

Baseline Security

Access control

20. User management

New users are either students or institute members. Their enrolment in the courses or their appointment as member of the institute is regulated elsewhere. Once this has taken place, personal information of these persons are entered into the Person database by the institute secretariat. Once this is done system management can use a WEB forms system to generate an account.

Detail of [starting](#) and [ending](#) the membership at the institute can be found here.

21. External user access computerroom

No one is allowed to access the computer server room without a IT Department person accompanying.

22. Standard passwords

During installation of any device that has a network access controlled by username/password combination, all defaults are removed and system management implements a new secure password. System management keeps track of these username/password combinations for all devices.

23. Network security

Network access is granted only by MACaddress of the device cabled to the network. Unknown MACaddresses are excluded access to the wired network. Wireless network access is granted on the basis of a guest facility or through authentication using local account information of ULCN account information.

For details on wireless see [here](#).

24. Password requirements

Passwords are not freely formatted, there are [restrictions in place](#).

25. Secure login

Access to the institute resources through a login procedure is always done in a [secure way](#)

26. User security policy

27. Network usage policy

28. BYOD

29. Remote access critical applications

30. Mobile equipment and concern data

From:
<https://helpdesk.physics.leidenuniv.nl/wiki/> - Computer Documentation Wiki

Permanent link:
<https://helpdesk.physics.leidenuniv.nl/wiki/doku.php?id=policies:security:access&rev=1515159034>

Last update: **2018/01/05 13:30**

