STATISTICS DENMARK

Statistics Norway
Statistisk sentralbyrå

Statistiska centralbyrån
Statistics Sweden

MOZ:2003:11

Consolidation of network administration

Report from a short-term mission

May 5th – 16th 2003

Niels Jespersen

TA for the 'Bridging Support Program to Strengthen the Institutional Capacity of the National Statistics', Mozambique

Instituto Nacional de Estatística

This report contains
restricted information
and is for official use only.

Ref. no. 104.Moz.98

May, 2003

Niels Jespersen
Statistics Denmark
Sejrogade 11
DK-2100 Copenhagen O
Denmark

njn@dst.dk

Phone: +45 39173585

1 EXECUTIVE SUMMARY

During the mission Webmail was established for INE staff. The result of this is that access to the mail system at INE has been greatly expanded. The Webmail System was documented in the form of a manual for installation, a manual for maintenance and finally a manual for the end-user of the web-mail system.

Furthermore, a draft IT Security Policy was formulated. It is the intention that this policy should be discussed at INE before it is implemented.

The Antivirus System at INE was reinstalled according to best current practice. The System was introduced at INE in December 2002, but has not been fully functional until after the reinstallation.

A one-day workshop was held for the staff at DISE. The subjects covered during the workshop were the general IT installation at INE, The draft security policy, the Webmail System and finally a detailed presentation of the Antivirus System.

Finally, a number of smaller issues regarding System Administration were discussed with the Network Administration staff at DISI.

2 INTRODUCTION

INE has been using networking for some time now, and was connected to the Internet at a short-time mission in September – October 2002 (the report from that mission is available as MOZ:2002:6).

Consequently the network is now a critical resource at INE. Its continued operation is needed in order to facilitate the statistical work at INE.

During the period since the short-time mission in September – October, a number of discussions have taken place between this consultant and long term Consultant Mogens Grosen Nielsen, regarding the initiatives needed to ensure a well functioning network at INE. These have lead to the formulation of the Terms of Reference for the mission as attached as ANNEX 1 of this report.

The main deliverable of the mission is Webmail as an extension to the mail system already in place at INE. Webmail gives staff and consultants at INE the possibility to access their mailbox and send and receive mail from anywhere with an Internet connection and a web browser. From homes, airport lounges and other connected places. The installation of the Webmail system is thoroughly documented for the purpose of future maintenance and for end user education. A workshop was held for one day during the final week of the mission where IT-staff was introduced to the detailed workings of the system.

The mission provided specific advice on selected areas of Network and System Administration. The areas selected have been chosen in cooperation with INE Network Administration staff. Finally, the mission provided a draft of a security policy for INE. This draft contains recommendations for policy statements regarding the operations of the INE it environment.

3 ACTIVITIES DURING THE MISSION

According to the terms of reference for the mission, these activities were carried out:

1. Implementing Webmail securely for all staff at INE.
2. Providing information about networking and Internet infrastructure at a one-day workshop.
3. Providing a follow up on recommendations given in the earlier report (MOZ:2002:6).
4. Providing a draft Security Policy which was discussed at the workshop.

Besides the work detailed in the terms of reference, the following activities were undertaken:

1. Providing documentation of design, installation and operation of the Webmail system.
2. Reinstalling the Antivirus System introduced at INE in December 2002.
3. Providing advice and guidance regarding specific system administration issues

See detailed description in Annex 2.

4 CONCLUSIONS AND RECOMMENDATIONS

In the Internet mission in 2002, the final report gave a number of recommendations. These recommendations were formulated in three categories: General recommendations, Internet recommendations and System Administration Recommendations.

The status for these recommendations has been evaluated during this mission, and a number of new recommendations have been formulated. Status and new recommendations are given in the table below, and ANNEX 4 contains a number of notes for the recommendations, existing and new.

