INFORMATION SECURITY GUIDE FOR STAFF

December 2013

TABLE OF CONTENTS

- This Information Security Guide is primarily intended to serve as a general guide for university staff members, regardless of their place of work. It is produced by a group of universities’ information security experts.
- Workgroup: Olavi Manninen, University of Eastern Finland, Mari Karjalainen, University of Oulu, Matti Levänen, University of Jyväskylä, Ulf Pensar, Hanken School of Economics, Jan Wennström, Åbo Akademi University.
- Photos: Raija Törrönen, University of Eastern Finland
- Layout: Raija Sassi, University of Helsinki
- Translation: Miia Santalahti, T:mi Käännös-Ässä
- The guide is partly based on the Student’s Information Security Guide published in 2009 and produced by Kenneth Kahri, University of Helsinki, Olavi Manninen, University of Kuopio, and Kaisu Rahko, University of Oulu.

- In addition to this document, two complementary guides have been prepared: the Information Security in a Nutshell document, which summarises the key issues of this guide, and the Mobile Security Guidelines, which contain instructions for the use of mobile devices.

WHY IS INFORMATION SECURITY SO IMPORTANT FOR YOU AND THE UNIVERSITY

- You have surely noticed issues related to information security in the media. Did you ever stop to think about the information security risks that are present in your daily routines?

- You may encounter, for example, a phenomenon called phishing, which aims at finding out users' passwords and using them for illegal financial gain.

- Another serious threat is malware, which can spread through networks and e-mail. Malware programs can, for example, steal or destroy your files, reveal your user IDs and passwords, or slow down networks.

- It is also important to pay attention to your own behaviour with regard to information security. For example, you may accidentally share confidential university information through cloud computing or e-mail services.

- If your work-related information ends up in the wrong hands, this may harm the operations and reputation of the entire university and cause financial losses. Information is the university's most valuable form of capital – protect your information appropriately!

- Everyone is obligated to maintain information security by observing the relevant laws and the university's information security rules and guidelines.

- The instructions provided in this guide help you protect the information, workstations and networks you use.

- If you suspect that a workstation you are using is infected by malware or that your user ID has been compromised, refer to the instructions listed at the end of this guide.

USE STRONG PASSWORDS AND KEEP THEM SAFE

- Use your personal username and password to log into the university's systems. Keep your user ID and password as safe as you keep your bank card and its PIN code.

- You are personally responsible for all activities carried out under your user ID. Never tell your password to anyone else; not even to the system administrators. If anyone asks for your password, it is definitely for a malicious purpose.

- Change your password at a regular interval according to the university's guidelines, and always if you have any doubt that it has been revealed to someone else.

- When you get a new password issued by IT support, immediately change it to one that is only known to you.

- Choose your password carefully. A good password is easy for you to remember but impossible for others to figure out. Don't use words that are commonly used or somehow connected to you. You shouldn't write down your password as such. See your university's instructions about choosing a good password.

- Choose different passwords for the university systems and any external services; this way, cracking the external service password will not compromise the university system's security.

E-MAIL USE

- The university e-mail address should be used as your - The university e-mail address should be used as your primary contact address for all work-related matters. The use of external e-mail services in any work-related purpose is forbidden. It is also forbidden to reroute e-mail to an external service.

- When offering services and handling official administrative duties, a separate, organisation-specific e-mail address should be used, such as registry@ university.fi.

- If you receive an e-mail message intended for another recipient, inform the sender about the wrong address. Remember that you are obligated to maintain the message contents as confidential. However, according to the Administrative Procedure Act, messages related to administrative tasks should primarily be forwarded to the right recipient, if it is known who that is.

- Make arrangements to ensure that your e-mail is monitored even when you are absent. If necessary, set an automatic out-of-office response indicating who handles your duties during your absence.

- Clearly distinguish your private e-mail messages from work-related ones (use separate folders in both your inbox and outbox).

- When sending e-mail, always remember that the recipient may forward you message to a wider audience than you intended, even though you mark it as confidential.

- E-mail messages may contain malware or direct you to sites that contain malware. Don't open messages if you are uncertain about their origin. You can also turn to IT support for further instructions.

- E-mail messages are usually conveyed in an unencrypted format, so sensitive messages and materials must be separately encrypted before sending them outside the university.

- Such sensitive information includes confidential information related to the university's operations, as well as personal data and contact information, bank details and health information.

- Be cautious about sharing your e-mail address. Avoid using the university e-mail address on online forums and social media (e.g. Facebook); get a separate e-mail account for such personal use. Whenever you use the university e-mail, you represent the university.

BEWARE OF PHISING AND OTHER SCAMS

- Apply healthy suspicion with regard to the reliability of e-mail messages. The e-mail's sender field may not indicate the actual source of the message. Malware applications can send e-mail without the user's involvement.

- 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.

- Always check the actual target address before clicking a link. Be extra careful with regard to links received in messages.

