PRODIGY
Making IT Smart

User Guidelines – Secure Work in the Organizational Network

• To maintain organizational information security and prevent breaches, fraud, and potential damage, all users must follow these critical guidelines. Due to the increasing use of AI tools, special attention should be paid to the risks associated with them.

Common Threat Vectors:

1. Email (Phishing & Fraud):

• - Do not open suspicious emails, attachments, or links – even from familiar senders.

• - Do not reset passwords or provide personal information without Helpdesk approval.

• - Ignore and report emails that contain fear-based or blackmail content.

2. Malicious Websites & Software:

• - Do not browse websites flagged by your browser as unsafe.

• - Avoid downloading software or files from unknown sources.

• - Do not approve pop-up windows on unfamiliar websites.

3. Phone Scams (Social Engineering):

• - Never provide information or allow remote access to someone claiming to be from Microsoft or any external provider.

• - Report all such attempts to the Helpdesk.

4. Using AI Tools (ChatGPT, Copilot, Gemini, etc.):

• - Never input sensitive, private, or internal business data into AI tools.

• - Do not share internal or organizational data with third-party platforms.

• - Verify all AI-provided information before relying on it – mistakes may cause damage.

• - Only use AI tools with prior approval from your IT department.

Additional Security Tips for Organizational Devices:

• - Keep your operating system and software up to date.

• - Ensure antivirus (e.g., ESET) is running and updated.

• - Do not connect to public Wi-Fi without using VPN.

• - Do not use your work email to register for untrusted external websites.

• - Use unique, strong passwords for each platform (including symbols, upper/lowercase letters, numbers).

• - Enable Two-Factor Authentication (2FA) on all possible accounts.

• - Do not upload company files to private cloud storage (Dropbox, Google Drive, etc.) unless approved by IT.

What to Do If You Suspect a Security Incident:

• - If files appear with strange extensions or won't open – disconnect from the network and contact the Helpdesk immediately.

• - If you receive a suspicious email or experience anything unusual – report it immediately.

• Remember: Information security is everyone's responsibility.

• Best regards,

• Prodigy Team