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 or though secure protocols

26. User security policy

Users have been instructed to handle password information with care.

All Linux and Windows systems have an automatic 'screen lock' enabled initiated after a period of inactivity.

27. Network usage policy

Wired network access is granted on the basis of membership of an associated institute as described in the account policy. Once connected to the wired network, access to system assets is controlled by user authorization and authentication. Authorization is governed by the status of the membership. Students and postdocs have supervisors granting the access restrictions. Postdoc usually acquire their on devices, while staff member are granted general access.

28. BYOD

External machines, not acquired through university funding or not maintained by system admin, can only obtain access to the wireless network to which general restrictions are applied.

29. Remote access critical applications

Only system managers require remote access to critical applications. Critical applications are not accessible from selected devices inside the IT Department infrastructure. System managers both need to authenticate to these devices and to the critical application for being granted access.

30. Mobile equipment and concern data

There are no mobile devices storing concern information.