. साइबर घटना/Incident रिपोर्टिंग 22

   महत्वपूर्ण URL एवं Website........

Technical Services, UP Police

थानों एवं उच्च कार्यालयों के लिए साइबर सुरक्षा दिशानिर्देश

1. साइबर स्पेस – एक परिचय

साइबर स्पेस से तात्पर्य हमारे आस-पास के डिजिटल वातावरण से है जिसमें कंप्यूटर, मोबाइल, नेटवर्क डिवाइस और इंटरनेट शामिल हैं। इसमें सूचना प्रौद्योगिकी के सुरक्षित और कुशल उपयोग से संबंधित प्रौद्योगिकियां, प्रणालियां और गतिविधियां शामिल हैं।

आज के समय में साइबर स्पेस हमारे दैनिक जीवन का एक अभिन्न अंग बन गया है, जिसमें सभी Digital Interaction और Communication शामिल हैं। व्यक्तिगत ईमेल से लेकर महत्वपूर्ण राजकीय कार्यों तक, साइबर स्पेस आधुनिक समाज का अनिवार्य अंग बन गया है, जो अभूतपूर्व सुविधा और कनेक्टिविटी प्रदान करता है।

साइबर स्पेस के तेजी से विकास के साथ, खतरों का परिदृश्य नाटकीय रूप से विकसित हुआ है। जो कभी साधारण वायरस थे, वे अब वित्तीय लाभ से लेकर राजनीतिक जासूसी तक के विविध उद्देश्यों वाले दुर्भावनापूर्ण कारकों द्वारा संचालित परिष्कृत साइबर हमलों में बदल गए हैं। हमारे डिजिटल बुनियादी ढांचे की सुरक्षा के लिए इसको समझना महत्वपूर्ण है।

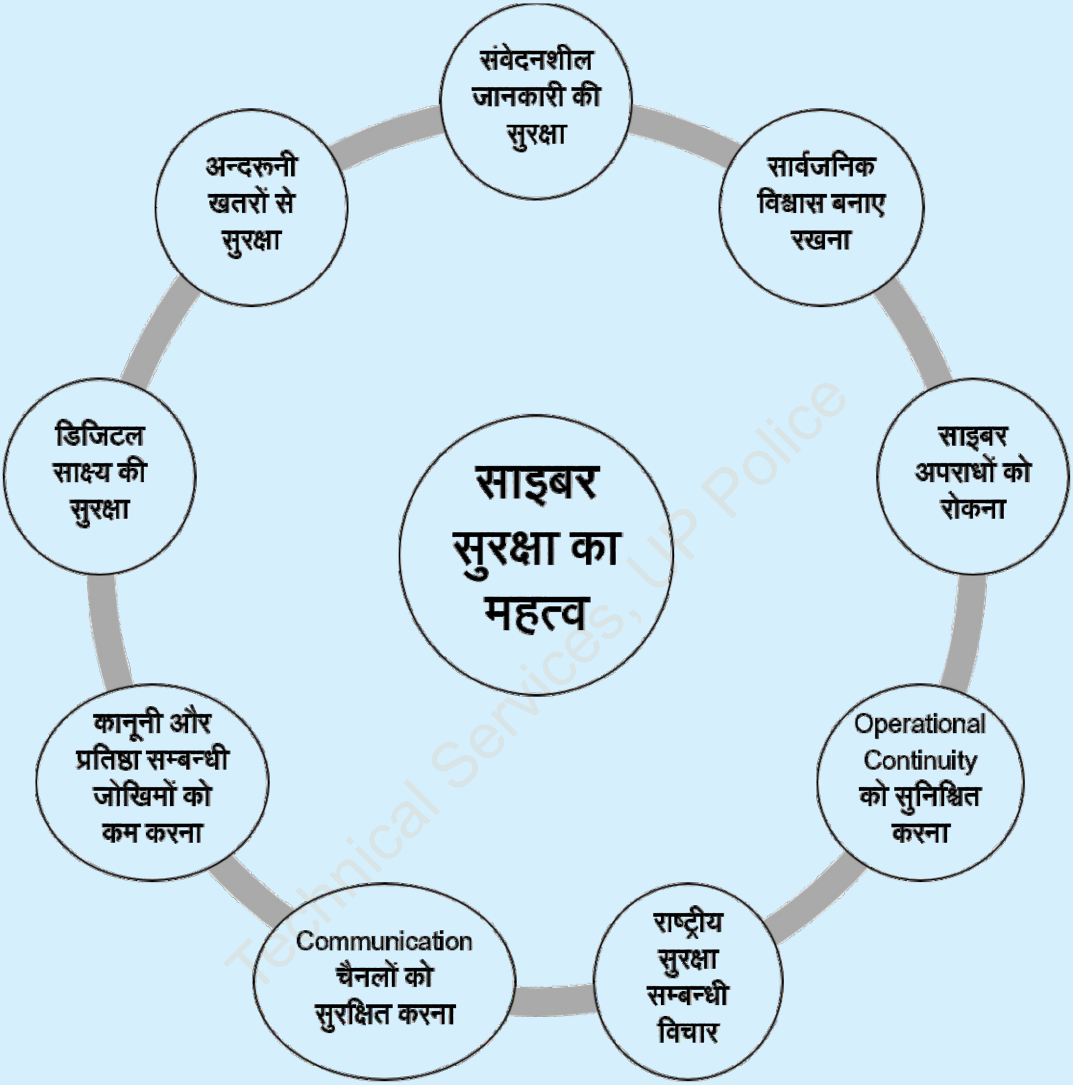
सोशल मीडिया प्लेटफ़ॉर्म ने हमारे संवाद करने, जानकारी साझा करने और दूसरों से जुड़ने के तरीके में क्रांति ला दी है। हालाँकि, वे पहचान की चोरी, फिशिंग और गलत सूचना के प्रसार सहित महत्वपूर्ण साइबर सुरक्षा जोखिम भी पैदा करते हैं। डिजिटल क्षेत्र में सुरक्षित रूप से क्रियाशील होने के लिए साइबर सुरक्षा सिद्धांतों की व्यापक समझ की आवश्यकता होती है।

साइबर अपराधी द्वारा सिस्टम को Compromise करने के लिए विभिन्न उपकरणों और तकनीकों का उपयोग किया जाता है। पीड़ितों के सिस्टम पर पहुंच प्राप्त कर, धोखा देकर, या पीड़ितों की जानकारी एकत्र करके कमजोरियों का फायदा उठाकर ठगी की जाती है अथवा अनैतिक आचरण के लिए बाध्य किया जाता है।

इसी क्रम में CERT-In, I4C तथा अन्य Cyber Security दिशा निर्देशों का अनुसरण करते हुए थानों एवं उच्च कार्यालयों के सुलभ सन्दर्भ एवं दिनचर्या में अभ्यास हेतु दिशा निर्देश तैयार किया गया है जिससे साइबर सुरक्षा सिद्धांतों की आधारभूत समझ विकसित की जा सके|

Technical Services, UP Police

2. पुलिस सेवाओं में साइबर सुरक्षा का महत्व



Technical Services, UP Police

2.1. संवेदनशील जानकारी की सुरक्षा

साइबर सुरक्षा, पुलिस के आपराधिक रिकॉर्ड, चल रही जांच और गोपनीय जानकारी जैसे संवेदनशील डेटा की सुरक्षा करती है और यह सुनिश्चित करती है कि यह अनधिकृत हाथों में न पड़े।

2.2. सार्वजनिक विश्वास/Public Trust बनाए रखना

प्रभावी साइबर सुरक्षा उपाय नागरिकों को यह आश्वासन देकर सार्वजनिक विश्वास बढ़ाते हैं कि उनकी व्यक्तिगत जानकारी और कानून प्रवर्तन एजेंसियों/ Law Enforcement Agencies के साथ interactions सुरक्षित और गोपनीय है।

2.3. साइबर अपराधों को रोकना

साइबर सुरक्षा उपाय Hacking, Identity Theft और ऑनलाइन धोखाधड़ी जैसे साइबर अपराधों को रोकने में मदद करते हैं जो सीधे Law enforcement agencies और उनके कर्मियों को प्रभावित कर सकते हैं।

