

ICT Handbook



FLYKTNINGHJELPEN
NORWEGIAN REFUGEE COUNCIL

Contents

1	Introduction	6
1.1	Purpose	6
1.2	Staffing	6
1.3	Work Description	7
1.4	Training of staff	7
1.5	Support Structure	8
1.5.1	See support flowchart annex	8
1.5.2	Basic support duties of the ICT officer (Level I support)	8
1.5.3	Support duties of HO ICT Dep. (Level II support)	8
2	Cost and Budgetting	8
3	ICT security	10
3.1	Why do we care	10
3.2	Threats in general	10
3.3	Professional responsibility	10
3.4	Avoiding Laptop Computer Theft	10
3.5	Policy based security	11
3.5.1	Only use NRC equipment, not personal computers	11
3.5.2	Do not take laptops home or outside of NRC premises unless it is part of the work description	11
3.5.3	Do not use personal email addresses	11
3.5.4	Do not use of personal removable media	12
3.5.5	Encrypted backup media	12
3.5.6	Cloud storage solutions are prohibited	12
3.6	Password guidelines for 103222nnnn accounts	12
3.6.1	Password rules	13
3.6.2	How to change your password	13
3.7	NRC layered security	13
3.7.1	Layered and 2 Factor Authentication	13
3.7.2	Why we use 2-factor security	13
3.8	Patching of Hardware / Firmware	14
3.9	HO supplied equipment	14
3.10	AV protection	14
3.10.1	What are Viruses?	14
3.11	Anti-Virus Software	14
3.11.1	Update the Anti-Virus Database	14
3.11.2	Run Regular Scans	14
3.11.3	Keep Windows Up-To-Date	15
3.12	In case of virus infection	15
4	Networking	17
4.1	The components of HO supplied network equipment	17

4.2	Network component cabling Guide	17
4.3	Standard network configuration	17
4.4	Available addresses	17
4.4.1	Reference	17
4.5	Local ISP/Landline	17
4.6	VSAT	18
4.6.1	Procurement of VSAT services	18
4.6.2	Astrium procurement process	18
4.6.3	Network guides	18
5	Communication and collaboration tools	18
5.1	Email	18
5.1.1	Email etiquette	18
5.1.2	Size of email attachments	18
5.1.3	Mobile email	19
5.2	Email Resources	19
5.2.1	Contact group	19
5.2.2	Group Email	20
5.2.3	Shared Address	20
5.3	Internet Messaging	21
5.3.1	Skype	21
5.3.2	Lync	21
5.4	When to use which IM tool	22
5.5	Using Public Wi-Fi	22
6	Procurement	24
6.1.1	General guidelines for procurement of new equipment	24
6.2	New Desktops	24
6.3	New Laptops	25
6.4	Printers and scanners	26
6.5	How to properly send out a RFQ	26
6.6	Inventory documentation	27
6.6.1	Naming convention and tracking variables	27
7	User Management	28
7.1	New person entering the office	28
7.1.1	Before a new arrival	28
7.1.2	New arrival	28
7.1.3	Changing position	28
7.2	Hand out of equipment	29
7.3	Person exiting the office	29
7.4	Each user	30
7.4.1	No generic accounts	30

7.5	Removal of equipment containing data	30
8	Computer Management	31
8.1	Minimum hardware requirements	31
8.2	General	31
8.2.1	Copy of NRC's software	31
8.3	Standard NRC software setup	31
8.4	Additional software recommendations	31
9	Personal responsibility of NRC equipment	32
9.1	Warranty	32
9.2	When to fix it yourself, and when not to...	32
9.3	Printers	33
9.4	Ink vs. Laser	33
9.5	Printer placement	34
10	Power supply and protection	35
10.1	Ensuring ground (earth) from start to endpoint	35
10.1.1	Why grounding is so important?	35
10.1.2	Standardize the plugs you use to ensure the grounding path	35
10.1.3	Power strips	35
10.2	UPS	36
10.3	Stabilizers	36
11	Hardware maintenance and cleaning equipment and its components	37
11.1.1	Procedures	37
11.1.2	Frequency and methods	37
11.1.3	Desktops Computers	37
11.1.4	Laptops	38
11.1.5	Printers	38
11.1.6	Scanners	38
11.1.7	Screen / Monitor cleaning	38
11.1.8	Networking equipment cabinets	39
11.1.9	Networking equipment	39
11.1.10	Cleaning tools	39
11.1.11	Cloth	39
11.1.12	Water or rubbing alcohol	39
11.1.13	Portable Vacuum – Blower	39
11.1.14	Cotton swabs	40
11.1.15	Foam swabs	40
12	Annexes	41
1.	Job Description ICT Officer	42
2.	Laptop Acceptance Form	45
3.	Trace Route guide	46

