INFORMATION SECURITY PLEDGE

Theme-4

Do's:-

- I shall make myself aware of the Information System Security policies of my bank and shall attend such awareness programs and when intimated to me.
- I shall not share password with any one.
- I shall change passwords at regular interval and keep very strong password with minimum of 8 alphanumeric characters.
- I shall make sure that anti-virus is installed and up to date on my computer.
- I shall make sure that all the discarded and obsolete records, old unused printouts will be shredded before disposed of.
- I shall make myself aware of the contact information of Helpdesk and Information Security team and shall inform immediately in case of any unauthorized activity noticed by me.
- I shall maintain records of any incidents/problems related to PC for future reference and for information security forensic purpose.
- I shall ensure that only minimum privileges are assigned to me to perform my duties.

Don't's:-

- I shall not write my passwords anywhere.
- I shall not use my official email id for personal use.
- I shall not click on link/ attachment from email unless I am sure that mail is from genuine source.
- I shall not disclose my organization related sensitive information on social media.

- I shall not use any unauthorized 3rd party video conferencing or collaboration tools for conduction sensitive organizational meetings.

- I shall not use any external mobile app based scanner (ex: Camscanner) for scanning organization's internal documents.
- I shall not use any external websites or cloud based services for converting/compressing organization's internal documents.
- I shall not leave my PC unattended whenever I am logged in.
- I shall not download any unauthorized software on my PC.
- I shall not use pen drive, unless it is scanned for virus.
- I shall not panic in case of any incidents, instead I shall inform incident/ crises management teams /helpdesk.
- I shall not do or allow tailgating/ piggybacking (a process where an unauthorized person follows an authorized individual to enter a secured premise) in office premises.
- I shall not use office computer resources for personal use.

*****

Payment Channels Security Tips

Theme-5

- Avoid creating common passwords and PIN for all your cards or payment apps.
- Do not choose password or PIN from your personal details e.g. DOB, Mobile no, name of close relatives.
- Close application/app after use.
- Do not install any remote control application in desktop/ mobile phone used for doing payments.
- Do not jailbreak or root your mobile phone used for doing payments.
- Never share your card related data, user name or password with anyone.
- Read OTP related messages carefully and ensure merchant name and amount before you enter OTP.
- Never share OTP with anyone.
- If your bank offers multi-factor authentication, opt for the same.
- Do not add fingerprint of other person on the device used for payment apps.
- If you lose connectivity of your mobile network, contact service provider immediately to avoid duplicate/cloning of SIM related frauds.
- Keep updated your mobile number and address in all the bank accounts.
- Do not fall prey to phishing/ vishing scam offering rewards or enforcing to dilute information in order to continue use of cards\ payment apps. Contact bank in case of doubt.
- Scanning QR codes only sends money and there is no way to receive money through the process.
- In any UPI app, PIN is only required to send money, to receive money PIN is not required.
- Do not share your account statement, details, balance with anyone unless it's necessary and after verifying the credentials of the person.
- Do not post any banking or related personal information on social media.
- Change your password/ PIN periodically even bank does not prompt for it.

*****

Work from Home Security Tips

Theme-6

1. Use Virtual Private Network (VPN) to connect to the network when you need to perform your work duties.
2. Do not share work data and information with your home computer or personal devices unless authorized by your organization.
3. Do not share your office device with friends and relatives.
4. Ensure your computer has up to date operating systems, applications and browser.
5. Ensure you have up-to-date anti-virus or malware protection software.
6. While sharing screen with other participants during remote sharing session, ensure you share necessary application window only rather full desktop or all content.
7. Avoid using any software which are not authorized by the organization.
8. Avoid using any social media or other sites not relevant to your work.
9. Remember essential cyber security best practices. Do not fall prey to phishing.
10. Ensure Wi-Fi and router security by a strong password, enabling WPA2 and other security setting.
11. Never connect to a public Wi-Fi network.
12. Even when you're working at home – do not leave your laptop unlocked and unattended.
13. Do not use any internet/cloud based file sharing services unless authorized.
14. Take back up regularly to the media authorized by the organization.