Recommendations from mission in September 2002

ID:	Description	Status and comments
REC1	A conservative installation and upgrade strategy should be decided.	It is still a good idea to have a conservative installation and upgrade strategy. However, the Windows NT platform will not be a platform to base the middle term future on. An general upgrade to Windows XP and Windows 2003 Server should be planned to be included in the activities for 2004 or early 2005 at the latest.
REC2	System administration staff should consist of at least two persons.	System administration staff does now consist of two persons.
REC3	Training should be provided to system administration staff	One person is already taking MCSE classes and is preparing for his first certification.
REC4	External support should be secured until internal staff is up to speed.	Has not been secured. In case of very complex issues in the it environment or larger breakdowns, external support is still expected to be necessary
REC5	Prepare disaster recovery plan	Has not yet been implemented. Should now be coordinated with the new work on IT security policy.
REC6	Problem solving guidelines.	Not implemented yet. Replaced by REC23.
REC7	Modernize INEs Antivirus solution.	The antivirus solution at INE war modernized at the end of 2002. There have been a number of problems with the installation. The software has been reinstalled in a correct way and reconfigured during this mission. Still to be done, is a removal and reinstall of client software on all pc's at INE.
REC8	Logging of downtime on Internet connection	This has not been implemented. It is still worth doing, as the service from the present Internet Service Provider (Netcabo) is much below what is expected.
REC9	External mail backup	This has not been implemented. It is still a good idea, especially since power supply in Maputo sometimes is gone for many hours.
REC10	Modem removal	Status unknown
REC11	Hosting of Web site	The website has been moved from Teledata to Netcabo. It is not recommended that INE hosts its own website for now. As long as service from the ISP and the power supply is as unstable as is the case, its not relevant.
REC12	Web mail	Web mail has been installed during this mission, and documentation for installation, maintenance,

		and the end user has been prepared.
REC13	Memory in proxy machine	More memory has not been installed. It is still a good idea to do so.
REC14	List of recurring operational task	This has not been implemented. The recommendation has been replaced by a new more general recommendation. See REC22 below.
REC15	“Out of Office”	It has been decided that you should use “Out of Office” messages to signal that you are away from the office.
REC16	Limitation on the size of external mail	It has been considered, and the decision is not to change the limit.
REC17	Backup procedures and backup policy	Backup procedures have improved since the last mission. The procedures should still be documented.
REC18	Reporting	Has not been implemented. The recommendation is replaced with a more general recommendation below. See REC27.
REC19	Printing model	The printing model has not changed since the last mission. It was decided to look further into changing during this mission.
REC20	Use of drive letters	The issue was discussed during this mission, and the recommendation is to use a model with three standard drives: Personal, Shared data, and Public software.

New recommendations formulated during this mission

Recommendations from mission in May 2003

ID:	Description	Status and comments
REC21	IT security policy	Draft version has been discussed. Continue the discussions and prepare an implementation plan.
REC22	Documentation	The system should be documented according to newly developed documentations standards.
REC23	Organization	There should at least one person present in the network administration unit to answer questions and to ensure stable systems. Two persons must know how to operate each system. One of the two persons should have the main responsibility for the operation of each system.
REC24	Printing model	The original recommendation is still valid.
REC25	Organization /access to central databases	
REC26	Reboot cable modem / use of Watchguard firewall	The cable modem still fails from time to time. Often it helps to turn it off and on again. Further investigation is needed, perhaps in cooperation with Netcabo. The Watchguard firewall was evaluated during this mission. It can sufficiently replace the existing one, in case this breaks down. However the Watchguard will need extensive nontrivial configuration before it can be used directly.
REC27	Reporting	Reporting every second week including list of activities, system downtime, summary of logs and risks.

5 The “INE Webmail CD”

The following software, documentation and configuration files have been provided on two copies of the CD labeled “INE Webmail CD”:

1. installation-of-webmail.doc
2. maintenance-of-webmail.doc
3. Web mail end user manual.doc
4. This draft report.
5. Service Pack 6a for NT, the high encryption version.
6. Windows NT 4.0 Option Pack, the server version.
7. Microsoft Management Console version 1.2
8. A modified default.htm that redirects the browser to /exchange/logon.asp
9. A file for pointing the OWA Server to the Exchange Server (lmhosts)
10. Diruse.exe, a program for providing statistics on disk usage
11. Antivirus at INE.ppt, a presentation of the Antivirus System at INE
12. General aspects of the network at INE and security.ppt, a presentation on network security
13. Security policy.doc

ANNEX 1 Terms of Reference for the mission

TERMS OF REFERENCE
Within the Scandinavian Program

For a short-term mission for a 2 week mission in May 2003
On
Consolidation of network administration

DRAFT

A.1.1 Background

The short term mission is part of a broader task in creating a well-functioning network administration at INE. This task includes hiring extra personnel, developing problem solving guides etc. See Project Description.

The short term mission has the following focus areas:

- Infrastructure and network administration, including information about Internet.
- Security. How to protect the installations at INE against the following treats: no energy supply, water, fire, hackers, hardware break down, virus etc. A security policy should be formulated.
- Standards/best practices for organization and access to centrally stored data and central equipment e.g. printers. These include among other things: standards/best practice for use of drive letters and access permissions for network files, standards/best practices for the organization of data on central servers.

