

# Information Security Golden Rules

**TIM- TÇX**



## Handle information with care

- 1 Lock your computer when you leave your desk
- 2 Don't leave sensitive data unattended
- 3 Prevent others from looking at your screen
- 4 Dispose of documents containing sensitive information in shredders or containers



## Protect your password and computer

- 1 Use unique, strong passwords, do not share them with anyone, change them regularly
- 2 Use different passwords for all your accounts
- 3 If your system is compromised, change your password immediately



## Communicate with caution

- 1 Only share information on a need-to-know basis, inside and outside the organization
- 2 Handle personal data with great care, particularly when distributing via mail
- 3 Discuss business and/or confidential information in a private area



## Take care when using e-mail, internet and social media

- 1 Use e-mail, social media and the internet responsibly and cautiously
- 2 Don't download documents and material from untrusted parties or e-mail addresses
- 3 Only send documents to reliable e-mail addresses

## Protect your mobile devices



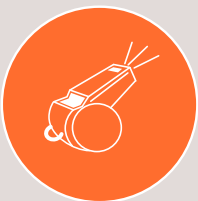
- 1 Set up a PIN or password on your devices
- 2 Lock your devices when not in use
- 3 Always keep your mobile devices in sight, never leave them in the car (boot)
- 4 Regularly connect with the company network and install the latest updates
- 5 Only use secure networks and VPN

## Keep our premises secure



- 1 All visitors to the KIT should be registered and escorted in and out
- 2 Pay attention to unaccompanied / unknown visitors or individuals
- 3 Your access badge is strictly personal, do not lend them to anyone

## Always report Information Security incidents



- 1 If you believe you received a phishing e-mail forward the message to Constant IT helpdesk and the Information Security Officer (ISO)
- 2 If you clicked on a link within a suspected phishing email, downloaded an attachment or filled in credentials, report it immediately to the Constant IT helpdesk and the ISO
- 3 Immediately report the lost and/or damaged mobile device or laptops used for business to the Information Security Officer, Constant IT service desk and to the police (for insurance purposes)
- 4 Report any found mobile device or laptop to the ISO
- 5 Report any suspicious activities on your laptop to the Constant IT helpdesk

## Read the relevant TCX information security related documents



- 1 HR Guide's chapter on information security
- 2 TIM Internal > Information Security > Employee documents
- 3 You will be informed of any new documents and updates to existing documents