2.4. परिचालन निरन्तरता/ Operational Continuity को सुनिश्चित करना

साइबर सुरक्षा महत्वपूर्ण प्रणालियों में व्यवधानों के खिलाफ सुरक्षा प्रदान करती है, निर्बाध संचालन सुनिश्चित करती है और संभावित डाउनटाइम को रोकती है जो सार्वजनिक/Public सुरक्षा से समझौता कर सकती है।

2.5. राष्ट्रीय सुरक्षा सम्बन्धी विचार/ Considerations

साइबर सुरक्षा राष्ट्रीय सुरक्षा का अभिन्न अंग है और उन साइबर हमलों को रोकती है जो महत्वपूर्ण बुनियादी ढांचे को compromise कर सकते हैं और Law Enforcement Agencies द्वारा प्रदान की जाने वाली आवश्यक सेवाओं को बाधित कर सकते हैं।

2.6. संचार/ Communication चैनलों को सुरक्षित करना

साइबर सुरक्षा, विभिन्न Law Enforcement Agencies के बीच संवेदनशील जानकारी के सुरक्षित संचार को सुनिश्चित करती है, अवरोधन या छेड़छाड़ को रोकती है।

2.7. Legal & Reputational Risks को कम करना

साइबर सुरक्षा, प्रोटोकॉल का अनुपालन, डेटा उल्लंघनों या साइबर हमलों से जुड़ी कानूनी जिम्मेदारियों और प्रतिष्ठा सम्बन्धी जोखिमों को कम करता है, Law Enforcement Agencies की अखंडता/ integrity को संरक्षित करता है।

2.8. डिजिटल साक्ष्य की सुरक्षा

साइबर सुरक्षा, डिजिटल साक्ष्य को Tampering से बचाती है, कानूनी कार्यवाही में इसकी स्वीकार्यता और विश्वसनीयता सुनिश्चित करती है।

2.9. अन्दरूनी खतरों से सुरक्षा

साइबर सुरक्षा उपाय अंदरूनी खतरों का पता लगाने और उन्हें रोकने में मदद करते हैं। यह सुनिश्चित करते हुए कि Law Enforcement Agencies के कर्मचारी जानबूझकर या अनजाने में कहीं संवेदनशील जानकारी को compromise अथवा अनाधिकृत रूप से साझा तो नहीं कर रहे हैं।

Technical Services UP Police

3. पुलिस सेवाओं के सम्बन्ध में सम्भावित साइबर खतरे

Technical Services, UP Police

- Goals of Cyber Attack
  - Money
  - Power
  - Control
  - Publicity
  - Revenge
  - Crackers
  - Learning
  - Strategic operation
  - Embed Sleepers
  - Espionage/Sabotage

- Attackers Profile
  - State/Nation Sponsored
  - Hobbyist & Learners
  - Activist & Enthusiasts
  - Insiders
  - Organized Gangs
  - Ideological Criminals

- Targets & Motives
  - Corporate
    - ✓ Defacement. Takeover Control
    - ✓ Financial, Extortion, Revenge
    - ✓ Information, Data Theft
    - ✓ Reputation Damage
  - Individual Personal
    - ✓ Yours and Family
    - ✓ Ransomware
    - ✓ Stalking, Blackmail, Scams
  - Critical National Infrastructure
  - Government & Political

3.1. Unauthorized Access

अपराधी संवेदनशील डेटाबेस तक अनधिकृत पहुंच का प्रयास कर सकते हैं, डिजिटल साक्ष्य या संवेदनशील डेटा से छेड़छाड़ कर सकते हैं जिससे चल रही जांच और कर्मियों से संबंधित गोपनीय जानकारी से समझौता हो सकता है।

Do's	Don'ts
✓ Verify sender's identity.	☒ Don't click without verification.
✓ Check URLs carefully.	☒ Don't share personal information.
✓ Report suspicious activity.	☒ Don't trust unsolicited requests.
✓ Educate yourself.	☒ Don't ignore security warnings.

3.2. Ransomware Attack

अपराधी महत्वपूर्ण प्रणालियों को encrypt करने के लिए रैंसमवेयर तैनात कर सकते हैं, Decryption Key के लिए भुगतान की मांग कर सकते हैं और दैनिक कार्यों को बाधित कर सकते हैं।

Do's	Don'ts
✓ Regular backup your data.	☒ Don't pay the ransom.
✓ Stay vigilant of suspicious emails.	☒ Don't click on suspicious links.
✓ Keep software updated.	☒ Don't delay reporting.
	☒ Don't disable security measures.

3.3. Phishing Attack

Law Enforcement Personnel को फिशिंग अटैक के माध्यम से लॉगिन क्रेडेंशियल से समझौता करने और सिस्टम तक अनधिकृत पहुंच प्रदान करने के साथ लक्षित/ target किया जा सकता है। Phishing Attack सामान्यतः e-mail Phishing, Social Media Phishing, SMS Phishing (Smishing), Voice Phishing (Vishing) आदि रूप से किया जाता है।

Do's	Don'ts
✓ Verify links before clicking.	☒ Don't Click on Suspicious Links or Attachments.
✓ Use multi-factor authentication.	☒ Don't Share Personal Information via Email.
✓ Keep software updated.	☒ Don't Trust Unverified Sender.
✓ Report suspicious communications	☒ Don't Use Weak Passwords

3.4. Spoofing

कोई व्यक्ति या सिस्टम धोखा देने के उद्देश्य से अपनी पहचान छुपाकर ऐसा दिखाता है कि वह किसी भरोसेमंद स्रोत से है। इसमें डेटा में हेरफेर करके आपको यह विश्वास दिलाया जाता है कि Sender Legitimate है, जिससे आप संवेदनशील जानकारी साझा कर सकते हैं या अपने सिस्टम की पहुँच दे सकते हैं।

Do's	Don'ts
✓ Verify email/IP addresses.	☒ Don't trust emails blindly.
✓ Use secure communication channels.	☒ Don't share sensitive information insecurely.
✓ Educate yourself.	☒ Don't trust display names or caller IDs without verification — they can be spoofed.
✓ Report and block suspicious or phishing emails and calls.	☒ Don't ignore browser warnings about unsecure or suspicious websites.

Technical Services, UP Police

3.5. Denial of Service (DoS) Attack

साइबर अपराधी नेटवर्क पर भारी ट्रैफ़िक लाकर Law Enforcement Services को बाधित करने का प्रयास कर सकते हैं, जिससे सेवा अनुपलब्ध हो सकती है। इससे जनता का विश्वास और पुलिस की प्रतिष्ठा ख़राब हो सकती है।

Do's	Don'ts
✓ Understand your network traffic. ✓ Develop a response plan. ✓ Implement Anti-DDoS solution. ✓ Scale bandwidth appropriately. ✓ Consider cloud-based protections ✓ Use Firewall with safety devices Intrusion Prevention Systems (IPS) etc.	☒ Don't ignore Unusual Traffic Patterns. ☒ Don't rely Solely on Firewalls: ☒ Don't delay Response. ☒ Don't host critical services without redundancy or load balancing. ☒ Don't delay response plans — every second counts during a DoS attack.

3.6. Social Engineering Attack

साइबर अपराधी अक्सर Human Vulnerabilities का लाभ उठाकर कर्मचारियों को धोखे में डाल सकते हैं। वे उन्हें इस तरह से प्रभावित करते हैं कि वे संवेदनशील जानकारी साझा कर दें या सुरक्षा प्रोटोकॉल का उल्लंघन कर बैठें। यह तकनीकें सामान्यतः Social Engineering attack में उपयोग की जाती हैं।

Do's	Don'ts
✓ Follow the official social media policy of department. ✓ Verify requests in person or via official channels. ✓ Be sceptical of urgent requests. ✓ Limit information sharing.	☒ Don't blindly comply with requests. ☒ Don't be fooled by urgency. ☒ Don't overshare information. ☒ Don't skip staying informed.

3.7. Malware Infection

Malicious Software (Malware), System को संक्रमित कर सकता है, जिससे अनधिकृत रूप से डेटा तक पहुंच, System में व्यवधान या संवेदनशील डेटा की चोरी (Exfiltration) हो सकती है।

Do's	Don'ts
✓ Install antivirus software. ✓ Be cautious of downloads. ✓ Regularly scan your devices. ✓ Keep software updated.	☒ Don't download from suspicious sources. ☒ Don't ignore security updates. ☒ Don't skip regular scans. ☒ Don't disable antivirus protection.

