Cyber Security Policy

- Keep Your Operating System and Software Up to Date
- Avoid clicking on unknown, unnecessary links
- Use Anti-Virus in your system
- Avoid revealing your personal information to any unknown person whether on-premises or off-premises

- Do not login with your credentials on any unknown device
- Avoid unsecured/public WI-FI access
- Avoid using company's device for personal use
- Follow company's policy and procedures
- Do not use personal devices for work purposes without a formal Bring Your Own Device policy

- Do not use unofficial communication tools for work (Slack, Discord, etc.)
- Do not install any applications on company devices without the explicit approval of your IT department
- Be aware of phishing and social engineering

Password Security

- Do not reuse passwords. If a data breach ever leaks one of your accounts, the attacker could gain access to other accounts using your reused passwords.

- Use company-provided authentication measures such as a password manager or Identity Access Management (IAM) solution.
- Do not leave passwords in an insecure location such as a post-it notes, journal, or unencrypted text file.
- Do not share your passwords or accounts with anyone, not even with your coworkers. Every employee must have their own unique login credentials so that their activity can be accurately monitored and managed by the IT department.
- Make long and simple passwords. Think of your password as more of a *passphrase*. Use a series of unrelated words to create long, simple passwords rather than short and complex ones. Passphrases are easier for you to remember and harder for attackers to brute force or guess.
- Leverage the most secure multi-factor authentication method available to you such as an authenticator app; avoid knowledge-based MFA as these methods are vulnerable to being disclosed via social engineering and open-source intelligence.

Physical Security

- Lock your workstation whenever you will not be physically present.
- Do not leave mobile devices unattended. This includes leaving devices in your car, in checked luggage, or on a table of a coworking space or coffee shop.
- Do not provide anyone with unauthorized access to the premises. If they need access they should have been provided with a designated contact.
- If a door requires a keycard or similar device to get in, ensure that you close the door behind you rather than holding it open for someone else.
- Keep any secure cabinets locked at all times; do not leave them unlocked unless you are immediately accessing its contents.

- Keep any keys, keycards, ID badges, or related access tools on you at all times.

USB Security

- Do not store sensitive or confidential data on any portable storage device. These devices are easily lost or stolen, making them a valuable target for hackers.

- Follow your organization's data security policies. They may include encryption requirements, specific procedures for USB devices, and designated devices.
- Do not insert unknown USB devices into company computers. The organization has policies and procedures surrounding USB devices such as requiring that they are scanned for malware using an air-gapped computer.
- Only use company-authorized USB devices. Do not bring personal USB flash drives to work and avoid using any USB devices that have been provided at conferences or trade shows unless they have been approved by your IT department.
- Do not bring company-provided USB devices home with you without prior approval and a legitimate need to do so. Instead, keep it locked in a secure cabinet in your workplace.
- Do not plug company-provided USB devices into personal computers. If your computer is infected with malware, it could transmit it to your company's network.