- Learn to tell which Internet addresses are genuine and which indicate fraud. Familiarise yourself with your university's guidelines.

- Advertisements and chain letters sent without the recipient's consent are considered spam. Never respond to such messages; just delete them. If an offer seems too good to be true, it probably is; don't take it.

- Universities apply various methods of spam and malware filtering, and this may affect the delivery of e-mail messages. Familiarise yourself with your university's practices.

- Apart from e-mail, you may also encounter other forms of attempted deception, e.g. by telephone or on social media services. Be cautious about unexpected invoices, messages from senders posing as system administrators, and unusual requests sent under your friends' names.

- If you suspect that you have been targeted by a fraud or attempted fraud, you can turn to your university's IT support or the police for further advice.

USE INTERNET SERVICES AND SOCIAL MEDIA RESPONSIBLY

- Many Internet services are implemented in the form of cloud services, which means that the information given by users is only stored on the service provider's servers, usually outside Finland. Before registering as a service user, always check the terms and conditions concerning data ownership and the hand-over of data to third parties.

- Familiarise yourself with your university's social media guidelines. Remember that only certain, designated people can officially represent the university in social media.

- Be cautious about personal data: think carefully about which information you share and with whom you share it. You are in charge of sharing your own personal information, but others' personal information can only be shared with their consent.

- For teaching purposes, you should primarily use services provided by the university. As a rule, students can only be required to use an external service for which registration is needed if this service has been officially approved by the university.

- If you are considering the use of a cloud service, verify its suitability from the universities' joint cloud service assessment site (see link in the list at the end of this guide). If confidential information is to be handled using the cloud service, make sure that the service is rated to be safe enough.

- Find out in advance how to erase all course materials from the network once the course is completed.

- Think very carefully about sharing information in various online services (Facebook, photo sharing services, etc.). Once a piece of information (a document, photo, personal information, opinion) has been uploaded or posted, it may be impossible to delete it permanently from the web.

- Remember the so-called netiquette in e-mail and online communications. For example, harsh comments posted on a discussion board may harm your reputation as well as that of the university.

- Be cautious about pop-up windows and advertisements. Malware spreads efficiently through social media and online services – click carefully!

- Check your user profile's privacy settings (who can access your information) in all online services and adjust them when necessary. Remember that the service provider may change the terms and conditions frequently.

- In online communities, it is easy to pretend to be someone you are not. Don't be too gullible with regard to things you read on the Internet.

- Don't add location data to photos you post online. Disable your camera's GPS functionality or remove the location stamp from photos before publishing.

- Don't add location data to photos you post online. Disable your camera's GPS functionality or remove the location stamp from photos before publishing.

USE YOUR EMPLOYER'S COMPUTERS RESPONSIBLY

- Always log in using your personal username.

- If you use a workstation that is in public use at the university, clear all temporary files you may have saved during your session before logging out.

- Always lock the workstation when you leave it, even for a minute (on Windows workstations: Win+L). This prevents unauthorised access to information systems and files with your account.

- Save all important data on a network drive or in your home directory. These are covered by the university's back-up procedures.

- When you produce or edit text or other materials, remember to save your changes regularly (in many Windows applications, the shortcut is Ctrl+S). This way, you won't lose all of the work done in case of technical failure.

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

- Dispose of confidential printouts and documents using a shredder or put them in the locked information-secure container.

- Installing software on the university's computers is usually forbidden and also technically prevented. If you need a certain application, contact the IT support.

- If you are using a university-owned computer in which you have administrator rights, observe the principles concerning home computers listed below.

KEEP YOUR OWN COMPUTER HEALTHY AND FUNCTIONAL

At home, you are the administrator of your own computer. Monitor its functionality and ensure proper information security according to the following instructions.

- If the computer is connected to the Internet, protect it with firewall and malware protection software.
- Don't install any software application you don't really need. Install all information security software updates. Remove all applications you no longer need.
- Create separate user accounts (without administrator rights) for all users of your computer, including yourself. Administrator rights should only be used for administrator-level tasks (software installation, creating other accounts).
- Take back-up copies of your files on a regular basis. Keep the back-up copies separated from the computer, preferably in a locked place if possible.
- Don't dispose of discarded computers, smart phones or flash drives with general waste. Data must be destroyed by means of overwriting or crushing the media; printouts by shredding.

TAKE GOOD CARE OF YOUR USB FLASH DRIVES

- Don't use a USB flash drive as the primary or only file storage, even though it is a practical tool for transferring data and making back-up copies. A flash drive can easily get lost.
- If you intend to save sensitive data on a USB flash drive, get one that encrypts the data or encrypt it yourself.

- Be wary of other users’ flash drives. They may contain a malware application that activates itself automatically and contaminates your computer.

- If you find someone’s flash drive on the university’s premises, take it to the IT support without checking its contents.

REMOTE USE – USING THE COMPUTER OUTSIDE YOUR WORKPLACE (AT HOME, ON TRIPS)

- Check from your university’s guidelines (remote work guidelines, information classification systems, etc.) as to which materials may be handled at home and on trips.