Besides the areas mentioned above the short term mission should also follow up on recommendations in mission report from October. See annex A.

A.1.2 Purpose of the mission

As stated in the project description the overall purpose is to have a well-functioning and self running network administration. In order to ensure this INE has hired one extra person. Thus there will be at least one person to take care of the network administration in working hours.

The specific purpose of this short term mission is a) to consolidate the existing network installations and network administration procedures at INE, b) to develop training material and to carry out training (on-the-job training and courses about network and network administration)

The existing and new staff at INE should be able to maintain and extend the installation after courses and on-the-job-training. The experienced staff should also be able to train new staff using the course material.

A.1.3 Expected results

1) Course material
2) Implemented solution in selected areas including policies and documentation (end user, operation and installation according to standards)
3) Mission report
4) Personnel trained in a) IT-infrastructure and network administration in general b) security in general and how to implement specific security solutions.

A.1.4 Activities

1. Detailed planning and prioritization
2. Courses, on-the-job-training and implementation of selected solution at the following areas:
    - Infrastructure and network administration, including information about Internet.
    - Security. How to protect the installations at INE against the following treats: no energy supply, water, fire, hackers, hardware break down, virus etc. A security policy should be formulated including among other things back up procedures.
    - Standards/best practices for organization and access to data and central equipment e.g. printers.
3. Writing of mission report and evaluation

A.1.5 Tasks to be done by INE to facilitate the mission

- Elaborate ToR for the mission
- Prepare and supply the consultant with necessary documents and information
- Supply good working conditions for the consultant

A.1.6 Consultant and Counterpart

Consultant:
Niels Jespersen from Statistics Denmark

Main counterparts:
Salomão Muianga

A.1.7 Timing of the mission

Two weeks (May 5 – May 16, 2003).

A.1.8 Report

The consultant will prepare a draft report to be discussed with INE before leaving Maputo. He will submit a final draft to INE for final comments within one week of the end of the mission. Statistics Denmark as Lead Party will print the final version within 3 weeks of the end of the mission.

These Terms of Reference were prepared by

Day / / ....

Approved by/in the name of the President of INE

Day / / ....

ANNEX 2 Detailed plan for activities during the mission

Week 1:

Activity	*Participants:*	*Remarks*
General introduction	Destina Uinge, Niels Jespersen, Anastácia Honwana and Salomão Muianga	
Detailed planning and prioritization	Niels Jespersen, Anastácia Honwana, Salomão Muianga and Pedro Miambo and Mogens Nielsen	The purpose of the meeting is to discuss, prioritize and schedule activities. The result is this document.
Infrastructure and network administration	Niels Jespersen, Salomão Muianga and Pedro Miambo and Mogens Nielsen	Evaluate existing installations and discuss/implement changes and possible extensions. Includes among other things: • Printer model • Antivirus – introduction and documentation • Organization/ access to central databases • Web usage statistics • Problem about rebooting the internet modem • Use of watchguard firewall • Web mail
Security and security policy	Niels Jespersen, Salomão Muanga and Pedro Miambo and Mogens Nielsen	Niels and Mogens prepare a draft of the security policy. Afterward the policy should be discussed with INE. Developing and implementing the full policy will be planned after Niels Jespersen's mission.
Develop course material, problem solving guidelines and documentation	Niels Jespersen and Mogens Nielsen	Problem solving guidelines and documentation can be used as part of the course material.

Week 2:

Activity	*Participants:*	*Remarks*
Courses	Niels Jespersen and staff at DISI.	Two sessions. One general course for all the staff at DISI and a specific course for Salomão, Pedro and Anselmo.
Writing of mission report, documentation, policies etc	Niels Jespersen and Mogens Nielsen	Mogens contribute to work on security policy.
Discussions about network solutions for the provinces	Niels Jespersen, Anastácia Honwana, Salomão Muianga and Pedro Miambo, Anselmo Nhane and Mogens Nielsen	
Evaluation	Destina Uinge, Niels Jespersen, Anastácia Honwana, Salomão Muianga and Destina Uinge.	The draft mission report and other material should be discussed and evaluated.