*****

सूचना सुरक्षा प्रतिज्ञा

विषय-4

करने योग्य:

- मैं अपने बैंक की सूचना प्रणाली सुरक्षा नीतियों के बारे में खुद को जागरूक करूंगा और जब मुझे सूचित किया जाएगा तो ऐसे जागरूकता कार्यक्रमों में भाग लूंगा ।
- मैं किसी के साथ पासवर्ड साझा नहीं करूंगा ।
- मैं नियमित अंतराल पर पासवर्ड बदलता रहूंगा और न्यूनतम 8 अल्फ़ान्यूमेरिक अक्षरों वाला बहुत मजबूत पासवर्ड रखूंगा।
- मैं यह सुनिश्चित करूँगा कि मेरे कंप्यूटर पर एंटी-वायरस स्थापित और अद्यतन है।
- मैं यह सुनिश्चित करूंगा कि सभी खारिज किए गए और अप्रचलित रिकॉर्ड, पुराने अप्रयुक्त प्रिंटआउट को निपटाने से पहले टुकड़े-टुकड़े कर दिए जाएंगे।
- मैं हेल्पडेस्क और सूचना सुरक्षा टीम की संपर्क जानकारी से खुद को अवगत कराऊंगा और मेरे द्वारा देखी गई किसी भी अनधिकृत गतिविधि के मामले में तुरंत सूचित करूंगा।
- मैं भविष्य में संदर्भ के लिए और सूचना सुरक्षा फोरेंसिक उद्देश्य के लिए पीसी से संबंधित किसी भी घटना/समस्या का रिकॉर्ड बनाए रखूंगा।
- मैं यह सुनिश्चित करूंगा कि मुझे अपने कर्तव्यों का पालन करने के लिए केवल न्यूनतम विशेषाधिकार दिए जाएं।

ऐसा न करें:

- मैं अपने पासवर्ड कहीं भी नहीं लिखूंगा ।
- मैं व्यक्तिगत उपयोग के लिए अपनी आधिकारिक ईमेल आईडी का उपयोग नहीं करूंगा।
- मैं ईमेल से आए लिंक/अटैचमेंट पर तब तक क्लिक नहीं करूंगा जब तक मुझे यकीन न हो जाए कि मेल वास्तविक स्रोत से आया है।
- मैं अपने संगठन से संबंधित संवेदनशील जानकारी सोशल मीडिया पर प्रकट नहीं करूंगा।
- मैं संवेदनशील संगठनात्मक बैठकों के संचालन के लिए किसी भी अनधिकृत तृतीय पक्ष वीडियो कॉन्फ्रेंसिंग या सहयोग उपकरण का उपयोग नहीं करूंगा।
- मैं संगठन के आंतरिक दस्तावेजों को स्कैन करने के लिए किसी बाहरी मोबाइल ऐप आधारित स्कैनर (उदा: कैम स्कैनर) का उपयोग नहीं करूंगा।
- मैं संगठन के आंतरिक दस्तावेजों को परिवर्तित/संपीड़ित करने के लिए किसी बाहरी वेबसाइट या क्लाउड आधारित सेवाओं का उपयोग नहीं करूंगा।
- जब भी मैं लॉग इन रहूँगा तो मैं अपने पीसी को अप्राप्य नहीं छोड़ूँगा।
- मैं अपने पीसी पर कोई भी अनधिकृत सॉफ्टवेयर डाउनलोड नहीं करूंगा।
- मैं पेन ड्राइव का उपयोग नहीं करूंगा, जब तक कि इसे वायरस के लिए स्कैन न किया गया

हो।

- किसी भी घटना की स्थिति में मैं घबराऊंगा नहीं, बल्कि घटना/संकट प्रबंधन टीमों/हेल्पडेस्क को सूचित करूंगा।
- मैं कार्यालय परिसर में टेलगेटिंग/पिग्गी बैकिंग (एक ऐसी प्रक्रिया जहां एक अनधिकृत व्यक्ति किसी अधिकृत व्यक्ति के पीछे एक सुरक्षित परिसर में प्रवेश करता है) नहीं करूंगा या इसकी अनुमति नहीं दूंगा।
- मैं व्यक्तिगत उपयोग के लिए कार्यालय के कंप्यूटर संसाधनों का उपयोग नहीं करूंगा।

