

SECURE INFORMATION SYSTEMS

USER ID AND PASSWORD

- Your user ID and password are always personal. Never disclose your user credentials to others or save them to a location where others could use them.
- Workplace user IDs and passwords may only be used for performing work duties. The user credentials should never be used for personal purposes such as signing up to online services.



EQUIPMENT

- Never give your devices to external parties or leave them unattended. Lock your computer when leaving the workstation or its vicinity.
- Keep your laptop, tablet and phone in a secure place and exercise care when on the move with them.
- Work equipment are intended only for performing work duties, and work-related data may only be saved on the organisation's information systems, devices and data storage media.

DATA PROTECTION

- When processing personal data, exercise care and protect the privacy of data subjects.
- The processing of personal data must always have legal basis. If you are unsure about the legality of personal data processing, contact your superior or the organisation's data protection officer.
- Disclosing personal data has to be done lawfully. Prior to disclosing data, always verify the identity of the recipient and find out whether they have the right to process the data.



SUSPECT A BREACH?

If you suspect that the security of data or personal data is threatened, contact immediately the person responsible for your organisation's data security:

