- **Update OS and Software**: Ensure the operating system and all software are updated with the latest security patches.

- **Install Antivirus Software**: Choose reliable antivirus software and ensure it’s always updated.

- **Enable Firewall**: Make sure the firewall is enabled to block unauthorized access.

- **User Account Management**: Set up a unique user account for the new employee with appropriate access levels. Avoid using the administrator account for daily tasks.

- **Strong Passwords**: Enforce the company’s strong password policy and ensure MFA is enabled.

- **Encrypt Data**: Use encryption for sensitive data and enable full-disk encryption if possible.

- **Backup Solutions**: Set up regular backups for important data. Ensure they are automated and tested regularly.

- **Browser Security**: Install security plugins/extensions and configure browser settings to enhance security.

- **Email Security**: Educate the new employee on recognizing phishing emails. Ensure email security protocols are in place.

- **Secure Network Connection**: Make sure the workstation connects via a secure network. Use VPNs when connecting remotely.

- **Disable Unnecessary Services**: Turn off non-essential services to reduce potential entry points for attackers.

- **Physical Security**: Ensure the physical security of the workstation, such as locking the computer when not in use and securing portable devices with locks.