ERiM

Erasmus
Research Institute
of Management

# TOP 10 to DO

## Basic Privacy and Security for Your Data

Author: Jeroen Melein
Updated by: Miriam Braskova, August 2018

Erasmus University Rotterdam

## 1. Practice good password management and do not share your credentials

- Create unique passwords that use a combination of words, numbers, symbols, and both upper and lower case letters. Also see the EUR ERNA password policy.
- Avoid using simple adjacent keyboard combinations. Passwords like "qwerty", "asdzxc", and "123456" are horrible passwords and are trivial to crack.
- Never use the password you have picked for your email account at any online site. If you do, and an e-commerce site you are registered at gets hacked, there is a good chance someone will be reading your e-mail soon.
- Never store your passwords in a plain text file or print.
- A strong password could be a sentence, easily remembered, where you swap some of the letters with numbers, e.g. "I enjoy educating students", can change to "I3nj0y3ducat!ngStud3nts" (swap o with 0, e with 3, i with !).

## 2. Ensure you login to your computer with a password and lock your screen when you are not using it

- To avoid unauthorized access to your data and accounts, always ensure that you need to enter a password when logging in. Set your settings that you need to enter your password immediately after your screensaver begins or after sleep.
- Always look your screen when you are not using it. For Windows lock your screen when you leave your desk with ⊞ + L, for Mac the command is Control + Shift + Power.

## 3. If you are not using an @wEURk laptop or desktop, keep your software up to date and install a virus scanner

- By doing this, you lower the probability that your workplace is hacked or affected by viruses, malware, ransomware, key loggers or Trojan horses.

## 4. Do not mix personal accounts with your work account

- Your personal accounts most probably have lower security settings and synchronize data with personal devices which are not protected by our measures and policies. Avoid any cross contamination between the two.
- For example, do not use your Gmail account for sending work e-mails or use your Hotmail account for sharing files using OneDrive.

## 5. Do not use public/free WiFi

- If you need to go on Internet, use your mobile phone to create a hotspot with password.

## 6. Privacy Awareness Session

- Follow a session to ensure that you are knowledgeable about legislation and impact on your work.
- Contact your manager or chairman to plan an awareness session, provided by RSM IMC.

## 7. Encrypt your workstation and/or laptop and any sensitive data you transmit

- All @wEURk laptops are provided with BitLocker. This is done automatically.
- f you have your own device, go to MyEUR and search for Bitlocker to find a guide on how to install it. If you have a Mac, lookup Filevault.
- If you lose your laptop or phone, contact the ICT helpdesk immediately.

## 8. Anonymize or pseudonymize personal data wherever possible. Delete sensitive data when you do not need them anymore

- After full anonymization, the data falls outside of any privacy regulations.
- Pseudonymization is a best practise for those researchers who work with personal data. Always ensure that you keep the key-file in a secure, encrypted location, only accessible by you and those who absolutely need it. Also ensure a back-up scenario.

## 9. Check with your Legal Counsel or Privacy Officer before sending personal and/or sensitive data outside of the university

- It is highly likely that you need to arrange matters by signing a contract or another agreement in order to be compliant and in order to safeguard privacy and/or intellectual property.

## 10. Always ensure that only the people who need access have access to sensitive data

- Do not store sensitive data in a location that can be accessed by larger groups (including department folders on a shared drive).
- When sharing in a dynamic group, always remove access for people leaving the group.