Security Tips

- Change your password frequently.
- Always logout.
- Do not share your password to anyone.
- Do not select the option auto save option on browsers for storing username and password.
- If you notice any suspicious activity in your MIMIS account please inform us immediately by calling to TANHODA.
- Make use of effective and updated antivirus.
- Avoid Public computers and networks.
- Do not type your password, authentication code, one time password (OTP) other than the space provided on our site.
- Do not click on login link in emails.
- You are advised not to use any personal data such as name or mobile number or sequential numbers or any keywords for your MIMIS Passwords.
- Keep your Computers and Mobile numbers from malware.
- You should not use public or shared computer like those in Internet cafes or a third-party computer for MIMIS software as you may be open to harmful or specific programs enabled within these computers, which could capture your information.
- Avoid using third party computer for MIMIS application. If used, ensure clearance of cache and history from browser after you have finished.
- Dear user, do not install any remote access application on your mobile. Never respond to any calls that ask you to share application code/OTP/passwords of applications installed on your mobile with anyone.