ANNEX 3 Persons met during the mission

- Dr. João Dias Loureiro, Presidente do INE.
- Ms. Destina Uinge, Director Adjunto DICRE.
- Ms. Anastásia Judas Honwana, Head of IT.
- Mr. Salomão Muianga, Network Manager.
- Mr. Pedro Miambo, Deputy Network Manager
- Mr. Hans Erik Altvall, Consultant, Coordinator.
- Mr. Mogens Grosen Nielsen, Consultant

ANNEX 4 PROPOSED SECURITY POLICY

IT Security Policy for INE

A.3.0. Introduction

This IT security policy is expected to be part of a general IT policy. The general policy will include policies for documentation, policies for the use of mail and Internet etc.

The next steps in the process of establishing a security policy will be
a) Discussion of the policy, status and plans for the implementation of the policy, timetable for implementation plans etc. and
b) Approval of the IT security policy

A.3.0.2 Background

Essentially an IT security policy states, in general terms, what is and is not permitted during the operation of a system or application. These rules are expressed below in the form short policies and supplemented with notes.

This draft only covers specific IT security issues. In the discussion about the policy security should also be seen in a broader perspective covering areas like fire damage, water damage and also security in the door locks, physical access controls etc.

It is assumed that 2 persons are performing the day-to-day administration of the network including user administration, installation, inspecting logs etc.

A.3.0.3 Goal of the IT security policy

The general goal is to provide management at INE direction and support for information security. Management should set a clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.

Furthermore the goal of the IT Policy is to ensure:

- Satisfactory level of IT security
- Rational use of IT investments
- Clear guidelines for users in connection with the use of IT
- Rational and effective utilization of IT

A.3.0.4 Use of the Policy

This Policy forms the minimum standards for work related to IT at INE.

A.3.0.5 Distribution

The approved IT Security Policy should be known and accessible to all who use the INE IT system.

A.3.0.6 Approval and updates

The President of INE will approve the IT Security Policy. It is the responsibility of DISI to update the IT Security Policy.

A.3.1. Access to the INE's IT Systems

The reasoning behind policies for user access is to ensure that the individual employee has the necessary access to the INE network to be able to do his/her job. These precautions are also designed to protect sensitive data against unauthorized access, as well to ensure stabile operations, minimize the use of energy as well as the danger of fire. In addition the Web mail access stresses the importance of having secret passwords.

Policy 1.1 Managing network access control

Access to the resources on the network must be strictly controlled to prevent unauthorized access. Access to all computing and information systems and peripherals shall be restricted unless explicitly authorized.

Access to systems must be authorized by the owner of the system and such access including the appropriate access rights must be recorded in an access control list. Such records are to be regarded as highly confidential and safeguarded accordingly.

Notes

- The individual workstations must be equipped with a so-called screensaver password, which is activated within max. 30 minutes. The guidelines for the screensaver-password follow the rules for the logon password. When departing the office, employees must log off the IT network and the equipment in use should be turned off.
- External persons, working at INE, have access only to the data for their projects. It is the responsibility of the Directors of the INE Directorates to inform DISI to which data the external persons should have access.

Policy 1.2 Managing passwords

The selection of passwords, their use and management as a primary means to control access to systems is to adhere to approved rules. In particular passwords should not be shared with any other person for any reason.

Notes

- Passwords must consist of at least 6 characters, one of which should be numeric. Passwords must be changed at least 4 times a year.

Policy 1.3 Monitoring System Access and Use

Access is to be logged and monitored to identify potential misuse of systems and information.

Notes

- The logs should be kept for at least 6 month and should be deleted after 12 months.

A.3.2. Communication and operation of IT equipment

Policy 2.1 Purchases of new hardware

All purchases of new system hardware and new components for existing systems must be made in accordance with the IT security policy and other organization policies as well as technical standards.

Notes

Policy 2.2 Supplying continuous power to critical equipment

An UPS (Uninterruptible Power Supply is to be installed for all critical equipment to ensure the continuity of services during power outages

Notes

Policy 2.3 Use of removable storage medium including diskettes, CD's and USB devices

Only people who are authorized to install or modify software shall use removable media to transfer data to/from the organization network. Any other person shall require specific authorization.

Notes

Policy 2.4 Defending network information against malicious attack

System hardware, operating and application software, the network and communication systems must all be adequately configured and safeguarded against both physical attack and unauthorized network intrusion.

Notes

- Definition of virus: A computer virus is a piece of malicious software that corrupts data, programs or systems.
- There is no 100% effective method of protection against virus. Virus attacks can be especially destructive for data, and thus it is important that a possible attack is reported immediately to the network administration staff.
- All servers and PCs connected to networks must have virus-scanning programs. DISI is responsible for installing and updating these programs. Only employees from DISI may deactivate or uninstall virus-scanning programs.
- It is essential that PCs owned by INE, but not on the network, also have virus-scanning program installed. It is the responsibility of the employee to install and update this program on stand-alone PC’s. Program licenses are issued by DISI.