4.	Astrium procurement process	48
5.	How to change WAN IP address	51
6.	Networking Components	55
6.1.	Fortinet Firewall	55
6.2.	Trapeze WLC2	55
6.3.	Steelhead Riverbed	55
6.4.	D-Link PoE Switch	56
6.5.	Wireless Access points	56
8.	What are viruses?	58
8.2.	The various forms of computer viruses:	58
8.3.	Worms and Trojans	58
9.	General Threats	60
10.	Support flowchart	62
11.	Firmware	63
12.1.1	Why does firmware need to be updated?	63
12.1.2	Should I always update my firmware?	63

1 Introduction

1.1 Purpose

The purpose of this Information and Communication Technology (ICT) handbook is to define, develop, and document the information policies and procedures that support organizational goals and objectives.

The policies and procedures provide:

- A foundation for a system of internal controls
- Guidance in current Computer and Network activities
- Criteria for decisions on appropriate IT security
- IT officers with direction and guidance in connection with those IT policies, procedures, and reports that should be uniform throughout the Company.

Information security policies and procedures represent the foundation for the organization's information security program. Information security policies serve as overarching guidelines for the use, management, and implementation of information security throughout the organization.

Internal controls provide a system of checks and balances intended to identify irregularities, prevent waste, fraud and abuse from occurring, and assist in resolving discrepancies that are accidentally introduced in the operations of the business.

When consistently applied throughout the organization, these policies and procedures assure that the information assets are protected from a range of threats in order to ensure continuity and best practice.

All additional departmental or functional policies and procedures written should conform to and parallel the policies in this manual. All changes to policies and procedures are required to be reviewed to ensure that there are no conflicts with the policies stated in this ICT Manual.

1.2 References

- Logistics Handbook
- Document Management Handbook

1.3 ICT strategy/intent/concept of operation

- Centralised incl why centralised?
- Locally managed computers, printers etc
- NRC ICT triangle – Robust, secure, efficient within realistic cost

1.4 Organisation structure

1.5 Staffing

Guidelines for staffing requirements are difficult to define as it depends on how many computers there are, the state of the ICT equipment in question, and how many offices the equipment are spread across.

General suggestions for staffing are as follows:

Size of Mission	Staffing suggestion	Number of locations
-----------------	---------------------	---------------------

1 – 20 computers	External hired assistance	1
20 – 45 computers	1 full time ICT officer	1 – 2
20 – 45 computers	1 ICT officer, with additional external help	3 - 5
45 - 75	1 ICT officer, with additional external help	2 – 3
75+ computers	1 senior ICT officer, 1 junior ICT officer	3+

These guidelines are just a general advisory, and should not be taken as an absolute. If the mission is up and running, functional, and the majority of the ICT officers work is maintenance, then one single ICT officer could be enough to handle 100+ computers, if they are spread over only a few locations. If the mission is expanding, opening a new location, or implementing major infrastructure changes, then additional help could be required.

1.6 Work Description

A template work description for an ICT Officer can be found in [the annex](#)

1.7 Training of staff

It **is** the job of the ICT officer to train users in NRC specific software such as the Portal, the Outlook launcher and Pledge. There are guides available already made to assist with this. Guides are available upon request from HO, or downloadable from the Intranet.

It is **not** the job of the ICT officer to train users in everyday usage of commercial software, such as Word, Excel, Access, Acrobat, etc. If the ICT Officer has the skills, time and is willing; then this is at the discretion of the ICT officer himself or herself, but generally it is the responsibility of the mission to require these skills at time of hiring, or train their staff in office product use by using an external source.

If the Mission feels there is a need to reinforce capacity for non-NRC software, such as the Microsoft Office suite of programs, the ICT department strongly recommends a thorough training need assessment before engaging an external trainer. This ensures resources are directed to areas in greatest need of reinforcement to improve overall performance.

The purpose the assessment is to identify performance requirements as well as the knowledge, skills, and abilities needed by the staff to achieve these requirements. The objective is to identify the gap between skills required and current skills.

Key questions to be considered include:

- What learning will be accomplished?
- What is needed and why?
- Who needs it?
- How will it be provided?
- How much will it cost?
- What changes in behavior and performance are expected?
- Will we realistically get them?

For more comprehensive or in-depth training needs, the HO ICT Department is happy to provide guidance.

1.8 Support Structure

1.8.1 See support [flowchart annex](#)

1.8.2 Basic support duties of the ICT Focal Point (Level I support)

- “Help desk”
- Immediate technical support.
- Front-line problem resolution.
- Installation of software, operating systems, updates and patches.
- Procurement assistance in suggesting suitable equipment and service solutions
- Preparation and deployment of hardware and computers.