*****

भुगतान चैनल सुरक्षा सुझाव

विषय-5

- अपने सभी कार्ड या भुगतान ऐप्स के लिए सामान्य पासवर्ड और पिन बनाने से बचें।
- अपने व्यक्तिगत विवरण जैसे जन्मतिथि, मोबाइल नंबर, करीबी रिश्तेदारों का नाम से पासवर्ड या पिन न चुनें।
- उपयोग के बाद एप्लिकेशन/ऐप को बंद कर दें।
- भुगतान करने के लिए उपयोग किए जाने वाले डेस्कटॉप/मोबाइल फोन में कोई भी रिमोट कंट्रोल एप्लिकेशन इंस्टॉल न करें।
- भुगतान करने के लिए उपयोग किए जाने वाले अपने मोबाइल फोन को जेलब्रेक या रूट न करें।
- अपने कार्ड से संबंधित डेटा, उपयोगकर्ता नाम या पासवर्ड कभी भी किसी के साथ साझा न करें।
- ओटीपी से संबंधित संदेशों को ध्यान से पढ़ें और ओटीपी दर्ज करने से पहले व्यापारी का नाम और राशि सुनिश्चित कर लें।
- ओटीपी कभी भी किसी के साथ साझा न करें।
- यदि आपका बैंक बहु-कारक प्रमाणीकरण प्रदान करता है, तो उसे चुनें।
- भुगतान ऐप्स के लिए उपयोग किए जाने वाले डिवाइस पर किसी अन्य व्यक्ति का फिंगरप्रिंट न जोड़ें।
- यदि आप अपने मोबाइल नेटवर्क की कनेक्टिविटी खो देते हैं, तो सिम संबंधी धोखाधड़ी/डुप्लिकेट से बचने के लिए तुरंत सेवा प्रदाता से संपर्क करें।
- सभी बैंक खातों में अपना मोबाइल नंबर और पता अपडेट रखें ।
- कार्ड/भुगतान ऐप्स का उपयोग जारी रखने के लिए पुरस्कारों की पेशकश करने वाले या जानकारी को प्रदान करने के लिए मजबूर करने वाले फ़िशिंग/विशिंग घोटाले का शिकार न बनें। संदेह होने पर बैंक से संपर्क करें ।
- क्यूआर कोड को स्कैन करने से केवल पैसे भेजे जाते हैं और इस प्रक्रिया के माध्यम से पैसे प्राप्त करने का कोई तरीका नहीं है।
- किसी भी UPI ऐप में सिर्फ पैसे भेजने के लिए पिन की जरूरत होती है, पैसे पाने के लिए पिन की जरूरत नहीं होती है ।
- अपने खाते का विवरण, जानकारी , शेष राशि किसी के साथ तब तक साझा न करें जब तक कि यह आवश्यक न हो और व्यक्ति की साख सत्यापित करने के बाद ही।
- सोशल मीडिया पर कोई भी बैंकिंग या संबंधित व्यक्तिगत जानकारी पोस्ट न करें।
- अपना पासवर्ड/पिन समय-समय पर बदलते रहें, भले ही बैंक इसके लिए संकेत न दे।

*****

घर से काम - सुरक्षा युक्तियाँ

विषय-6

1. जब आपको अपने कार्य कर्तव्यों का पालन करने की आवश्यकता हो तो नेटवर्क से जुड़ने के लिए वर्चुअल प्राइवेट नेटवर्क (वीपीएन) का उपयोग करें।
2. जब तक आपके संगठन द्वारा अधिकृत न किया जाए, अपने घरेलू कंप्यूटर या व्यक्तिगत उपकरणों के साथ कार्य डेटा और जानकारी साझा न करें।
3. अपने कार्यालय उपकरण को दोस्तों और रिश्तेदारों के साथ साझा न करें।
4. सुनिश्चित करें कि आपके कंप्यूटर में अद्यतन ऑपरेटिंग सिस्टम, एप्लिकेशन और ब्राउज़र हैं।
5. सुनिश्चित करें कि आपके पास नवीनतम एंटी-वायरस या मैलवेयर सुरक्षा सॉफ़्टवेयर है।
6. रिमोट शेयरिंग सत्र के दौरान अन्य प्रतिभागियों के साथ स्क्रीन साझा करते समय, सुनिश्चित करें कि आप केवल आवश्यक एप्लिकेशन विंडो साझा करें, न कि पूर्ण डेस्कटॉप या सभी सामग्री।
7. किसी भी ऐसे सॉफ़्टवेयर का उपयोग करने से बचें जो संगठन द्वारा अधिकृत नहीं है।
8. किसी भी सोशल मीडिया या अन्य साइटों का उपयोग करने से बचें जो आपके काम से प्रासंगिक नहीं हैं।
9. आवश्यक साइबर सुरक्षा सर्वोत्तम प्रथाओं को याद रखें। फ़िशिंग का शिकार न बनें.
10. WPA2 और अन्य सुरक्षा सेटिंग सक्षम करके एक मजबूत पासवर्ड द्वारा वाई-फ़ाई और राउटर सुरक्षा सुनिश्चित करें।
11. कभी भी सार्वजनिक वाई-फाई नेटवर्क से कनेक्ट न करें।
12. यहां तक कि जब आप घर पर काम कर रहे हों तब भी - अपने लैपटॉप को अनलॉक और अकेला न छोड़ें।
13. जब तक अधिकृत न हो, किसी भी इंटरनेट/क्लाउड आधारित फ़ाइल साझाकरण सेवाओं का उपयोग न करें।
14. संगठन द्वारा अधिकृत मीडिया के पास नियमित रूप से अपना बैकअप रखें।

*****