Script 20 – Digital Security

Our Mission, Your Pension Data Security.

Keeping the Fund’s information systems safe from all digital threats is an important part of the Fund’s mission. The Fund has a Unit dedicated to overseeing all types of risk, including an Information Security Officer and a Risk Officer. The Fund is prepared for all types of attacks from hackers. In order to prevent these attacks, the Fund has in place security measures such as firewalls, anti-malware solutions, strong authentication mechanisms, etc. – and the most important thing…the Fund remains constantly vigilant.

The Funds’ preparations are sophisticated and are recognized and awarded with ISO 27001 (twenty-seven thousand one) information security certification. Maintaining this certification requires the Fund to be audited every year in order to ensure the continuous improvement of the Fund’s Information security.

The Fund and its dedicated officers work hard to ensure that staff are well informed and always aware of potential attacks. This information is important for all Fund staff as well as all Fund members: participants, retirees and beneficiaries.

The following suggestions are for professional engagement but should also be followed in your personal digital lives.

Remember always be aware and cautious of possible attacks when receiving any email, using any website, or publishing information in any social network, connecting to a public WIFI or plugging-in a USB device to your computer or any other electronic device. Because you never know where a hacker could be hidding…

Beware!
Passwords: Fund staff and all clients of the Fund should use strong passwords with a minimum of 13 characters and each should include small letters, capital letters, numbers and special symbols. Or use a long “passphrase” that you can remember and make it hard to guess by others. And do not forget to change your password every two or three months. Remember do not share your passwords with anyone or store it in computers that do not belong to you.

If you receive an unsolicited e-mail from an unknown sender asking you to open a file, to click on and follow a link or to send pension related information or to confirm any personal information (like your Member Self-Service username or password or anything else), before doing anything try to confirm that the e-mail is authentic, examine the e-mail address of the sender and if you have any doubt forward the e-mail to: helpdeskpf@unjspf.org requesting verification or delete it.

The Fund will never ask a Client to send a username or password or bank account information through e-mail.

The Fund hopes that all of its members will register on the Member Self-Service site. This is a secure site which is protected by the Fund and by you when you register. Please follow the advice of this video and use a strong password that you keep secure. For more information, refer to the Fund’s website (www.unjspf.org) to see other whiteboard videos and other learning materials.

And always, be Aware, Pay attention and help us keep your Pension data secure.