

Security Baseline

Classification

3. Registration of assets

A list is available that records purpose and ownership of all assets

4. Line managers

Due to the limited size of the IT Department there is no highly detailed denotation of line managers, but a crude list of responsibilities by person is available.

5. Classification

There are [guidelines](#) for the classification of information.

6. Licensed software

Whenever a piece of software requires licensing, this is either performed centrally at the ISSC or done locally. Many software packages, however, are open sources or GNU licensed and do not need any licensing agreement.

7. Buildings

The vastgoed expertise center is responsible for the building infrastructure of the university, including the housing of the IT equipment according to the requirements set out by the IT department.

8. IT rules of conduct

These rules are made available through a university webpage, to which each new arrival at the institute is pointed in a welcoming email or course.

9. Exit procedure

There is a well defined exit procedure for all personal leaving the scientific institute. It is described on the helpdesk wiki pages to which each member of an institute has been pointed at start of the employment and which remains available throughout the employment.

10. Computer room access

The main computer rooms are inaccessible to the general personal of the institute. Access is only granted to the IT Department members. In addition a standard user restricted authentication access is in place of all data, with different levels of access based on the security requirements pre data item.

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

Permanent link:
<https://helpdesk.lorentz.leidenuniv.nl/wiki/doku.php?id=policies:security:classification&rev=1515154448>

Last update: **2018/01/05 12:14**