3.8. Weak Endpoint Security

व्यक्तिगत उपकरणों पर अपर्याप्त सुरक्षा, साइबर खतरों के लिए Entry Point प्रदान कर सकती है, जिससे Law Enforcement Agencies की समग्र सुरक्षा स्थिति/ Overall Security Posture से समझौता हो सकता है।

Do's	Don'ts
✓ Keep software updated. ✓ Deploy endpoint protection. ✓ Implement access controls. ✓ Educate users.	☒ Don't allow Unmanaged Devices. ☒ Don't disable Security Features. ☒ Don't ignore Alerts.

Technical Services, UP Police

3.9. Insecure Third-Party Access

Third Party Seller या सेवा प्रदाताओं के साथ अपर्याप्त रूप से सुरक्षित बातचीत से साइबर खतरे उत्पन्न हो सकते हैं, जो संभावित रूप से अनधिकृत संस्थाओं के लिए संवेदनशील जानकारी को उजागर कर सकते हैं।

Do's	Don'ts
✓ Assess vendor security practices. ✓ Define clear security expectations. ✓ Monitor continuously. ✓ Limit access.	☒ Don't assume Compliance. ☒ Don't neglect Ongoing Oversight. ☒ Don't overlook Incident Reporting. ☒ Don't disable antivirus protection.

3.10. Hacking

वह प्रक्रिया है जिसमें कोई व्यक्ति बिना अनुमति के कंप्यूटर सिस्टम, नेटवर्क या डेटा तक पहुँच प्राप्त करता है। इसका उद्देश्य डेटा चोरी करना, उसे बदलना या सेवाओं को बाधित करना हो सकता है। यह व्यक्तिगत, कॉरपोरेट या सरकारी स्तर पर गंभीर नुकसान पहुँचा सकता है।

Do's	Don'ts
✓ Use strong and unique passwords. ✓ Keep systems and software updated. ✓ Enable firewalls and antivirus software. ✓ Monitor network activity regularly.	☒ Don't reuse old or simple passwords. ☒ Don't ignore security updates. ☒ Don't turn off security tools. ☒ Don't click unknown links/download files blindly.

3.11. Cyber Stalking

किसी व्यक्ति की ऑनलाइन गतिविधियों पर लगातार नज़र रखी जाती है और उसे बार-बार संदेश या धमकियाँ भेजी जाती हैं। इसका उद्देश्य डराना, मानसिक रूप से परेशान करना या नियंत्रण करना हो सकता है। यह अपराध विशेष रूप से सोशल मीडिया और मैसेजिंग ऐप्स पर देखने को मिलता है।

Do's	Don'ts
✓ Block and report stalkers immediately. ✓ Keep evidence (screenshots, messages). ✓ Update privacy settings on social platforms. ✓ Inform law enforcement if it escalates.	☒ Don't respond to threatening messages. ☒ Don't share personal info publicly. ☒ Don't accept unknown friend requests. ☒ Don't ignore persistent harassment.

3.12. Cyber Bullying

वह प्रक्रिया है जिसमें किसी व्यक्ति को इंटरनेट के माध्यम से अपमानित किया, धमकाया या मजाक उड़ाया जाता है। यह विशेष रूप से स्कूल और कॉलेज के बच्चों को प्रभावित करता है। इसके कारण पीड़ित को भावनात्मक आघात लगता है और आत्मविश्वास की कमी हो सकती है।

Do's	Don'ts
✓ Support and report victims of bullying. ✓ Save evidence like messages or screenshots. ✓ Educate youth about digital etiquette. ✓ Use platform safety tools like blocking/reporting.	☒ Don't ignore signs of bullying. ☒ Don't retaliate or engage with bullies. ☒ Don't share embarrassing content of others. ☒ Don't assume it's harmless fun.

Technical Services, UP Police

3.13. Child Pornography

यह एक गंभीर अपराध है जिसमें बच्चों की अश्लील सामग्री को बनाना, वितरित करना या देखना शामिल है। यह बच्चों के अधिकारों का उल्लंघन है और इसके लिए कड़ी कानूनी सजा होती है। Internet और Dark Web इसका प्रमुख माध्यम हैं।

Do's	Don'ts
✓ Report any such content to law enforcement.	☒ Don't download or share illicit material.
✓ Monitor children's online activity.	☒ Don't ignore suspicious activity or websites.
✓ Use parental controls and content filters.	☒ Don't access dark web or illegal forums.
✓ Support awareness campaigns against abuse.	☒ Don't overlook child safety online.

3.14. Cyber Espionage

इसमें किसी संस्था या सरकार की गोपनीय जानकारी को डिजिटल माध्यम से चोरी किया जाता है। यह अक्सर दूसरे देश की एजेंसियों या कम्पनियों द्वारा गुप्त रूप से किया जाता है। इसका उद्देश्य आर्थिक लाभ या रणनीतिक जानकारी हासिल करना होता है।

Do's	Don'ts
✓ Use encryption for sensitive communications.	☒ Don't share internal data on public platforms.
✓ Apply network segmentation and access control.	☒ Don't use weak authentication.
✓ Conduct regular security audits.	☒ Don't ignore suspicious activity logs.
✓ Train employees in security awareness.	☒ Don't underestimate insider threats.

3.15. Software Piracy

इसमें बिना लाइसेंस के सॉफ़्टवेयर को कॉपी करना, इंस्टॉल करना या वितरित करना शामिल है। यह कॉपीराइट कानून का उल्लंघन होता है और कानूनी कार्यवाही का कारण बन सकता है। Pirated Software से Virus और Security Risk भी बढ़ जाते हैं।

Do's	Don'ts
✓ Use licensed and original software.	☒ Don't download software from untrusted sources.
✓ Educate employees on legal software use.	☒ Don't share software illegally.
✓ Verify software source authenticity.	☒ Don't ignore licensing agreements.
✓ Perform software audits regularly.	☒ Don't disable anti-piracy protections.

3.16. Intellectual Property (IP) Infringement

जब कोई व्यक्ति किसी और की Intellectual Property जैसे Software, Music, Patent आदि को बिना अनुमति उपयोग करता है। यह Copyright और Patent कानूनों का उल्लंघन है। इससे मौलिक रचनाकारों को आर्थिक और नैतिक नुकसान होता है।

Do's	Don'ts
✓ Use properly licensed and credited material.	☒ Don't download or share pirated content.
✓ Respect trademarks and copyrights.	☒ Don't copy content without permission.
✓ Educate employees about IP laws.	☒ Don't use third-party content as your own.
✓ Perform regular copyright audits.	☒ Don't ignore DMCA or takedown notices.

Technical Services, UP Police

3.17. Email and Internet Fraud

इसमें नकली ईमेल, वेबसाइट या मैसेज के जरिए लोगों को धोखा दिया जाता है। इसका उद्देश्य व्यक्तिगत जानकारी चुराना या पैसों की ठगी करना होता है। यह सबसे आम साइबर अपराधों में से एक है और लगातार बढ़ रहा है।

Do's	Don'ts
✓ Verify sender's identity before responding. ✓ Report suspicious emails to IT or CERT. ✓ Use spam filters and email scanners. ✓ Educate users on spotting fraud signs.	☒ Don't click on unknown links or attachments. ☒ Don't share sensitive info via email. ☒ Don't trust emails demanding urgent action. ☒ Don't open emails from unknown sources.

3.18. Botnets

संक्रमित कम्प्यूटर का एक नेटवर्क होता है जिसे साइबर अपराधी दूर से नियंत्रित करते हैं। इनका उपयोग DDoS Attack, Spam भेजने और डेटा चोरी के लिए किया जाता है। उपयोगकर्ता को पता भी नहीं चलता कि उसका कम्प्यूटर इन हमलों में शामिल है।

Do's	Don'ts
✓ Use updated antivirus software. ✓ Patch all vulnerabilities promptly. ✓ Monitor unusual outbound traffic. ✓ Segment network access for endpoints.	☒ Don't ignore slow system behaviour. ☒ Don't install unknown software. ☒ Don't open attachments from unknown senders. ☒ Don't connect compromised devices.

