FH Vorarlberg
University of Applied Sciences

IT SECURITY GUIDELINES
FOR STUDENTS OF THE FH VORARLBERG

TABLE OF CONTENTS

This document does not replace other binding regulations (e.g. education contract or terms of use). The provisions contained in this document are binding (except for points which are merely formulated as recommendations).

Last update: June 13th, 2019

GUIDELINE FOR DEALING
WITH IT RESOURCES OF THE FH VORARLBERG

The term IT resources covers hardware and software as well as the associated network connections that are made available to students (e.g. in computer pools, libraries and research centres).
Administration or security functions (e.g. malware, password protection or firewall rules) already configured by the IT of the FH Vorarlberg on computers of the FH Vorarlberg may not be changed.
The copying of programs, software components, fonts etc. from computers of the FH Vorarlberg is prohibited, as is the independent installation of programs, software components or fonts.

Private commercial activities are expressly prohibited. The following priorities apply to the use of the IT facilities (higher-weighted activities first):

- Teaching activity (during the lesson work in the same room may only be carried out with the express consent of the teacher)
- Events of the FH Vorarlberg
- Preparation and follow-up of exercises from the classroom
- private, non-commercial activities which serve to practice and deepen the subject matter of the course
- Entertainment (Internet surfing, games, etc.) and further training, provided that these activities do not lead to excessive wear and tear or damage to the facilities.
-

In the event of operational disruptions, IT Support must be informed; maintenance activities of IT Support have priority.

CORRECT HANDLING OF PASSWORDS

You will receive an IT user account with password at the beginning of your studies and will be asked to change this password the first time you log in.

Under no circumstances may you share your password with third parties!

If you make several mistakes when entering the password, the account will be blocked for several minutes. A change of your password is possible under Account and E-Mail, the reuse of the last five passwords is not possible. The length of a password is essentially the best protection against possible misuse (e.g. brute force attacks). Today, it is only recommended to change the password if there is a suspicion (e.g. "read along" or known security gaps in IT services).

For the IT services at the FH Vorarlberg a single password is used in connection with your user account. For the use of "eduroam", especially on private devices, a separate password is strongly recommended (background: e.g. regular security problems on mobile devices).
The password of your user account of the FH Vorarlberg may not be used under any circumstances for services not operated by the IT department of the FH Vorarlberg (e.g. cloud provider).
For the administration of your other passwords (e.g. cloud, but also for private use) the use of a password manager is recommended (e.g. https://www.enpass.io/).

DATA BACKUP ON IT SYSTEMS OF THE FH VORARLBERG

DATA BACKUP ON SERVERS OF FH VORARLBERG

A regular data backup is carried out primarily to ensure the general functionality of the FH IT infrastructure. A **recovery** of individual files, entries or e-mails **is not planned** if the user has accidentally deleted this data.
Against this background, it is advisable to store important work results of the day on a private data carrier (external hard disk or USB stick) or better "in the cloud" using cloud file storage solutions. The FH Vorarlberg already provides you with 1 TB free of charge in connection with your Office 365 account.

DATA BACKUP ON LOCAL COMPUTERS AT FH VORARLBERG

Local hard disks of the computers available to the students are basically encrypted, are not backed up and can be deleted at any time (also due to the new installation of the devices).

RECOMMENDATIONS FOR DATA SECURITY
WHEN USING YOUR PRIVATE DEVICES

RECOMMENDATION FOR HANDLING PASSWORDS AND CORRECT SECURITY SETTINGS ON PRIVATE DEVICES (EN)

On private notebooks, we strongly recommend that you provide your IT user account with a password for logging in (no "auto-login"). In addition, the IT user account should not have any local administrator rights (use your own "administrator user"). The password should correspond to the usual quality standards and should not be identical with the password of your FHV user account for reasons of data security. Please also note to configure a screen lock after a short period of inactivity, which can be unlocked with your password. On smartphones, tablets, etc. it is recommended to implement this via fingerprint, PIN code, etc. IT generally recommends the use of a **password manager**, as of 2018 IT recommends either a product based on KeePass (advanced) or Enpass (free for desktops, very inexpensive for smartphones, supports device sync and browser).

PROTECTION AGAINST MALWARE ON PRIVATE DEVICES

We strongly recommend to install the virus scanner of the operating system or another virus scanner on private devices. Please configure your computer so that the operating system, applications and virus scanner are updated automatically on a daily basis.

PROTECTION AGAINST DATA LOSS ON PRIVATE DEVICES

We also recommend periodically (at least once a week) backing up the local data carriers to an external storage medium (e.g. external hard disk) on private devices using the tools provided by the operating system.

ENCRYPTION OF PRIVATE DEVICES OR DATA CARRIERS

We also strongly recommend encrypting private devices (notebooks, smartphones, etc.) with the means provided by the respective operating system (Windows Bitlocker or MacOS FileVault).
ATTENTION: If you lose the encryption password, your data will be irretrievably lost! Save this in a password manager (see above).
Please also note that students must independently implement the encryption of other data carriers (e.g. USB sticks) if they have personal data or data from the FH Vorarlberg on them.)

FURTHER BINDING REGULATIONS AND INFORMATION

Irrespective of whether you use a computer from FH Vorarlberg or a private device, the following regulations apply:
Within the scope of the use of IT resources (on devices of the FH Vorarlberg or on private devices which are connected with the IT infrastructure of the FH Vorarlberg) the valid legal regulations, license and terms of use as well as the applicable copyright regulations have to be complied with. The user is personally liable for any infringements. If claims are made against FH Vorarlberg in such cases, the user shall indemnify and hold FH Vorarlberg harmless; negligent or intentional damage to property and the cost of remedying the same shall be charged to the party responsible and, if necessary, also claimed as damages.

The IT department may at any time and without the prior consent of the user restrict student, business or private use if legal, contractual or security-related risks become apparent to FH Vorarlberg. Information to the respective users concerned shall be provided at the latest in retrospect, unless the restriction is automated.
There is no entitlement to separate treatment of private applications or data. *Background: If you use the IT infrastructure of the FH Vorarlberg with a computer of the FH Vorarlberg or with a private computer, we cannot distinguish between student, business or private use.*

There is no entitlement to functionality or performance features, data backup, data security or availability or IT support in connection with private use. Background: Requirements in connection with private use must not be at the expense of the FH Vorarlberg.

In addition, the following pages offer further information:

- A general description of the technical and organizational measures we use to keep IT security as high as possible.
- The acceptable usage policy that you have agreed to upon acceptance of your account or upon a new update.
- The privacy statement can be found at any time at inside.fhv.at/display/hilfe/datenschutz, which supplements the general data protection declaration of the FH Vorarlberg at www.fhv.at/datenschutz/.