1.8.3 Support duties of HO ICT Dep. (Level II support)

- Installation and guidance on baseline infrastructure.
- Specialized technical consulting and services.
- Institutional communication on resources.
- Specialized training, materials and services.
- Policies and procedures.
- Backend tools and management.

1.9 Telecomputing support

How

Whom

When

2 Cost and Budgeting

- Total cost of ownership
- Running cost
- Procurement cost

Cost of hardware

+

Cost of software (office, AV, etc.)

+

Cost of support /divided over/ number of computers (+ travel costs of having support flown out there, potentially external support cost)

+

Electricity (if powered by generator)

+

Cost of internet /divided over/ number of computers

+

Cost of shipping / procurement / storage / **transport**

+

Cost of deployment (all computers need a 1+ hours of love and care before being able to be deployed)

+

Cost of blanket cost of HO services /divided over/ number of computers

- + **Potential external support devices** (Power strip, UPS, Stabilizer)
- + **External peripheral devices** (mouse, keyboard, carry bag, screen)
- + **Printing** (not sure how to spec that, but more computers equals more printing)
- + **Cost of network infrastructure** /divided over/ number of computers
- + **Cost of retirement** (one day the computer will have to be taken out of commission, and this takes several hours of backup, deletion, reformatting, etc..)

Looking at how the big boys do these calculations:

Hardware – 26%

Software – 20%

Support – 41%

Communications – 13%

(source Microsoft estimates 2008)

Some thoughts regarding indirect costs:

Indirect Costs

Indirect costs are all, in some way, related to lost productivity – with direct implications for profitability and competitiveness.

Availability takes precedence over all other requirements: A system is only useful if it's up, running and functioning well! Maintaining high availability requires significant maintenance and management and a pro-active approach.

Hidden costs include:

Downtime – scheduled and unscheduled. All or part of the network is not available to users.

Suboptimal functioning – e.g. inappropriate or outdated applications software, slow computers or poorly trained users.

User-induced problems – e.g. deleting critical files, ignoring warning messages, clicking on pop-ups that install viruses, changing configurations.

"Shadow support" – internal support provided by advanced end users on top of their official job duties. (When these end users are proficient and know their limits, this can save, rather than cost, money, but only if the time they spend on IT saves more than the productivity lost from their normal duties.)

"Futz" Factor - use of computers for non-business purposes (e.g. online games, surfing the Web or personal emails).

"Fiddle" Factor – time spent by users changing the look and feel of their computers e.g. changing the desktop, installing desktop accessories, fiddling with fonts.

Time that is often not tracked or is overlooked – for example, time spent researching purchases and getting quotes; time spent dealing with vendors before a problem is diagnosed and fixed.

3 ICT security

3.1 Why do we care

There are many reasons why you should protect the information on computer, including:

- Ensuring that information remains confidential and only those who should access that information can
- Knowing that no one has been able to change your information, so you can depend on its accuracy (information integrity)
- Making sure that your information is available when you need it (by making back-up copies and, if appropriate, storing the back-up copies off-site)

Computers are an inseparable part of our work today, life that has increasingly become technology driven. Besides hardware, security of the new-age machines is threatened by malicious software, viruses, Trojans etc. all designed to cripple a system. Loss of computer security leads to corruption or loss of data, misuse or theft of information, identity theft and unauthorized use of information, transmission of computer viruses that can affect third parties and can lead to potential liability, services interruptions, security breaches that can threaten safety.

At the end of the day it is the ICT department's job to see to that not only all computers are protected and meet the minimum requirements of the NRC's standard setup, but also that the users store and work with data in a way that protects data from loss, corruption and theft.

3.2 Threats in general

See ["General Threats" annex](#) for in-depth look at the threat picture of NRC

3.3 Professional responsibility

Each staff member is responsible for following the rules and upholding the security guidelines and policies outlined to comply with NRC rules and regulations.

Each staff member of NRC has a personal responsibility to minimize the probability that he or she loses control of confidential information. This applies to printed copies, digital/electronic copies on removable media and storage on personal computers or information sent over email.

Your NRC security focal point or line manager must be notified if they experience loss or theft of information that might be harmful to NRC's reputation or ability to operate, its staff, our beneficiaries or partners.

3.4 Avoiding Laptop Computer Theft

Due to size and portability, laptop computers are especially vulnerable to theft. Staff members should follow the rules set out below. A staff member will be held personally responsible for any NRC laptop computers, equipment, and/or accessories that are stolen or lost during the time they have been assigned to that staff member.

