Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

IT Services
Management

ETH Zürich
Dr. Rui Brandao
Head of IT Services
STB J 19
Stampfenbachstrasse 69
8092 Zurich, Switzerland

Phone +41 44 632 21 50
rui.brandao@id.ethz.ch
www.id.ethz.ch

IT Best Practice Rules

History Of Change

Version	History / Status	Date	Author
1.0	Initial version	27/08/2013	Author association IT Services
1.1	New content version	06/09/2016	Dieter Gut, IT Services
1.2	Minor adjustments	17/01/2017	Dieter Gut, IT Services
1.3	Check actuality, renew links	05/23/2018	Dieter Gut, IT Services
1.4	Update item #9, system scan	03/06/2019	Dieter Gut

These regulations address:

⬢ Operators/users of self-administered mobile devices which belong to ETH and/or are directly connected with the ETH network and/or synchronise with data of ETH. This includes all smartphones and tablets/pads.

▲ Operators of “BYOD” (Bring Your Own Device), meaning self-administering systems which are directly or indirectly connected with the ETH network. This includes private PCs with access to ETH data (VPN).

🟩 Operators of server systems, such as web servers, database systems and operators of IT infrastructures for user groups.

These symbols will help you to recognise the regulations which are relevant to you.

These regulations are referenced from the rules governing telematics (BOT, RSETHZ 203.21). They are only recommendations, but they should only be disregarded if there is a compelling reason. Adherence will be reviewed if there is an incident.

1. ⬢ 🔺 🟩

Install the current firmware and a current operating system. Do not install any operating systems or applications for which the manufacturer has stopped delivering support (updates). Exceptions will need to be operated in a specially protected network. Always install software from a trustworthy source.

⬢

Check regularly whether the website of the manufacturer of your smartphone offers fixes or new releases for your devices. Many devices are not up-to-date when purchased.

2. ⬢ 🔺 🟩

Make sure that your software and operating system is **up-to-date**. If possible, use automatic updates or specify regular time windows for system maintenance. As per legislation RSETHZ203.23, you are obligated to perform timely updates.
Caution: “Out of the box” software is frequently not up-to-date at all and needs to be updated immediately after installation.

3. ⬢ 🔺 🟩

Please ensure that you only use secure passwords on your system. Please ensure that all accounts are protected with a secure password, a non-trivial PIN or other similar mechanisms. Tips for secure passwords are listed in our IT Security Campaign: https://itsecurity.ethz.ch/en/#/use_good_passwords. The current technical password policy for ETH passwords is displayed while entering or changing the NETHZ password.

Do not use the same passwords for the ETH systems as you use to foreign systems, such as online shops, supplier access, private accounts, e-Banking, social networks (Facebook, LinkedIn etc.), private e-mail accounts etc. Should you have the same passwords despite this rule, please change the passwords of the ETH systems immediately.

🟩

It is recommended to implement technical password policies to force a certain degree of password quality.

4. ⬢ ▲ ■

Secure the user data and configurations of your system regularly and check the reproducibility of backups.

5. ⬢ ▲ ■

Systems may not be operated without malware protection. Otherwise, you may endanger your own system as well as others and potentially contribute to the distribution of malware and criminal cyber activities. Protection programs are to be updated regularly.

⬢

There are free programs also available and recommended for smartphones (example: “Avira Free Android Security”, “Lookout” for Android and Apple iPhones). These products will also regularly scan your installed apps and signal any kind of security problem.

■

If a virus protection software causes functional or dynamic problems on servers, it can be configured correctly to protect and not disturb other programs.

6. ⬢ ▲ ■

Please prevent the use of your systems by strangers, friends or relatives and never pass on your credentials (accounts, passwords, codes, PINs).

7. ⬢ ▲

As far as technologically possible, always encrypt your devices, such as laptops, tablets and pads, smartphones or memory sticks. That way, nobody will be able to access your personal data or ETH data in case the device is lost. Classified and/or sensitive data should never be stored on mobile devices.

8. 🔺

In case of suspicion of having been compromised, cut your system from the ETH network and/or the Internet immediately. Only reconnect once you have ensured that your system is in order (again) and does not pose a danger for anyone else.

9. 🔺 🟩

Scan your system regularly for existing or new vulnerabilities and resolve them. To do so, always install software from a trustworthy source only. Any malware protection SW is able to scan your system regularly or on demand. All operating systems and most of trustworthy SW has a function for updating automatically. Always use these features. Additionally you can apply utilities like https://patchmypc.com/home-updater-download in order to perform security inspections.

10. 🟩

If you want to install a new server, please determine the following first:

- Which data will be stored on the server?
- How sensitive is this data?
- Who should be able to access it from where?

Let security@id.ethz.ch advise you on where in the network to place the system. Document your risk assessment.

11. 🟩

If possible, separate exposed systems from systems with sensitive data (e.g. web server from servers with end user data). If a server which is visible from the Internet is compromised, the actual data on a better protected system will still be safe.

12. 🟩

Remove or lock the services and applications you do not require. A web server should only be located on systems which also offer web services.

13. 🟩

As far as possible, restrict the access rights to directories with user data and to user data itself. Specify exactly who can read and change what and remove access rights from everyone else.

14. 🟩

Use the productive server systems only for the intended purpose. Test and surf sessions do not belong on productive server systems.

15. 🟩

For administrative remote access, only use secure source systems. Access from servers which are administered by a third party (e.g. Internet Café) or mobile systems (mobile phone, tablet, ...) is not permitted since key loggers may be installed or the connection may not be protected against spyware. Only use encrypted connections for administrative access.

16. 🟩

Check the assignment of access rights periodically and remove the rights for persons who may have left or taken over different tasks. It is recommended to document such periodic checks.

17. ⬢ 🔺

In case of Wi-Fi connections on mobile devices, such as with EDROAM, the certificates must be imported and the check of the certificates must be active. This way, the mobile devices cannot be tricked by a fake, malicious access point with the same name and no data connections can be read by third parties.