3.19. Insider Threats

Insider Threats तब उत्पन्न होते हैं जब कंपनी का ही कोई कर्मचारी या अधिकृत व्यक्ति अपने अधिकारों का दुरुपयोग करता है। इसका उद्देश्य जानबूझकर डेटा चोरी, नुकसान या धोखाधड़ी हो सकता है। यह खतरनाक इसलिए होता है क्योंकि इसमें अपराधी के पास पहले से ही System की पहुँच होती है।

Do's	Don'ts
✓ Monitor employee access and behaviour. ✓ Apply the principle of least privilege. ✓ Conduct background checks. ✓ Establish whistle-blower mechanisms.	☒ Don't give unnecessary access rights. ☒ Don't ignore red flags in behaviour. ☒ Don't allow use of personal USB devices. ☒ Don't bypass audit trails.

3.20. Data Breach

Data Breach तब होता है जब कोई अनधिकृत व्यक्ति किसी System में घुसकर संवेदनशील या निजी जानकारी तक पहुँच बना लेता है। इसमें User Data, Password, Credit Card Details आदि शामिल हो सकते हैं। इससे व्यक्ति और संस्था दोनों को गम्भीर नुकसान हो सकता है।

Do's	Don'ts
✓ Encrypt sensitive data. ✓ Use multi-layer authentication. ✓ Regularly audit access logs and systems. ✓ Train staff in data handling protocols.	☒ Don't store unprotected personal information. ☒ Don't ignore access control policies. ☒ Don't delay breach disclosure or response. ☒ Don't leave data unattended or unmonitored.

Technical Services, UP Police

3.21. Electronic Money Laundering

यह वह प्रक्रिया है जिसमें अवैध रूप से कमाए गए पैसे को डिजिटल माध्यम से वैध दिखाया जाता है। इसमें Crypto Currency, e-Wallet और Online Banking का उपयोग किया जाता है। यह आर्थिक अपराधों और Terror Funding से जुड़ा हो सकता है।

Do's	Don'ts
✓ Monitor digital transactions for irregularities.	☒ Don't engage with unknown e-wallets.
✓ Follow KYC norms and transaction limits.	☒ Don't allow others to use your accounts.
✓ Report large unexplained transfers.	☒ Don't deal with unlicensed money handlers.
✓ Audit digital payment systems regularly.	☒ Don't ignore suspicious funding sources.

3.22. Crypto Jacking

Crypto Jacking एक ऐसा हमला है जिसमें किसी उपयोगकर्ता की जानकारी के बिना उसका Device, Crypto-Currency Mining के लिए इस्तेमाल किया जाता है। इससे Device Slow हो जाती है और बिजली की खपत बढ़ जाती है। यह अक्सर Website Scripts या Malware के ज़रिए होता है।

Do's	Don'ts
✓ Monitor CPU/GPU usage regularly.	☒ Don't ignore slow or overheating systems.
✓ Use crypto-jacking detection tools.	☒ Don't install unverified browser extensions.
✓ Apply ad-blockers and script blockers.	☒ Don't visit risky websites without protection.
✓ Educate users on background mining signs.	☒ Don't ignore permission prompts.

3.23. Online Drug Trafficking

इसमें अवैध नशीली दवाओं की खरीद-बिक्री Internet या Dark Web के ज़रिए की जाती है। इसका उपयोग गुमनाम रूप से Crypto Payment और Encrypted Chats के माध्यम से किया जाता है। यह अपराध कई देशों की सुरक्षा एजेंसियों के लिए एक चुनौती है।

Do's	Don'ts
✓ Report suspicious online transactions.	☒ Don't engage with or promote illegal substances.
✓ Monitor online behaviour of minors.	☒ Don't visit or transact on dark web sites.
✓ Collaborate with law enforcement on findings.	☒ Don't ignore drug-related online slang/activities.
✓ Use filters and alerts in network monitoring.	☒ Don't assume online platforms are drug-free.

Technical Services, UP Police

4. उभरते साइबर खतरे

4.1. Digital Arrest

a) "Digital Arrest" कानूनी रूप से मान्यता प्राप्त शब्द नहीं है। यह एक Scam है जिसमें अपराधी, पुलिस या अन्य Law Enforcement Agency (CBI, Customs etc.) का रूप धारण करते हैं और किसी व्यक्ति पर अपराध का झूठा आरोप लगाते हैं, अक्सर "अपना नाम हटाने" या "गिरफ़्तारी से बचने" के लिए पैसे या संवेदनशील जानकारी की मांग करते हैं।

b) इस पूरी प्रक्रिया के दौरान पीड़ित को वीडियों कॉल के माध्यम से घर से बाहर या किसी से बात करने से प्रतिबंधित करते है।

c) इस पूरी प्रक्रिया को फर्जी वीडियो कॉल, नकली दस्तावेज़ और इतने प्रोफेशनल तरीके से किया जाता है कि पीड़ित, अपराधियों के अनुसार दिये गये निर्देशों का पालन करने लगता है।

Do's	Don'ts
✓ Stay Calm and Don't Panic. ✓ Verify the Caller, know the Facts. ✓ Report Suspicious Activity ✓ Understand the Law. Educate Yourself/Others ✓ Use Official Channels	☒ Don't Share Personal Information ☒ Don't Make Immediate Payments ☒ Don't Trust Unverified Documents ☒ Don't Isolate Yourself ☒ Don't Engage Further

Technical Services, UP Police

4.2. KYC Scam

a) इस धोखाधड़ी में साइबर अपराधी व्यक्तिगत जानकारी चुराने, Identity Theft करने या अवैध रूप से वित्तीय खातों तक पहुँचने के लिए पहचान सत्यापन प्रक्रियाओं का फायदा उठाते हैं।

b) धोखेबाज कॉल करते हैं और KYC Update करने, बैंक खाता/क्रेडिट/डेबिट कार्ड ब्लॉक करने की जल्दी का दिखावा करते हैं |

c) इससे व्यक्तियों, व्यवसायों और वित्तीय संस्थानों को महत्वपूर्ण वित्तीय नुकसान और प्रतिष्ठा को नुकसान हो सकता है।

Do's	Don'ts
✓ Verify Requests. ✓ Use Official Contacts. ✓ Report Incidents. ✓ Check KYC Update Methods	☒ Never share your account login details, card information, PINs, passwords, or OTPs ☒ Do not share KYC documents or their copies with unknown ☒ Do not click on suspicious or unverified links received via mobile or email.

4.3. Part time/Online job fraud

a) स्कैमर द्वारा काम की तलाश कर रहे लोगों को धोखा दिया जाता है।

b) स्कैमर्स वेबसाइट, सोशल मीडिया पर फर्जी जॉब पोस्ट करते हैं या ईमेल भेजते हैं, जिसमें उच्च वेतन और आसान काम का वादा किया जाता है।

c) स्कैमर फर्जी SMS भेजकर प्रतिष्ठित कम्पनियों में पार्ट टाइम जॉब का ऑफर देते हैं |

d) उनका लक्ष्य पीड़ित के पैसे या व्यक्तिगत जानकारी चुराना होता है।

e) अनजान व्यक्ति के साथ कोई भी वित्तीय लेन-देन करने से पहले सावधान रहें |

Do's	Don'ts
✓ Use trusted sources. ✓ Verify the caller, check credentials. ✓ Ask questions. ✓ Verify emails.	☒ Avoid upfront fees. ☒ Do not trust sponsored search results ☒ Never apply for jobs without verifying the authenticity ☒ Avoid clicking on unverified or suspicious links ☒ Avoid financial transactions with unknown individuals

4.4. Online Shopping Fraud

a) यह धोखाधड़ी एक साइबर अपराध है जिसमें धोखेबाज, पीड़ितों को अवैध खरीद्दारी करने के लिए धोखा देते हैं।

b) वे नकली वेबसाइट बनाते हैं या वैध प्लेटफ़ॉर्म में हेरफेर करते हैं, ऐसे Offer पेश करते हैं जो बहुत लुभावने प्रतीत होते हैं, और व्यक्तिगत तथा वित्तीय जानकारी चुराते हैं, जिससे वित्तीय नुकसान होता है और Online Marketplace में अविश्वास होता है।

Do's	Don'ts
✓ Compare prices. ✓ Use cash-on-delivery. ✓ Choose verified sellers. ✓ Verify offers. ✓ Secure transactions.	☒ Do not make e-shopping transactions using public computers or networks. ☒ Do not save your card details, date of birth, phone number, etc., on unreliable e-shopping websites. ☒ Do not make advance payments on C2C platforms like OLX, Quikr, etc., without verifying the seller's credentials. ☒ Do not scan QR codes to 'receive' money

