Annexure – COC (Cybersecurity)

Group Cybersecurity - *Do's and Don'ts*

Objective

Taghleef is in the process of uploading ethical policies in the Ti website for internal and external usage. All the Ti Units are required to include the Cybersecurity Do' and Don'ts as part of the Employee COC (Code of Conduct) detailed in the following section and upload the same.

Details

Employees as well as external users are responsible for the Information security, in particular Cybersecurity for safeguarding the confidentiality and integrity of the Taghleef information and assets.

The below actions (Do's and Don'ts) should be complied while using the Information communication technology environment of Taghleef.

Do's

1. Should Use passwords that are not common for a hacker to guess and try to log into your systems. Always, use different passwords for different accounts. If one password gets hacked, your other accounts are not compromised.
2. Should keep your passwords or passphrases confidential and cannot be shared with anyone at any point in time.
3. Should pay attention to caution & phishing traps, links in email and watch for telltale signs of a scam. Especially when the caution in email reads it is an external email, If you receive a suspicious email, the recommended action is forward to IT, delete the message, and report to IT department /IT Helpdesk support and to the supervisor as relevant immediately to avoid further damage.
4. Should destroy information that are on hard copies and that are no longer needed. Use the designated confidential destruction bins throughout the office or use a crosscut

shredder for shredding the confidential documents. For all electronic storage media, please do consult with IT.

5. Before procuring the s/w, application, or tool, should contact IT to verify, approve if the s/w or application or tool is safe and secured to be used in Ti's IT environment.
6. Should be sensitive of your surroundings when printing, copying, faxing, or discussing confidential information. Should pick up printed documents from printers, copiers, or faxes without letting them lie on the printer, copier, or fax machines.
7. Ensure to lock your computer and mobile phone when not in use. This protects the data from unauthorized access and use.
8. Please do remember that wireless is inherently insecure. Should avoid using public Wi-Fi hotspots for Taghleef assets. When you must, use agency provided virtual private network software to protect the Taghleef data and the device. If in doubt, please reach out to your respective IT resources.
9. Should report all suspicious activity and cyber incidents to your Manager, IT department and other department as relevant.
10. Should keep all areas containing sensitive information physically secured and allow access by authorized individuals only. Part of your job is making sure Ti's data to be properly safeguarded, and is not damaged, lost or stolen.
11. Social media access should be avoided in general but if your job role need an access to the social media sites then you should use privacy settings on social media sites to restrict access to your personal information as well as official information.

Don'ts

1. Should not share the password with others or write them down. You are responsible and accountable for all activities associated with your credentials and will be held accountable in case of an incident related to your computers and phones
2. Should not open mail or attachments from an untrusted source.
3. Should not leave sensitive information lying around the office.
4. Should not leave printouts or portable media containing private information on your desk. Lock them in a drawer to reduce the risk of unauthorized disclosure.

Annexure – COC (Cybersecurity)

5. Should not post any private or Taghleef sensitive information, such as credit card numbers, passwords, or other private information, on public sites, including social media sites, and send it through email unless authorized to do so.
6. Should not click on links from an unknown or untrusted source, do not ignore the caution in the email. Cyber attackers often use them to trick you into visiting malicious sites and downloading malware that can be used to steal data and damage networks.
7. Should not be tricked into giving away confidential information. It's easy for an unauthorized person to call and pretend to be an employee or business partner. Don't respond to phone calls or emails requesting confidential data.
8. Should not try to procure or install unauthorized programs on your work computer without verification and approval from IT. Malicious applications often pose as legitimate software.
9. Should not plug in portable devices without permission of your Manager & verification of the device by IT department. These devices may be compromised with code just waiting to launch as soon as you plug them into a computer.
10. Should not leave devices unattended. Keep all mobile devices, such as laptops and cell phones physically secured. If a device is lost or stolen, report it immediately to the IT support, your manager and other department as relevant.
11. Should not leave wireless or Bluetooth turned on when not in use. Only do so when planning to use and only in a safe environment.
12. Should not use official assets for personal purpose

The Ti/Taghleef Information Technology team is dedicated to protecting Ti privacy; safeguarding Ti's information assets, data, and infrastructure; identifying and mitigating vulnerabilities; detecting, responding, and recovering from cyber incidents; and promoting cyber awareness.

Remember - cyber security is everyone's responsibility

Annexure – COC (Cybersecurity)

Employee Acknowledgement:

I hereby confirm to comply with all provisions of the Code of Conduct along with the details mentioned in the Annexure – COC (Cybersecurity).

Name	:	Employee No.	:
Signature	:	Date	: