



## Department of Molecular Life Sciences (DMLS)

---

# DMLS IT Regulations

## Regulations on computer usage and network access in the Institute

*Fabio Snozzi, Werner Wolz & Marco Schmidli, DMLS IT- and network-coordinators*

### 1 Access to the network

The computer network of the University of Zurich is operated and maintained by the Central IT Services ("Zentrale Informatik" or "ZI"). Therefore, their regulations and guidelines apply to all users of the UZH computer network (see: <<https://www.zi.uzh.ch/de/staff/it-security/guidelines-and-security-rules.html>>). Additionally, the following regulations are effective for the DMLS computer network:

#### 1.1 Connections to the cable-bound DMLS Ethernet network

**1.1.1** Network devices (laptops, computers, network printers, etc.) may not be connected to the cable-bound DMLS computer network without permission from the DMLS IT staff. Computers must be checked by the DMLS IT staff for proper configuration and you have to agree to these guidelines with your signature at the end of this document, before your computer may be connected to the network for the first time.

**1.1.2** There is no guest access to the UZH network with the exception of the wireless networks (WLANS) *uzh*, *uzh-5GHz*, *eduroam* and *public* (see section **1.2.2** below).

**1.1.3** Static IP addresses may only be used if they were assigned to a device by a DMLS network coordinator. If a static IP address has been assigned by the DMLS IT staff, it must not be changed by the user. The name resolution service (DNS) must be configured to use the DNS servers of the DMLS or the Central IT Services only.

**1.1.4** Computers must be registered with the DMLS IT staff before they may be connected to the network. Only registered computers can use a dynamically assigned IP address (DHCP).

#### 1.2 Connections to the *uzh*, *uzh-5GHz*, *eduroam* and *public* wireless networks

**1.2.1** Computers and other network devices (e.g. tablet computers, mobile phones) may be connected to the *uzh*, *uzh-5GHz*, *eduroam* and the *public* wireless networks in the DMLS without restrictions or permissions from the DMLS IT staff. Nonetheless, the regulations and guidelines set by the Center for Informatics Services ("Zentrale Informatik") do apply (see 1.).

**1.2.2** UZH students may use the WLANS *uzh* and *uzh-5GHz*, guests may use either *eduroam* with the credentials of their home university or a VPN connection to an external VPN server via the *public* WLAN. Furthermore, any UZH user may apply for a one-day account for visitors at any time ("WLAN für Tagesgäste"). Visitor accounts for a congress or meeting must be applied for with the DMLS IT staff at least 2 weeks in advance.

**1.2.3** Many servers and services in the DMLS block network connections initiated from outside the DMLS computer network and are not available from the *uzh*, *eduroam* and *public* WLANs.

**1.2.4** Printing to the DMLS network printers is possible from all over the UZH network via IP-Printing. In order to use a printer it must be set up with its IP address or, if available, host name. Regular DMLS staff members may use the UZH PrintPlus printers, printing costs will be charged directly to the work group's account.

### 1.3 Connections from the UZH network to the Internet

**1.3.1** Computers and other network devices (e.g. tablet computers, mobile phones) may be connected to the *uzh*, *uzh-5GHz*, *eduroam* and the *public* wireless networks in the DMLS without restrictions or permissions from the DMLS IT staff. Nonetheless, the regulations and guidelines set by the Center for Informatics Services ("Zentrale Informatik") do apply (see 1.).

**1.3.2** VPN connections may only be used with the VPN client included in Windows or Mac OS X or with a VPN client provided by the Central IT Services of the University. The UZH VPN service may only be used to connect your computer from outside the UZH to the UZH network. You may not use VPN connections to public VPN or commercial VPN services (e.g. in order to circumvent geo-blocking or to anonymize network traffic).

## 2 Computers

All computers (physical computers and virtual machines as well) must fulfill the following requirements in order to connect to and use the DMLS computer network:

**2.1** All computers must have at least two different accounts: a restricted (standard) user account for daily work and an administrator's account for system administration (system management, installation of software & updates, computer backup). The administrator's account may not be used for daily work (reading e-mails, browsing the web, using office and scientific programs, etc.).

**2.2** The operating system must always be up-to-date. Security relevant updates for the operating system must be installed either automatically (preferred) or manually as soon as they are available ("Microsoft Update" or "Windows Update" for Windows and "Software Update" for Mac OS X).

**2.3** Critical software must always be up-to-date, security relevant updates must be installed as soon as possible. Critical programs are: web browsers (Safari, Firefox, Google Chrome), e-mail programs (Apple Mail, Thunderbird, Outlook, etc.), Adobe Flash Player, Adobe Acrobat/Acrobat Reader, Java, Microsoft Office and all other applications that are used to open/download files from the Internet.

**2.4** All computers must have an up-to-date anti virus software installed and the program should be configured to download virus definition updates on a daily basis. The DMLS holds a license for the commercial enterprise anti virus software Bitdefender Endpoint Security. Bitdefender Endpoint Security may only be installed on work computers. Many anti virus companies offer free anti virus software for home use which may be installed on privately owned computers.

**2.5** The software firewall of the operating system must be activated (note: in all versions of macOS the firewall is deactivated by default!).

**2.6** Computer names will be assigned to DMLS computers by the DMLS IT staff, exclusively, and must not be changed by the user.

**2.7** The operating system language and the keyboard layout must be either English or German. Other languages and/or keyboard layouts are not supported and such computers may not be connected to the DMLS computer network (except the *public*, *eduroam* and *uzh(-5GHz)* WLANs).

**2.8** If you intend to (re-)install or upgrade an operating system on your computer for whatever reason, you have to contact the IT staff in advance (including your privately owned computer, if you want to connect it to the cable-bound DMLS network).

**2.9** Computers purchased on behalf of the Institute or a DMLS work group are the property of University of Zurich. Laptops assigned to a DMLS user have to be returned to the DMLS IT staff including all accessories by the user on leaving the Institute.

**2.10** Computer hard disks must not be encrypted (VeraCrypt, BitLocker [Windows], File Vault [macOS], etc.) unless having checked back with the DMLS IT staff in advance.

## 3 Software

**3.1** The following operating systems are supported by the DMLS IT staff and allowed in the DMLS network: Windows 7 SP1, Windows 8.1 & Windows 10, macOS 10.12.6, 10.13.6 & 10.14.x, Linux (please check back with the DMLS IT staff).

**3.2** Any software installed on a computer has to be properly licensed. Unless stated otherwise, a single license may only be installed on one computer (e.g. Adobe Creative Suite). For each installation of a software a separate, individual license has to be purchased, with the exception of campus, faculty's, or Institute's licenses or other different licensing schemes, e.g. Open Source software (GPL).

**3.3** Installation and usage of cracked software or software with stolen/cracked serial numbers is strictly forbidden. You will be personally held responsible for any legal consequences.

**3.4** Installation and operation of personal file sharing software, like Bit Torrent, Gnutella, The Pirate Bay, Kazaa, eDonkey, etc., is not allowed. These programs can cause an enormous amount of network traffic which may interfere with regular IT services. Often, those file sharing programs are contaminated with malicious components, like spy ware, dialers and/or Trojan horse programs.

**3.5** The following commercial software is commonly available in the DMLS: Bitdefender Endpoint Security, Microsoft Office for Windows and Mac, FileMaker Pro, CLC Workbench, Sequencher and MacVector (<<https://www.imls.uzh.ch/en/services/intsvc/itsup/app/sw.html>>). Furthermore, the University offers a distinct range of software, see here: <<https://www.zi.uzh.ch/de/staff/software-elearning.html>>.

**3.6** Users are encouraged to prefer the use of free and open source software (GIMP, Open/Libre Office, Inkscape, Scribus, VLC) over closed source and commercial software (Adobe Creative Suite [Photoshop, Illustrator, etc.], Microsoft Office) whenever possible and appropriate.

**3.7** Any software or software license that you may have received from the DMLS has to be removed from your computer when you leave the institute.

## 4 Data

**4.1** All users are personally responsible for their own data.

**4.2** Usually, data on the file servers will be backed up once a day unless otherwise stated.

**4.3** Private data like photos, videos and music are banned from DMLS servers and may be deleted by the DMLS IT staff without any prior notice immediately on discovery.

**4.4** Files containing illegal or inappropriate contents are banned from DMLS servers and may be deleted by the DMLS IT staff without any further notice immediately on discovery.

## 5 Passwords

**5.1** Unless explicitly specified as a group password, any password given to you by the ZI or the DMLS IT staff is your personal secret and may not be shared with anybody else. It is strongly recommended to change frequently used passwords from time to time.

**5.2** Do not use the same password on different servers or web pages, especially, if there is personal and/or financial information (e.g. credit card numbers) or access to critical infrastructures associated with an account.

**5.3** Use strong and complex passwords consisting of at least 10 small, capital, and special characters and numbers. Do not use whole words or parts of words and names in a password.

## 6 Security compromise

A security compromise may be the presence of a Trojan horse program, a Virus/Worm or other malware on a computer or a misconfiguration of the operating system (e.g. back door user accounts, back door services) or passwords leaked to unauthorized persons or systems.

**6.1** If a user of a computer, the staff of the Central IT Services ("Zentrale Informatik") or the IT staff of the Institute should detect a security compromise on a user's computer, it must be disconnected from the network immediately!

**6.2** If a security compromise is detected, the affected computer might only be reconnected to the University network after the hard disk is freshly formatted, the operating system and all applications are installed from scratch by the DMLS IT staff and all relevant passwords are changed.

Zurich, 05.07.2019

I herewith confirm that I have fully read and understood the instructions above. I am aware that I may not receive any support from the IT staff if I do not follow these instructions. I am also aware that in case of a security compromise on my computer (Virus-like programs, "hacker" intrusion) or in case of severe violations of these rules, my computer may be withdrawn at any time and my e-mail and file server accounts may be locked immediately.

Name:	Work group:
Signature:	Date:

I herewith confirm that I have fully read and understood the instructions above. I am aware that I may not receive any support from the IT staff if I do not follow these instructions. I am also aware that in case of a security compromise on my computer (Virus-like programs, "hacker" intrusion) or in case of severe violations of these rules, my computer may be withdrawn at any time and my e-mail and file server accounts may be locked immediately.

Name: Martina Lehmann	Work group: Robinson Group
Signature: 	Date: 23.09.2025

Version date: 05.07.2019