4.5. Investment Scam

a) निवेश घोटाले में धोखाधड़ी वाली योजनाएं शामिल होती हैं जो High Return का वादा करती हैं, जो अक्सर सच होने के लिए बहुत लुभावने प्रतीत होता है।

b) ये घोटाले वैध आर्थिक गतिविधि के माध्यम से लाभ उत्पन्न करने के बजाय नए निवेशकों के पैसे से पहले के निवेशकों को भुगतान करते हैं। इसे **Ponzi Scheme** के नाम से भी जाना जाता है।

Do's	Don'ts
✓ Invest with Registered Entities. ✓ Verify Investment Products. ✓ Stay Informed/cautious if investment scheme is in form of MLM (Multi-Level Marketing). ✓ Report suspicious activity.	☒ Don't panic. ☒ Don't trust unbelievable returns. ☒ Don't join dubious/doubtful groups. ☒ Don't ignore red flags ☒ Don't invest without physical verification

Technical Services UP Police

4.6. Search Engine Fraud

a) यह तब होती है जब धोखेबाज Search Result में हेराफेरी करके फर्जी संपर्क जानकारी प्रदर्शित करते हैं, खुद को वैध संस्था बताते हैं।

b) पीड़ित जो अनजाने में इन नंबरों पर कॉल करते हैं, वे पासवर्ड और खाते के विवरण जैसी संवेदनशील जानकारी प्रदान कर सकते हैं, जिससे वित्तीय नुकसान, Identity Theft और अन्य गंभीर परिणाम हो सकते हैं।

Do's	Don'ts
✓ Visit official websites. ✓ Verify contacts. ✓ Watch for red flags. ✓ Verify secure website by https in the URL.	☒ Don’t trust search results. ☒ Don’t share info unprompted.

4.7. Social Media Impersonation

a) Social Media Impersonation तब होता है जब कोई व्यक्ति किसी वास्तविक व्यक्ति या संगठन की नकल करते हुए नकली खाता बनाता है।

b) जालसाज, परिवार का सदस्य/मित्र/बैंक कर्मचारी/सरकारी अधिकारी होने का दिखावा करके पीड़ित को पैसे या संवेदनशील जानकारी देने के लिए धोखा देता है।

c) इन धोखाधड़ी वाले खातों का उपयोग दूसरों को धोखा देने के लिए किया जाता है, जिससे अक्सर Identity Theft, Financial Scam, प्रतिष्ठा को नुकसान और गलत जानकारी का प्रसार होता है।

d) नकली WhatsApp/Facebook नकली DP (Display Picture) का उपयोग करके नकद और उपहार कूपन मांगने की विधी अपनाई जा सकती है।

Do's	Don'ts
✓ Verify contacts/accounts. ✓ Be cautious. ✓ Report Impersonation on 1930. ✓ Be alert to calls, emails, or other methods of contact that ask for sensitive information. ✓ Always verify from person/organization on normal call before transferring fund.	☒ Confirm fund requests. ☒ Don’t make payments. ☒ Never share personal or confidential details on social media. ☒ Don’t share meeting schedule/appointment/ sensitive data on social media. ☒ Never trust contact/DP/Photo.

Technical Services, UP Police

4.8. SIM Swap Fraud

a) इसमें धोखेबाज आपके फ़ोन नंबर को अपने SIM Card में ट्रांसफर कर लेते हैं।

b) इससे उन्हें आपके Call, SMS और 2-Factor Authentication Code तक पहुँच मिल जाती है, जिससे Identity Theft, Account Takeover और Financial Fraud हो सकता है।

c) जालसाज अक्सर नेटवर्क स्टाफ़ बनकर आपको अपग्रेड या लाभ देने की पेशकश करते हैं ताकि आपसे व्यक्तिगत विवरण प्राप्त किया जा सके।

d) जालसाज पीड़ित के फर्जी पहचान प्रमाण के साथ नया सिम प्राप्त कर सकते हैं और OTP(One Time Password) आधारित लेनदेन को नियंत्रित कर सकते हैं।

e) अपराधी फिर पीड़ित के संपर्कों को कॉल करने और SMS भेजने के लिए फ़ोन नंबर का उपयोग कर सकते हैं।

Do's	Don'ts
✓ Enable 2-Factor authentication. ✓ Use strong PINs. ✓ Stay updated ✓ Report SIM loss/no network. ✓ Report suspicious activity.	☒ Never store sensitive data or share OTPs with strangers via calls or texts. ☒ Never share personal or confidential details on social media.

4.9. Deepfake Cybercrime

a) साइबर अपराधी वास्तविक फुटेज या रिकॉर्डिंग में हेराफेरी करके नकली वीडियो या ऑडियो क्लिप बनाने के लिए उन्नत AI का उपयोग करते हैं।

b) इसके उपरान्त नकली फुटेज, Social Media, Messaging App और e-Mail के माध्यम से फैलाए जाते हैं, जो अक्सर सार्वजनिक हस्तियों, मशहूर हस्तियों या अधिकारियों को निशाना बनाते हैं।

c) इसका लक्ष्य दर्शकों को धोखा देना, राय में हेराफेरी करना या गलत जानकारी फैलाना है।

d) अपराधी Deepfake को वास्तविक दिखाने के लिए सोशल इंजीनियरिंग तकनीकों का उपयोग कर सकते हैं, जिससे व्यक्ति और संगठन जोखिम में पड़ सकते हैं।

Do's	Don'ts
✓ Stay informed. ✓ Verify content. ✓ Use trusted sources.	☒ Don't share unverified media. ☒ Don't trust suspicious sources. ☒ Don't trust blindly. ☒ Don't ignore privacy.

4.10. Remote Access Fraud

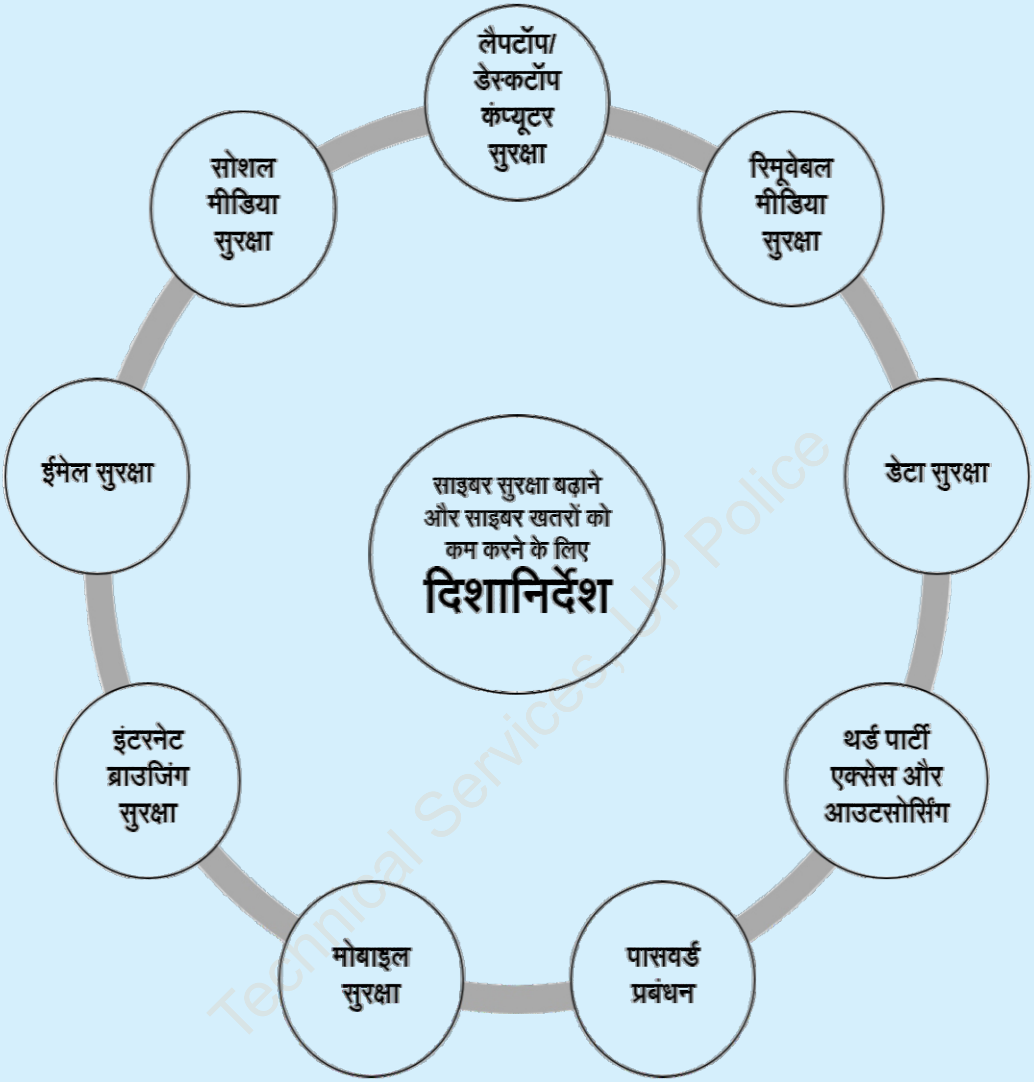
a) जालसाज तकनीकी सहायता कर्मचारी/रिफंड प्रोसेस करने वाले विश्वसनीय संस्थाओं का दिखावा/प्रतिरूपण/Impersonation करते हैं और पीड़ित का संवेदनशील डेटा/वित्तीय जानकारी चुराने के लिए Remote Access App install करने के लिए प्रेरित करते हैं।