Policy 2.5 Operation according to documented procedures

The organization’s system must be operated and administered using documented procedures in a manner which is both efficient but also effective in protecting the organizations security. The operation procedures include regularly review of logs by the staff and regularly summary in status reports.

Notes:

Policy 2.6 Rules for storing of data

All users of information system whose job function requires them to create or amend data files, must save their work on the system regularly in accordance with rules for storing data, to prevent corruption or loss through system or power failure.

Notes:

Policy 2.7 Managing backup and recovery procedures

Back up of organizations data files and the ability to recover such data is a top priority. Management is responsible for ensuring that the frequency of such backup operations and the procedures for the recovery are documented and meet the needs of INE.

Notes:

- Definition of a backup. A backup is a security copy of the data from a server, making it possible to backup the data of the server. To "restore" is to re-establish data from a backup. Data files lost by mistake and which are older than one working day, can in most cases be re-established from a backup, though possibly in a previous version.
- Data to be included in the back up should be stored in personal or shared folders. Data in these folders are located at the central server. Backups will not be made of the local hard drives.
- Projects requiring disk space on a server should have established a project area (a shared folder), as project material should not be stored on departmental drives or other places.
- When a project is terminated/completed, DISI should be informed. It is then their responsibility to record the project data on a CD Rom before it is removed from the servers.
- For all disk areas – ordinary data discipline requires that the owner is responsible for removing old or obsolete files.
- Backups are made of the data on all servers, so that the amount that maximally can be lost is the work of a single day (workday). If the system breaks down on a workday, the system should be up and running again within 24 hours after DISI has been informed.
- DISI can re-establish single files upon request of the data owner.
- A disaster recovery plan should be prepared

ANNEX 5 Notes on individual recommendations

REC1: General recommendation 1: A conservative installation and upgrade strategy should be decided.
Installation of new software and upgrading existing software is a resource demanding activity both in terms of manpower and money. It should therefore be decided to carefully consider each new software product introduced and each upgrade contemplated in terms of value added and resources spent. Specifically, the basis of NT on workstations and servers should not be upgraded during 2003, as the upgrade to Windows 2000/XP is very manpower and planning intensive compared to the value gained.

REC2: General recommendation 2: System administration staff should consist of at least two persons.
The day to day tasks of operation of the network add up to more work than one person can accomplish. Furthermore, system administration is very vulnerable in being dependent on only one person. Consequently, at least two persons should be assigned to the work area. Of these, at least one should be an experienced system administrator.

REC3: General recommendation 3: Training should be provided to system administration staff
The skill set of system administrators need to be widened and deepened as the installation gets more complex. The methods of choice for bringing the proper training to the staff is the set of training courses in Microsoft Technologies that lead to the acknowledged MCSE certification. MCSE is short for Microsoft Certified System Engineer. The training should be given to the two persons assigned to system administration. MCSE comprises courses which are offered in Maputo. The training will take up to a year to complete in the staff's free time, but value will be apparent shortly after the training is initiated.

REC4: General recommendation 4: External support should be secured until internal staff is up to speed.
The training will provide more and more value as the courses progress, but until the time when the staff is up to speed with all day to day tasks of operating the network, external support should be secured. Tasks that should be included in the support agreement include: Exchange configuration and administration, General network troubleshooting, Advanced NT system administration, Advice on automating common tasks.

REC5: General recommendation 5: Prepare disaster recovery plan
As the network at INE gets to be a critical resource for producing statistics, the consequences of losing this resource get more serious. Outages and breakdowns can be minimized but not avoided altogether. To minimize consequences and duration of smaller and larger breakdowns, INE should have a disaster recovery plan. Such a plan should cover disasters ranging from broken hardware such as the firewall connecting INE to the Internet to big disasters such as fires in the server room. Questions like "Did you store all backups in the server room during the fire? Sorry, INE is out of business!" are better asked **before** the fire. This plan should be revised regularly and also tested regularly for viability.

REC6: General recommendation 6: Problem solving guidelines.
In order not to solve the same problem twice and to facilitate structured accumulation of knowledge, it is suggested to introduce "problem solving guidelines". An example of a problem solving guideline could be "How to connect my Outlook-Express client at home to read INE mail?".

