CYBERSECURITY

1. We remember that awareness of threats and appropriate actions are crucial for the security of our data and devices online, as well as for the organization in which we work.

2. We remember to regularly update the application software and operating systems used in the organization.

3. We comply with the principles of the GDPR - we know our rights and obligations arising from the provisions on the protection of personal data.

3. We do not leave our unlocked devices unattended. We block the access so that no unauthorized person could use them during our absence.

4. We try to be careful on social media - being wary of what we share online, as it can be used to create a fake profile.

5. We use secure internet networks or use encrypted VPN when we connect to publicly available, unknown wireless WI-FI networks (e.g. in hotels, restaurants, bars, etc.).

6. We always use anti-virus and anti-spam software with enabled automatic update of anti-virus database and at least a firewall built in the operating system.

7. We do not share sensitive data about employees or organization in public places in the presence of third parties (e.g. smoking, on a train, etc.).

8. We use unique, complexity appropriate passwords (containing upper and lower case letters, numbers, special characters, e.g. #,$,!).

9. We do not plug in unknown mass storage devices, e.g. a flash drive being found or donated by a contractor, as well as phones, portable drives, etc., into the company computers.

10. We carefully read the messages and notifications appearing while logging. We remember that cybercriminals can fake internet websites.

We notify the IT department when:

- there is any suspicious activity on the website view;
- we notice its unusual behaviour;
- website is deceptively similar to the original one;
- website name contains misspellings or letters merge into a sequence of characters being similar to the ones on the original website.

11. We are wary of phishing, as these are attempts to extort users' personal data and log-in credentials to websites, e.g. electronic banking or IT systems used by our organization. Most often, this threat takes the form of specially crafted messages sent via e-mail, with the same principle as with website fraud, being deceptively similar to the original sender's email addresses and may contain misspellings or merging letters into a sequence of characters being similar to the original email addresses.

12. We never send unencrypted sensitive data via the public internet network that can be used for identity theft (personal ID number, ID card number, etc.).

Phishing – *is a method of fraud in which a criminal impersonates another person or institution in order to obtain confidential information, infect a computer with malware or persuade the victim to perform specific actions. It is a type of attack based on social engineering.*