Baseline Security

System management

11. System management guidelines

We have developed guidelines (as recorded in the sysadmin wiki, restricted access) for

- Initialize
- Decommissioning
- Backups
- System repairs
- Fault management
- Log management
- Contacts
- Emergency procedures
- Security measures

12. OTAP

For system upgrades, new services and software development virtual machines or separate hardware is used to develop, test and accept new functionality before it is put into the production environment.

13. Services according to SLA

Although there is not a real SLA for the services provided by the IT department but monthly meetings with physics management and bi-yearly evaluation by bservatory Computer commission make sure that agreements are met.

14. Asset reliability, external vulnerabilities

All systems are equipped with virus scanners, spam blockers, malware removers, etc. In particular the mail servers bounce all .exe or .zip type of files. On each file server all data transfer passes through virus scanners before it is stored. In addition ransomware protection tools are implemented on each desktop and integrated in file servers.

Constant monitoring of illegal behaviour is in place on all systems. And in case of suspicious activity system management is informed.

15. Backup policy

Due to the very large amount of data under the responsibility of the IT Department only a limited set of data are being backed up a a regular basis. In fact for data classified as Restricted or Private a full backup scheme is in place.

16. Backup

Backups are made on spinning media, that are monitored and maintained 24x7x365

17. Off-site backup

For the 'data generated' (in house), classified as Restricted, a backup facility is in place at the TU Delft in collaboration with the ISSC.

18. Information exchange

Data transfer of Restricted and Private from or to external resources should always take place in a secure way. Therefore, remote file transfer is only possible through encrypted protocols, scp, sftp, https or encrypted submission. Protocols like telnet, ftp or http are disabled for this type of data.

19. Change management

There is no ITIL procedural change management in place. Each change is done in close collaboration with the owner of the asset.