Security Policy For National Eye Database - NED Web Application

Introduction

This document has been produced to ensure that:

- High level security in terms of patients confidentiality, centre confidentiality, integrity and availability of data information is maintained at all time.
- All Source Data Provider (SDP) and site coordinators are aware of their authority and accountabilities as stated in the Authorization List.

Management

A) User Level

1. Do not disclose your user ID or password to anyone else
2. Do not give your mobile phone to anybody else while logging into the web application.
3. Log in the pin number immediately after receiving the number via SMS.
4. Users are responsible to update/edit their own center data.
5. Should the user lose their mobile phone or change a new mobile phone number please notify:
   NED Database Administrator: **+(603) 4041 8615 / 4051 2296**
   NED Manager: **+(603) 612 63333 extension 4060**
6. Password management as per Appendix A (Security Practices)
7. Should the user forget their password, please fill in the web form at the **Forgot Password** link at log in page of the web application.

B) Centre/Institution Level

1. Agree to allow other authorized users within the same institution as per Authorization List for their specific responsibilities.
2. Ensure that your database is updated regularly to maintain its real-time accuracy.
3. Agree to share aggregate data from your centre for the purpose of research by qualified researchers, or for any other purpose by persons demonstrating a need to access NED's database following approval by the Technical Committee of NED.
4. The SDPs themselves hold sole responsibility with regards to data release of their own patients to any third party.

I HEREBY ACKNOWLEDGE AND ACCEPT that my access and use of Web Application shall be governed by this Security Policy.

_____

Signature

Name: _____

Institution Name: _____

Email Address: _____

Date: _____

Appendix A

Security Practices

As a good security practice you are strongly advised to:

Keep your password confidential!

- **Avoid** sharing or divulging your Password to anyone. This includes any person who may appear to represent or work for the Registry. Our administrator never requires your password at any time.
- **Avoid** using the same Web Application Password for any other web-based services such as for e-mail or for Internet Service Provider login.
- **Avoid** choosing a Password that is easily anticipated by a third party, like your NRIC number, telephone number, date of birth, etc.. You should select a unique Password to make it difficult for anyone to anticipate.
- **Avoid** writing down or saving your Password on your browser or any other software. Memorize your Password.
- If you suspect your Password may have been compromised, change your Password immediately.

Ensure you are accessing the correct website!

- Never access the website via a hyperlink from an e-mail. Always enter the correct website address yourself. Which is either **www.acrm.org.my/ned**

Only access Web Application using a secure and trusted computer!

- **Never** access your Web Application on Computers/devices which you have doubts with regard to security, such as those located in public places. If you have to use computers (for example, when you are on trips), change your password once you have access to a secure computer.
- Keep your operating system (e.g. Microsoft Windows) and Internet-related software updated with the latest security patches.
- Protect your computer from viruses and malicious programs with anti-virus software and firewalls where possible. Always update your anti-virus software with the latest virus signatures.
- Always log out your online session by clicking on the "logout" button whenever you leave your computer, even for a short while. Do not simply close the browser window when you wish to end the Web Application session.

For further information on the above, or any aspect of Internet security, please contact our Administrator helpdesk at:
NED Database Administrator: **+(603) 4041 8615 / 4051 2296**