b) वे Screen Sharing App के माध्यम से व्यक्तियों को उनके डिवाइस तक अनधिकृत पहुँच प्रदान करने के लिए धोखा देते हैं।

c) एक बार पहुँच प्रदान करने के बाद, वे संवेदनशील डेटा चुरा सकते हैं, खातों पर नियंत्रण कर सकते हैं और धोखाधड़ी वाले लेन-देन कर सकते हैं।

Do's	Don'ts
✓ Trust carefully. ✓ Verify identity. ✓ Avoid unknown software. ✓ Enhance security. ✓ Remove after Use.	☒ Never share personal or financial information remotely and avoid entering credentials while someone has screen access. ☒ Log out of all payment-related apps before downloading any screen-sharing software.

5. साइबर स्पेस में उपयोगकर्ता के लिए स्वीकार्य व्यवहार और दिशानिर्देश



Technical Services, UP Police

साइबर स्पेस में स्वीकार्य व्यवहार के मानक को बनाए रखना महत्वपूर्ण है। उपयोगकर्ताओं को ऐसी गतिविधियों में शामिल होने से बचना चाहिए जो डेटा की गोपनीयता से समझौता करती हैं या स्थापित प्रोटोकॉल का उल्लंघन करती हैं। Access Protocol का पालन करना, सुरक्षा सम्बन्धी घटनाओं की तुरंत रिपोर्ट करना और स्वीकार्य उपयोग नीतियों का पालन करना आवश्यक है। Cyber Security Trends और Best Practices के बारे में निरंतर शिक्षा और जागरूकता, उपयोगकर्ताओं को साइबरस्पेस का कुशलतापूर्वक उपयोग करने और संभावित जोखिमों को प्रभावी ढंग से कम करने में सक्षम बनाती है।

5.1. लैपटॉप/डेस्कटॉप कंप्यूटर सुरक्षा

a) केवल अधिकृत और लाइसेंस प्राप्त सॉफ़्टवेयर का उपयोग करें तथा सभी Pirated OS और Application का उपयोग तुरंत बंद करें।
b) नियमित कार्य के लिए कंप्यूटर/लैपटॉप तक पहुंचने के लिए केवल Standard User (Non-Administrator) Account का उपयोग करें। उपयोगकर्ताओं को Administrative access केवल उच्च/संबंधित प्राधिकारी के अनुमोदन से ही दिया जाना चाहिए।
c) OS और फ़र्मवेयर को विश्वसनीय/आधिकारिक स्रोत से update करें।
d) प्रत्येक मशीन पर एंटीवायरस Install होना चाहिए जो नवीनतम वायरस Definition, Signature और पैच के साथ updated होना चाहिए।
e) उपयोग में न होने पर डेस्कटॉप को हमेशा लॉक (Window Key + L)/ लॉग ऑफ करें।
f) यदि कोई अन्य उपयोगकर्ता नहीं है तो कार्यालय छोड़ने से पहले डेस्कटॉप बंद (Shut Down) कर दें।
g) प्रिंटर के सॉफ़्टवेयर को नवीनतम अपडेट/पैच के साथ updated होना चाहिए।
h) प्रिंटर पर इंटरनेट एक्सेस की अनुमति नहीं दी जानी चाहिए।
i) डेस्कटॉप/लैपटॉप और मोबाइल फोन पर जीपीएस, ब्लूटूथ, एनएफसी और अन्य सेंसर अक्षम/Disable रखें। आवश्यकता पड़ने पर ही इन्हें सक्षम/Enable किया जाये।
j) किसी भी असुरक्षित सामग्री पर पासवर्ड, आईपी एड्रेस, नेटवर्क डायग्राम या अन्य संवेदनशील जानकारी न लिखें (उदाहरणस्वरूप Sticky/Post-It Notes, उपयोगकर्ता के टेबल पर सादा कागज Pin/ Paste किया हुआ आदि)
k) Remote Access के लिए Open-Proxy, Tor, Free 3rd Party VPN सेवाओं का उपयोग करने से बचें।
l) पहले Installation के समय सभी Default Configuration को बदल दिया जाये।
m) Anydesk, Teamviewer, Ammyy Admin आदि जैसे किसी भी Remote Desktop Application को Block करना सुनिश्चित करें।
n) Wi-Fi Network को कनेक्ट करने के लिए उपयोग किए जाने वाले उपकरणों को नेटवर्क ब्रिजिंग से बचाने के लिए Wired नेटवर्क से एक साथ कनेक्ट करने की अनुमति नहीं दी जानी चाहिए।
o) संवेदनशील संगठनों में Wireless LAN की अनुमति नहीं दी जानी चाहिए।
p) DHCP को अक्षम/Disable करें और सभी वायरलेस उपयोगकर्ताओं को Static IP Address निर्दिष्ट/Assign करें।
q) संगठन को दैनिक संचालन करने के लिए आवश्यक Ports, Protocol और Services की पहचान करनी चाहिए और अन्य सभी को ब्लॉक करना चाहिए।
r) **भौतिक सुरक्षा:** भौतिक सुरक्षा लागू करके आईटी सिस्टम तक अनधिकृत पहुंच, physical damage और छेड़छाड़ को रोका जाना चाहिए। महत्वपूर्ण/संवेदनशील क्षेत्रों की निगरानी सीसीटीवी कैमरों के माध्यम से की जानी चाहिए और कम से कम 180 दिनों की फुटेज संग्रहीत की जानी चाहिए।

Technical Services UP Police

5.2. रिमूवेबल मीडिया सुरक्षा

a) पहली बार उपयोग से पहले रिमूवेबल मीडिया को Low Level Format करें।

b) रिमूवेबल मीडिया तक पहुँचने से पहले एंटीवायरस सॉफ़्टवेयर से स्कैन करें, फाइल्स/फोल्डर्स को Encrypt करें।

c) अपने दस्तावेज़ों को हमेशा Strong Password से सुरक्षित रखें।

d) किसी भी अनधिकृत डिवाइस पर रिमूवेबल मीडिया को प्लग-इन न करें।

e) अपनी खुद की डिवाइस लाओ (BYOD-Bring Your Own Device) को प्रतिबंधित किया जाना चाहिए और उच्च/संबंधित प्राधिकारी द्वारा authorisation के बिना किसी भी अज्ञात डिवाइस को नेटवर्क में अनुमति नहीं दी जानी चाहिए।

