Namdev Finvest Private Limited

Har Pal Aap Ke Saath ..

General Computer Usage	
DOs	**DON'Ts**
Always download applications and software from trusted sources.	Do not install or use pirated copies of software /Applications under any circumstances. These may contain malware
Regularly update the operating system and application. and Anti-Virus software of the system.	Do not use guessable/weak passwords like “password@123", etc.
Ensure backup of important data, files, and documents at regular intervals.	Do not click on untrusted/unexpected Pop-Up advertisements/ programs
Lock the computer screen when not in use.	Do not dispose of a computer or hard drive without wiping and deletion of data
Always keep the computer firewall “on.”	
Scan all the files/contents downloaded from websites, e-mails, or USBs."	
Uninstall unnecessary programs or software	

Avoid public Wi-Fi	
DOs	**DON'Ts**
Make sure the Public Wi-Fi you are using has a valid VPN.	Don't use any public Wi-Fi if it's not having a valid VPN.
Use a Mobile network or any other connection if public Wi-Fi does not have a valid VPN.	Don't enable your Bluetooth and Wi-Fi in every public place you visit.

Namdev Finvest Private Limited

Har Pal Aap Ke Saath ..

Take caution regarding data security	
DOs	**DON'Ts**
Be accountable for your IT assets and data	Don’t store sensitive information in the portable device without strong encryption.
Adhere to Policies on the Use of IT Services and Resources	Don’t leave your computer / sensitive documents unlocked.
Use good judgment to protect your data	Don’t discuss something sensitive in a public place. People around you may be listening to your conversation.
Protect your laptop during the trip	
Ensure sensitive information on the computer screen is not visible to others Protect your user ID and password	

Password security Management	
DOs	**DON'Ts**
Use complex passwords.	Don’t use the same password in multiple services/websites/apps.
Change your passwords at least once in 45 days.	Don’t save your passwords or any unprotected documents in the browser.
use different passwords for different accounts. If one password gets hacked, your other accounts are not compromised.	Don’t write down any passwords, IP addresses, network diagrams, or other sensitive information on any unsecured.
	Don't share your password with any other person.

Namdev Finvest Private Limited

Har Pal Aap Ke Saath ..

Recognize internet-based commerce/ E commerce	
DOs	**DON'Ts**
Check the terms and disclaimers of an e-shopping site before acquiring its service.	Don’t make any e-shopping transactions using computers in an Internet café
Choose well-known or trustworthy e-shopping sites.	Don't visit untrustworthy sites out of curiosity
Check the trustworthiness of the e-commerce website (e.g. checking the SSL certificate) Use digital certificates for executive transactions over the web	Don’t use easily guessed passwords, such as HKID card number, phone number, date of birth
Use a strong password, and change your password regularly.	
Logout immediately after you finish your e-shopping activities.	
Retain and review your transaction records.	
Use different passwords for bank accounts, university accounts, and external accounts.	

Guidelines for using public computers	
Dos	**DON'Ts**
Always reboot when starting to use public PCs.	Don’t leave without closing all browsers and logging out from public PCs.
Clean up cache files after use.	Don't let others watch over your shoulder while logging in or doing online transactions.
Use company-allocated Desktop and Laptop for official work.	Personal Devices like Laptops and tablets are prohibited on office premises.

Namdev Finvest Private Limited

Har Pal Aap Ke Saath ..

General Internet Safety Precautions	
DOs	**DON'Ts**
Validate the website you are accessing	Don't download data from doubtful sources.
Install personal Firewall	Don't visit untrustworthy sites out of curiosity, or access the URLs provided on those websites.
Be cautious if you are asked for personal information.	Don't use illegal software and programs.
Use encryption to protect sensitive data transmitted over public networks and the Internet.	Don't download programs without permission from the IT team.
Install anti-virus, perform scheduled virus scanning, and keep virus signature up-to-date. Apply security patching in a timely.	
Backup your system and data, and store it securely.	

Email Security Practices	
DOs	**DON'Ts**
Do scan all email attachments for viruses before opening them.	Don't open email attachments from unknown sources.
Use email filtering software.	Don't send mail bomb, forward or reply to junk email or hoax message.
Only give your email address to people you know.	Don’t click on links embedded in spam mail
Use digital certificates to encrypt emails that contain confidential information staff can use confidential email.	Don’t buy things or make charity donations in response to spam email.
Use a digital signature to send emails to prove who you are.	Don't respond or reply to spam in any way.
If you receive a suspicious email, the best thing to do is to delete the message and report it to your IT team. Always check the " From" field to validate the sender.	