Cyber security is everyone's responsibility

We work together to protect our business and customers

ACCEPTABLE USE

FOR DIGITAL ASSETS

Do not attempt

to bypass or disable the security measures in your computer to access content that can put the company at risk, such as visiting blocked websites.

Do not install

or use applications not authorised by the company.

Do not share

your corporate username and password with anyone, including colleagues or third parties.

Do not click

on suspicious links or attachments in emails. When in doubt, report.

Remember

- Cybercriminals take advantage of **human error or non-compliance** in their cyberattacks. Ninety-five percent of **cybersecurity breaches** are caused by human actions.
- **Unconfiguring** your antivirus, installing **pirated software** or **using VPNs** to bypass your computer's controls are some actions that threaten your company's security.

- Use the **corporate application installer** to securely access the tools provided by the company.
- If you need other specific applications or programmes for your work, **use ITNow** to request **individual authorisation for each of them**.
- **Do not use alternative browsers** or access the internet to download or enter prohibited and unsecure websites. These websites are frequently visited by **cybercriminals** and put your computer at serious risk.

- Your corporate username and password are **private and are never to be shared**. They are for your use and protection: **do not give them away**.
- The **reuse** of credentials and your corporate email in other systems and personal services is **prohibited**.
- Do not forget that you **should not write down** your blocker passwords or corporate credentials on post-it notes or notebooks.

- **Email phishing attacks** are the main entry point for **cyber-attacks on companies**.
- Always **check the authenticity of the sender**. If in doubt, verify it by contacting the sender through another channel, e.g., by calling them on the phone.
- Recognise the **warning signs** of these scam attempts, such as messages with urgent requests or threats, and grammatical or design errors.