5.3. डेटा सुरक्षा

a) संवेदनशील/व्यक्तिगत डेटा की पहचान और वर्गीकृत करें तथा data at rest और data in transit के दौरान ऐसे डेटा को encrypt करने के उपाय लागू करें।

b) उचित प्रमाणीकरण/Authentication और प्राधिकरण/Authorization नियंत्रणों के साथ किसी भी डिफ़ॉल्ट/कमजोर/गलत कॉन्फ़िगर की गई सेटिंग्स की समीक्षा करें और बदलें।

c) Strong पासवर्ड और Multi-Factor Authentication (MFA) के उपयोग को लागू करने वाली नीतियां विकसित करें और बनाए रखें।

d) Personal Storage Devices, मीडिया उपकरणों को आधिकारिक/Official सूचना प्रणालियों या इन्फ्रास्ट्रक्चर से जुड़ने की अनुमति नहीं दी जानी चाहिए।

e) डेटा बैकअप नीति विकसित और क्रियान्वित करें। बैक-अप Process का दस्तावेजीकरण/Documented, Schedule और निगरानी की जानी चाहिए।

f) किसी आकस्मिक घटना की स्थिति में data loss को रोकने और तेजी से पुनर्प्राप्ति/Recovery सुनिश्चित करने के लिए सभी Business-Critical Data का नियमित रूप से बैकअप लिया जाना चाहिए।

g) सभी ऑपरेटिंग सिस्टम और एप्लिकेशन सॉफ़्टवेयर के लिए Original Disk/setup का एक सेट बनाए रखा जाना चाहिए जो यह सुनिश्चित करता है कि एक वैध, वायरस-मुक्त बैकअप मौजूद है और किसी भी समय उपयोग के लिए उपलब्ध है।

5.4. 3rd पार्टी एक्सेस और आउटसोर्सिंग

a) यह सुनिश्चित करना चाहिए कि third-party/बाहरी व्यक्ति की डाटा तक पहुंच प्रतिबंधित हो, और इसे केवल Non-Disclosure-Agreement पर हस्ताक्षर करने के बाद ही साझा किया जाना चाहिए।

b) उनकी साइबर सुरक्षा स्थिति/Posture, Data Management Process/Practices और उद्योग मानकों जैसे ISO 27001 के अनुपालन का आँकलन किया जाना चाहिए।

Technical Services, UP Police

c) विक्रेता/Vendor द्वारा एकत्र और Processed Data को उचित रूप से संरक्षित किया जाना चाहिए (विभाग की स्पष्ट सहमति / समझौते के बिना किसी अन्य के साथ साझा नहीं किया जाना चाहिए) और आवश्यकता पड़ने पर विभाग को उपलब्ध कराया जाना चाहिए।

d) बाहरी कर्मियों को संगठन की सूचना सुरक्षा नीतियों और प्रक्रियाओं का पालन करना चाहिए।

e) बायोमेट्रिक डिवाइस Standardisation Testing and Quality Certification(STQC) प्रमाणित होनी चाहिए।

5.5. पासवर्ड प्रबंधन / Password Management

a) बड़े अक्षरों, छोटे अक्षरों, संख्याओं और विशेष वर्णों के संयोजन का उपयोग करके, कम से कम 8 अक्षरों की लंबाई वाले जटिल पासवर्ड का उपयोग करें।

b) वाक्यांश/Phrases को प्राथमिकता दें और Bitwarden, Nordpass जैसी वेबसाइटों से Password Strength की जांच करें।

c) 2-3 माह में कम से कम एक बार पासवर्ड बदलें।

d) Multi-Factor Authentication (MFA) का उपयोग करें।

e) सभी वेबसाइट/ऐप में एक ही पासवर्ड का उपयोग न करें।

f) पासवर्ड को ब्राउज़र या किसी असुरक्षित दस्तावेज़ में सेव न करें।

g) किसी भी असुरक्षित सामग्री पर कोई भी पासवर्ड, IP Address, Network Diagram या अन्य संवेदनशील जानकारी न लिखें (उदाहरणस्वरूप Sticky/Post-it Notes, उपयोगकर्ता के टेबल पर सादा कागज पिन किया हुआ या पोस्ट किया हुआ आदि)

h) किसी भी अनधिकृत व्यक्ति के साथ सिस्टम पासवर्ड, प्रिंटर पास कोड या वाई-फ़ाई पासवर्ड साझा न करें।

Technical Services UP Police

5.6. मोबाइल सुरक्षा

a) सुनिश्चित करें कि मोबाइल OS (Operating System) नवीनतम Patch के साथ update किया गया है।

b) अपने मोबाइल डिवाइस को Root/Jailbreak न करें। यह प्रक्रिया कई अंतर्निहित सुरक्षा को अक्षम कर देती है और आपके डिवाइस को साइबर खतरों के प्रति Vulnerable बना देती है।

c) मोबाइल फोन पर Wi-Fi, GPS, Bluetooth, NFC और अन्य सेंसर को अक्षम/Disable रखें। आवश्यकता पड़ने पर ही इन्हें सक्षम/Enable किया जाना चाहिए।

d) Play Store (Android के लिए) और Apple App Store (iOS के लिए) से ही Apps download करें।

e) ऐसे किसी भी ऐप को डाउनलोड करने से पहले सावधानी बरतें जिसकी rating खराब हो या उपयोगकर्ता आधार/User-Base कम हो आदि।

f) किसी भी संवेदनशील चर्चा/बैठक में भाग लेते समय मोबाइल फोन स्विच ऑफ/ एयरप्लेन मोड में कर दें या मोबाइल को चर्चा कक्ष के बाहर किसी सुरक्षित क्षेत्र में छोड़ दें।

g) ब्लूटूथ पेयरिंग या फ़ाइल शेयरिंग के लिए किसी भी अज्ञात अनुरोध को स्वीकार न करें।

h) किसी ऐप को इंस्टॉल करने से पहले, प्रत्येक अनुमति के उद्देश्य व आवश्यक अनुमतियों को ध्यान से पढ़ें।

i) अगर कोई ऐप अपनी ज़रूरत से ज़्यादा अनुमति मांगे और उसका काम उस अनुमति से जुड़ा न हो, तो ऐसा ऐप इंस्टॉल न करें (जैसे कि Calculator App अगर GPS और Bluetooth की अनुमति मांगे)।

j) मोबाइल डिवाइस का 15-अंकीय IMEI नंबर नोट करें और इसे ऑफ़लाइन रखें। यह मोबाइल डिवाइस के Physical Damage/चोरी की स्थिति में रिपोर्टिंग के लिए उपयोगी हो सकता है।

k) फोन को स्वचालित रूप से लॉक करने के लिए auto lock का उपयोग करें या अपने मोबाइल फोन तक पहुंच को प्रतिबंधित करने के लिए Passcode/Security Pattern द्वारा संरक्षित Keypad Lock का उपयोग करें।

l) अपने फोन और मेमोरी कार्ड का नियमित ऑफ़लाइन बैकअप लें।

m) कंप्यूटर से मोबाइल पर डेटा ट्रांसफर करने से पहले डेटा को Latest Updated Antivirus से स्कैन करना चाहिए।

n) SMS या सोशल मीडिया आदि के माध्यम से भेजे गए किसी भी लिंक को खोलते समय सावधानी बरतें, खासकर जब लिंक से पहले रोमांचक ऑफ़र, लुभावने छूट या ताज़ा समाचार की जानकारी देने का दावा किया गया हो। ऐसे लिंक फिशिंग या मैलवेयर पेज पर ले जा सकते हैं, जिससे आपकी डिवाइस की सुरक्षा Compromised/Infected हो सकती है।

o) अपने फोन में Auto Download Disable करें।

p) हमेशा एक updated एंटीवायरस सॉफ्टवेयर रखें।

q) एप्लिकेशन द्वारा उपयोग की गई कोई भी Secret Key को Unencrypted संग्रहीत नहीं किया जाना चाहिए।

r) आंतरिक सरकारी दस्तावेज़ों को स्कैन करने के लिए किसी भी बाहरी मोबाइल ऐप आधारित स्कैनर सेवाओं (उदाहरण: कैम स्कैनर) का उपयोग न करें।

s) हवाई अड्डा, होटल या शॉपिंग सेंटर में निःशुल्क चार्जिंग स्टेशन का उपयोग करने से बचें अन्यथा **Juice Jacking** का शिकार हो सकते हैं जिसमें सार्वजनिक USB चार्जिंग स्टेशन से हैकर्स USB पोर्ट का फायदा उठा सकते हैं और डेटा ट्रांसफर करने, मैलवेयर इंस्टॉल करने या संवेदनशील जानकारी चुराने के लिए कर सकते हैं।

5.7. इंटरनेट ब्राउजिंग सुरक्षा

a) सरकारी एप्लिकेशन/सेवाओं, ईमेल/बैंकिंग/भुगतान संबंधी सेवाओं या किसी अन्य महत्वपूर्ण एप्लिकेशन/ सेवाओं तक पहुंचने के दौरान, हमेशा अपने ब्राउज़र में Private Browsing/Incognito/InPrivate Mode का उपयोग करें।

b) भुगतान संबंधी कोई भी जानकारी, पासवर्ड या अन्य संवेदनशील जानकारी इंटरनेट ब्राउज़र पर संग्रहीत न करें। यह हैकर्स का प्राथमिक लक्ष्य है।

c) 3rd Party VPN सेवाओं (जैसे: NordVPN, ExpressVPN, Tor, PROXY आदि) का उपयोग न करें।

d) अपने इंटरनेट ब्राउज़र में किसी 3rd Party Toolbar (उदाहरण: Download Manager, Weather Toolbar, Ask Me Toolbars आदि) का उपयोग न करें।

e) इंटरनेट से कोई भी अनधिकृत या Pirated Software, download न करें।

f) किसी भी गेम को इंस्टॉल करने या खेलने के लिए अपने आधिकारिक device का उपयोग न करें।

Technical Services UP Police

g) किसी भी छोटे/Tiny URL को खोलते समय सावधानी बरतें (उदाहरण: tinyurl.com/ab534/)। मैलवेयर और फिशिंग साइट्स, ऐसे लिंक से फिशिंग/मैलवेयर वेबपेज बनाकर आपका डिवाइस Compromise कर सकते हैं।
h) सुनिश्चित कर लें कि वेबसाइट्स/एप्लिकेशन वैध SSL/TLS प्रमाणपत्र के साथ "https" से Open हो रही हैं।
i) फिशिंग हमलों को कम करने के लिए पॉप-अप, अज्ञात ई-मेल और लिंक से बचें।

5.8. ईमेल सुरक्षा

a) सुनिश्चित करें कि NIC की मेल पर Multi-Factor Authentication कॉन्फ़िगर किया गया है।
b) किसी भी अनधिकृत व्यक्ति के साथ ईमेल पासवर्ड या ओटीपी साझा न करें।
c) Official Communication के लिए किसी भी अनधिकृत/बाहरी ईमेल सेवा का उपयोग न करें।
d) Unknown Sender द्वारा भेजे गए मेल में मौजूद किसी भी लिंक या अटैचमेंट को खोलें नहीं।
e) "Login Hisitory" टैब पर क्लिक करके NIC की ईमेल सेवा पर पिछली लॉगिन गतिविधियों की नियमित रूप से समीक्षा करें। यदि Login History में कोई विसंगति देखी जाती है, तो उसे तुरंत NIC-CERT-In को सूचित किया जाना चाहिए।
f) महत्वपूर्ण जानकारी वाले ई-मेल को encrypt करने के लिए PGP(Pretty Good Privacy) या Digital Certificate का उपयोग करें।
g) Macros वाले दस्तावेज़ डाउनलोड करते समय सावधानी बरतें। हमेशा "Macros Disabled" का विकल्प चुनें और यह सुनिश्चित करें कि MS Office जैसे ऐप्स में Protected Mode चालू हो।

5.9. सोशल मीडिया सुरक्षा

a) सोशल मीडिया का उपयोग करने से पूर्व विभाग की Social Media Policy को जरूर पढ़े।
b) सोशल मीडिया और नेटवर्किंग साइटों तक पहुंच के दौरान व्यक्तिगत जानकारी के उपयोग/प्रदर्शन को सीमित और नियंत्रित करें।
c) मित्र/संपर्क के रूप में किसी अनुरोध को स्वीकार करने से पहले हमेशा उस व्यक्ति की प्रामाणिकता की जांच करें।
d) सोशल मीडिया खातों को सुरक्षित करने के लिए Multi-Factor Authentication का उपयोग करें।
e) किसी भी अज्ञात संपर्क/उपयोगकर्ता द्वारा भेजे गए लिंक या फ़ाइलों पर क्लिक न करें।
f) किसी भी आंतरिक सरकारी दस्तावेज़ या जानकारी को सोशल मीडिया पर प्रकाशित, पोस्ट या साझा न करें।
g) सोशल मीडिया के माध्यम से कोई भी असत्यापित जानकारी प्रकाशित, पोस्ट या साझा न करें।
h) @gov.in/@nic.in ईमेल एड्रेस को किसी भी सोशल मीडिया प्लेटफॉर्म पर शेयर न करें।
i) आधिकारिक सोशल मीडिया प्लेटफ़ॉर्म खातों की पहुंच केवल नामित अधिकारियों और Systems तक ही सीमित होनी चाहिए।
j) आधिकारिक सोशल मीडिया प्लेटफ़ॉर्म के संचालन के लिए हमेशा एक Dedicated/अलग e-Mail Account का उपयोग करें।

Technical Services UP Police

k) आधिकारिक e-Mail Account/सोशल मीडिया प्लेटफ़ॉर्म के लिए हमेशा Credentials के एक अलग सेट का उपयोग करें जिसके Account Credentials, Password Policy के अनुसार होना चाहिए।

l) आधिकारिक सोशल मीडिया के संचालन के लिए व्यक्तिगत e-Mail account का उपयोग न करें।

m) सोशल मीडिया हैंडल पर पोस्ट की जाने वाली सामग्री को संगठन के भीतर सक्षम प्राधिकारी(Competent Authority) द्वारा अनुमोदित किया जाना चाहिए।

n) सार्वजनिक उपकरणों/अनधिकृत उपकरणों पर आधिकारिक सोशल मीडिया प्लेटफ़ॉर्म खातों का उपयोग न करें।

o) यदि कर्मचारी की भूमिका बदल जाती है या कर्मचारी संगठन छोड़ देता है तो आधिकारिक सोशल मीडिया खातों तक उसकी पहुंच समाप्त कर दें।

6. साइबर घटना/Incident रिपोर्टिंग

a) कृपया NIC CERT (https://niccert.nic.in) और CERT-In (https://www.cert-in.org.in) द्वारा प्रकाशित सुरक्षा सलाह देखें।

b) संदिग्ध मेल और फिशिंग मेल सहित किसी भी Cyber Security Incident की रिपोर्ट NIC-CERT (incident@nic-cert.nic.in) और CERT-In (incident@cert.org.in) को करें।

c) वित्तीय साइबर धोखाधड़ी से संबंधित शिकायत राष्ट्रीय हेल्पलाइन नंबर 1930 पर कॉल करके दर्ज की जा सकती है तथा शिकायत को बाद में विस्तृत विवरण के साथ https://cybercrime.gov.in/ पर पूरा किया जाना चाहिए।

d) साइबर सुरक्षा संबंधी अधिसूचनाओं/जानकारी के लिए निम्नलिखित संसाधनों का संदर्भ लिया जा सकता है:

SN	Resource URL	Description
1	https://www.meity.gov.in/cybersecuritydivision	Laws, Policies & Guidelines
2	https://www.cert-in.org.in	Security Advisories, Guidelines & Alerts
3	https://nic-cert.nic.in	Security Advisories, Guidelines & Alerts
4	https://www.csk.gov.in	Security Tools & Best Practices
5	https://cyberpolice.uppolice.gov.in/en	Cyber portal of UP Police for Security Advisories, Guidelines & Alerts
6	1930 & https://cybercrime.gov.in	Report Cyber Crime, Cyber Safety Tips
7	https://guidelines.india.gov.in/	Guidelines for Indian Government websites
8	https://cert-in.org.in/PDF/guidelinesgovtentities.pdf	Cyber Security Guidelines
9	https://i4c.mha.gov.in/awareness.aspx	Cyber Security Awareness
10	https://cytrain.ncrb.gov.in/staticpage/pdf/Cyber-security-tips-by-cyber-dost.pdf	Security Advisories, Guidelines & Alerts
11	e-Mail: adgts@nic.in & CUG: 9454400175	Nodal CISO, Uttar Pradesh Police

Ram Doot Singh
Cyber Security & SDC Team,
Technical Services, Uttar Pradesh Police

Naveen Arora, IPS
ADG, Technical Services &
CISO, Uttar Pradesh Police

Technical Services, UP Police

उत्तर प्रदेश पुलिस

National Crime Records Bureau
Ministry of Home Affairs
5th Conference
आज़ादी का अमृत महोत्सव

CISO साइबर सुरक्षा निर्देशिका

तकनीकी सेवायें, उत्तर प्रदेश पुलिस

e-Mail: adgts@nic.in

Website: https://uppolice.gov.in