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

- The computer provided by your employer is intended for your use only. Don’t lend it even to your own family members.

- Use a VPN connection to establish a secure connection to the university’s services.

- When travelling, keep your computer safe from thieves. It is recommend to protect the hard drive using technical encryption.

- If you handle confidential printouts at home, make sure they are appropriately stored and disposed of.

BE CAUTIOUS WITH OPEN LANS AND PUBLIC WORKSTATIONS

- If you use public wireless LANs, only contact e-mail and other services that use an encrypted connection (the address starts with https://) or a VPN connection.

- You always leave a trace of your computer and software usage. Learn to clear the browser's cache memory and delete the most typical traces of your session.

- You should never rely on the information security of Internet cafés, libraries or other public workstations; they may have a program that collects user data. Consider whether it is necessary to access, for example, your e-mail from such a workstation.

ALSO KEEP YOUR MOBILE DEVICES SECURE

- Phones, tablets and other mobile devices must be protected as carefully as computers.

- Don't open messages that come from unknown senders or seem suspicious for some other reason. They may contain malware that send messages in your name or cause other kinds of harm and extra costs.

- Protect your mobile devices against theft. Set a security code (in addition to the PIN code) to prevent outsiders from accessing your data. Find out whether it is possible to remotely clear your device contents if necessary.

- Disable wireless connections (Bluetooth and WLAN) when you don't need them.

- Remember to also take back-up copies of the important data stored in your mobile devices. Dispose of your data when you discard the device.

- Don’t install any software application you don’t really need. Only download and install software from authorised distributors.

- When travelling, remember that foreign data transfer costs are high, so use your mobile device’s data transfer connection with consideration.

- Carefully consider whether you should share your location data in online services.

WHAT TO DO WHEN YOUR EMPLOYMENT ENDS

- The right to use the university’s IT services is tied to your employment relationship.

- When your employment contract ends, the university will close your user account and, after a certain period of time, delete your e-mail folder and other files permanently. Before your user account is closed, take care of the following:

    - Notify your contacts about the change of e-mail address.

    - Agree on the hand-over of necessary work-related materials to the university with your supervisor far enough in advance.

    - Copy all personal files you want to keep from the university’s servers for yourself, and delete the remaining ones.

    - Copy your private e-mail messages for yourself or forward them to another e-mail account.

    - Uninstall all software you have installed on your own computer under rights granted through the university.

SUSPECT A MALWARE INFECTION OR SECURITY BREACH?

- Anti-virus software can never provide full protection against malware, because new versions emerge all the time. If you have reason to believe that the workstation you are using is or has been infected by malware, proceed as follows:

- Go to another workstation and immediately change all passwords you have used on the infected workstation. If you use the same password in several services, change it in all of them. Notify the customer support of the main services you have used about the possible malware infection and user ID theft in order to facilitate investigating the case.

    1. If the infected computer belongs to the university, contact the IT support. If the infected computer is your own, don't use it until you find someone to remove the malware. Your university's IT support may be able to provide you with some assistance in clearing the malware from your own computer. Help can also be found through the anti-virus software vendor's website.

    2. If you suspect a security breach or system abuse, contact the person in charge of the service. If the suspected breach concerns a university service or a service you have used with the university user ID, contact the university's IT support. With regard to other services, send a notification to the organisation's abuse address (e.g. abuse@[domain]) or call the organisation's switchboard and ask to speak to the person in charge of information security. Clearly describe what you have observed and when it has happened. Leave your name and contact details so that you can be contacted for further information if necessary.

- If you suspect a security breach or system abuse, contact the person in charge of the service. If the suspected breach concerns a university service or a service you have used with the university user ID, contact the university's IT support. With regard to other services, send a notification to the organisation's abuse address (e.g. abuse@[domain]) or call the organisation's switchboard and ask to speak to the person in charge of information security. Clearly describe what you have observed and when it has happened. Leave your name and contact details so that you can be contacted for further information if necessary.

MORE INFORMATION AND LINKS

- Your university's information security site
  Learn your university's information security rules and guidelines.

- Instructions for safe Internet usage
  http://www.tietoturvaopas.fi/en/index.html

- Information about information security threats and instructions on protection against them
  http://www.tietosuoja.fi -> english

- Netiquette: common courtesy in online communications
  http://en.wikipedia.org/wiki/Etiquette_(technology)

- Instructions about securing communications, information security threat notifications
  http://www.cert.fi/en/index.html

- Finnish Competition and Consumer Authority's instructions about recognising scams
  http://www.kuluttajavirasto.fi/en-GB/scams/

- Information security instructions for mobile device users
  http://www.fucio.fi/tietoturva/mobile-security-guidelines.pdf

- Universities' cloud assessment site (in Finnish)
  http://pilviohje.eduuni.fi

- Copyrights from the teacher's perspective (in Finnish)
  http://www.opettajantekijanoikeus.fi