Security Baseline

Development and Maintenance

31. System ownership

32. New information systems procedure

33. Additional risc analysis

34. Operational acceptance asset

35. Security update procedure

For all systems, server, desktops, stoarge and other devices security updates are implemented as a continuous process. Every day the software repositories are automatically interrogated for new security updates, which are then applied immediately.

36. Logfiles

Log files are stored local to the system where they are created. However, each log is analysed automatically and in case of a non-regular situation system managers are emailed with an indication of the non-regular behaviour. Upon receipt of such an incident the log on the system in question will be analysed. In case of a true irregularity an incident is initiated.

All systems use one set of time servers inside the IT Department server hardware to synchronize all clocks on all devices. The IT Department time servers themselves use international time servers to keep their time synchronized to the 'world'.

37. Security incidents recording

Security incidents are recorded in a mail folder of the IT Department Head.

38. Security incidents responsible

The Security manager as defined by the roles is the responsible person for all incidents and works in collaboration with all team members to resolve the incident.

39. Calamity procedures

There is no true calamity procedure and each case is handled ad hoc, with teh following requirements in mind:

- Minimize downtime of critical services
- Communicate the calamity to all users/steakholders
- Maximize the collaborative effort within the IT Department team
- Strive to full resolution of the calamity