The outline of a guideline could comprise the following parts: short problem description (how, when and by whom was the problem encountered). Problem resolution (description of steps that solves the problem). Possible workaround (description of how to continue with an alternative solution of the problem).

The description of problem solving guidelines should start immediately. One person should be responsible for adding and updating descriptions. The guidelines should be published on the Intranet in two categories: One for guidelines that describe problems affecting end-users and one for guidelines that are relevant to administrators only.

REC7: General recommendation 7: Modernize INEs Antivirus solution.

The network border between the INE network and the Internet has been secured against virus attacks in the Internet part of the mission. Antivirus software is employed on workstations and servers today in order to guard against viruses entering from the inside via diskettes and cdroms. But the software is old and does not support a centralized administration. It should be seriously considered to implement new antivirus software on workstations and servers in order to guard properly against viruses and other malignant software.

REC8: Internet Recommendation 1: Logging of downtime on Internet connection
It is recommended that outages are logged in a manual log file with information about time, duration and possibly reason for the outage. This log will form the necessary material for evaluating the service provided over a period.

REC9: Internet Recommendation 2: External mail backup
It is recommended that adding an external mail backup service is seriously considered. This requires the cooperation of a service provider, who will agree to accept incoming mail to ine.gov.mz, whenever the service at INE is unavailable to the public Internet. When mail service at INE is restored, mail will be forwarded automatically from the service provider to INE.

REC10: Internet Recommendation 3: Modem removal
Modems formerly used to facilitate dialup access to external mail should be retired from service after the users of the modems have had time to empty their external mailboxes.

REC11: Internet Recommendation 4: Hosting of Web site
The web-site should for the time being stay hosted at Teledata. When and if the site develops into a dynamic database driven site, this decision should be reconsidered. It should be considered already today to contact Teledata in order to get log files of incoming traffic to www.ine.gov.mz in order to analyze usage patterns.

REC12: Internet Recommendation 5: Web mail
The future need to access Exchange from the outside should be considered and evaluated with regard to the added complexity and operational cost of a fully configured Outlook Web Access solution.

REC13: Internet Recommendation 6: Memory in proxy machine
Add memory to the Proxy machine to at least 256 MB in order to improve the performance of web access.

REC14: Internet Recommendation 7: List of recurring operational task
Create a list of recurring operational tasks, and add to that list a monthly task of checking the current version of operating systems and server applications against the current list of fixes from the vendor.

REC15: Internet Recommendation 8: “Out of Office”

It should be considered whether the user-friendly "Out-of-Office" messages should be delivered to the outside.

REC16: Internet Recommendation 9: Limitation on the size of external mail
After a period of a few months, the size limitation of one megabyte on mails should be reconsidered based on experience.

REC17: Administration recommendation 1: Backup procedures and backup policy
Backup procedures should be fully automated and documented. A backup policy should be formulated.

REC18: Administration recommendation 2: Reporting
Monthly reporting of operational incidents should be introduced.

REC19: Administration recommendation 3: Printing model
For administrative reasons the printing model should be systematically changed to Windows printing with central print queues.

REC20: Administration recommendation 4: Use of drive letters
The use of drive letters and access permissions for network files should be standardized.

– REC21: IT policy
An implementation plan should be made. Discussion with the management at INE and approval.

– REC22: Documentation.
User administration, backup and antivirus system should be documented according to standards with operation manuals. There should be operation manuals for administration, backup and antivirus procedures. How to implement the standards at the network administration should be discussed.

REC23: Organization.
There should at least one person present in the network administration unit to answer questions and to ensure stable systems. Two persons must know how to operate each system. One of the two persons should have the main responsibility for the operation of each system.
A:

- Administrator manager,
- responsibility for file server
- firewall/ proxy server
- printer server and reporting

B:

- Backup,
- antivirus,
- installation of workstation,
- helpdesk.

The helpdesk activity includes solving day-to-day problem for end-users. A catalog of frequently asked questions should be introduced. Se notes about problem solving guidelines REC6.

In order to ensure clear responsibility job descriptions should be made.

REC24 Printing model

REC25: Organization /access to central databases

REC26: Reboot cable modem / use of Watchguard firewall

REC27: Reporting

The network administration staff is responsible for reporting to the management of DISI and DICRE every second week. The following items should be included in the report:

1. Status and plans for activities at the network administration area
2. Systems not available.

   System name: ________. Downtime (down/up):_____/______. Reason:_____________
3. Summary of logs (virus attacks, web usage etc)
4. Risks.