STAFF MEMBER'S INFORMATION SECURITY IN A NUTSHELL

1) Handle work-related tasks using the equipment provided by your employer whenever possible.

2) You are responsible for all activities carried out under your user ID. Protect all information in your possession, both your personal as well as university-related matters. Never tell your password to anyone else.

3) Choose a password that is easy for you to remember but impossible for others to figure out. Choose different passwords for the university services and any external services.

4) Make arrangements to ensure that your e-mail is monitored even when you are absent. Set automatic out-of-office responses when necessary.

5) Don't open e-mail messages if you are uncertain of their origin. E-mail messages may contain malware or direct you to sites that contain malware.

6) Beware of phishing, i.e. messages asking you to share your user ID and password or enter them on a website form. System administrators never ask for your password.

7) Always check the actual target address before clicking a link. Be extra careful with regard to links received in e-mail messages. Learn to tell which Internet addresses are genuine and which indicate fraud.

8) Before registering as an online service user, always check the terms and conditions to make sure that data ownership will not be transferred and no data will be handed over to third parties. Think very carefully about sharing information about yourself or the university in various online services (Facebook, photo sharing services, etc.).

9) Malware spreads quickly through web services and social media. Be cautious about pop-up windows, advertisements and invitations - click carefully!

10) Protect your own computer with a firewall, anti-virus software, back-up copies and software updates. Also, protect your smart phone and other mobile devices e.g. with a lock code. Only install applications that you really need on your computer and mobile devices.

11) Don't use a flash drive as the primary or only data storage. If you intend to save sensitive data on a USB flash drive, get one that encrypts the data.

12) If you print something using a shared printer, pick up your printout immediately.

13) If you suspect a security breach or system abuse, contact the university's IT support or the person in charge of the service.

14) When your employment relationship ends, agree on the hand-over of necessary work-related materials to the university with your supervisor.

22.10.2013