3.4.1.1 *Tips on how to protect your laptop from being stolen:*

1. Do not leave a laptop in an unlocked vehicle, even if the vehicle is in a driveway or garage.

2. Never leave a laptop unattended in plain sight.
3. If you must leave your laptop in a vehicle, the best place is in a locked trunk.
4. Be aware of the damage extreme temperature can cause to computers.
5. Carry your laptop in a nondescript carrying case or bag when traveling.
6. Do not leave a meeting or conference room without your laptop. Take it with you.
7. Never check a laptop as luggage at the airport.
8. Lock the laptop in your office during off-hours or in a locked cabinet or desk when possible.

If a theft does occur, immediately notify ICT and your OPS department.

3.5 Policy based security

3.5.1 Only use NRC equipment, not personal computers

The policy reads:

“Use of private computer equipment is in general prohibited, unless written permission has been granted from local IT and has been authorized by the CD.”

This means that no NRC employee should be using a personal computer in the office.

As simple as the rules reads; no one should come in to the office with their own computer and do official NRC work on it, and then take it (and the data it contains) out of the office back home at the end of the day. Anyone who needs to work on a computer should either have their own NRC owned and administered computer, or share a computer with someone else in the office.

With personal computers, NRC cannot assure that:

- all the software needed is present and legally obtained
- the user is the only person accessing NRC data and resources
- the computer is virus free and uncompromised
- The computer is compatible with NRC ICT resources

3.5.2 Do not take laptops home or outside of NRC premises unless it is part of the work description

The policy reads:

“Because of the high risk associated with laptops (theft, loss, breakage); no user is allowed to take their laptop with them home or outside of the office unless written permission has been given from their manager in writing.”

As the policy reads, no one is allowed to take NRC computers outside of NRC premises unless it is part of their work description and part of their job. No one is supposed to take laptops home for the weekend or overnight unless it is for work.

3.5.3 Do not use personal email addresses

The policy reads:

“Each person in need of an email address will be assigned an official NRC email address.

If this has not happened, consult your line manager or contact IT directly for assistance to receive one.

Anyone working for the NRC should have a @nrc.no email address. Any other NRC address format should be changed as soon as possible for the new format. At no stage should a private email address be

used for official communication. Gmail, yahoo, Hotmail, etc. addresses are prohibited to be used for official communication.

3.5.4 Do not use of personal removable media

The policy reads:

“Removable media (Portable hard drives, USB memory sticks, SD cards, etc.) should be used cautiously. Information that in context could be harmful to NRC’s reputation, ability to operate, or its staff and /or beneficiaries should not be stored on unmanaged removable media”.

There should be no use of personal removable media unless absolutely necessary, and even if that is the case it should only be used for temporary storage. Users should not bring personal memory devices and use for work. If there is a need to use removable media, it should be NRC owned and managed equipment, and should not leave the office and be stored securely in the office or FAM safe after office hours. All media that is used for long-term storage must be encrypted and should be locked away in the FAM safe (or equivalent) during nighttime and after office hours. No one should be walking around with NRC data in their pocket nor bring it outside the premises of the NRC offices.

3.5.5 Encrypted backup media

The policy reads:

“If there is a need for making backups in a department:

- Data can only be stored on NRC owned removable media
- The device must be encrypted
- The device should never leave the NRC premises.
- The device must be stored in the FAM safe (or equivalent) when not in use.”

Any backups should only exist on NRC owned and managed storage media, that has to be encrypted.

The media has to be stored in the FAM safe (or equivalent) when not being in used.

Backup media should never be used for anything other than backup.

3.5.6 Public cloud storage solutions are prohibited

The policy reads:

“There is a general prohibition on storing NRC information on 3rd party cloud solutions (e.g. DropBox, Google Docs, SkyDrive etc.).”

Using any form of cloud based storage solutions is by default prohibited. Just like with removable media we need to control where data is stored, and using online storage solution is thus prohibited.

3.6 Password guidelines for 103222nnnn accounts

Passwords are personal and should never be disclosed to anyone.

If it is suspected that anyone has obtained knowledge of someone’s password, it had to be instantly changed.

The password / passphrase should be remembered (not written down).

It is recommended to use a “pass phrase” instead of a password.

Pass phrases may contain spaces, and are much more secure, and easier to remember.

Examples of pass phrases are:

"My car is very fast!"
"east west north south 1985"
"My kids are the best!"

3.6.1 Password rules

- Passwords / passphrase must be changed every 3 months
- Password /passphrase length must be 14 letters, or more, it can contain spaces.
- You cannot use the same password / passphrase again after it has expired.

3.6.2 How to change your password

- Open your internet browser and go to <https://mail.nrc.no>
- Check the box that says: "I want to change my password after logging on."
- Type in your username (103222???) in the "Domain\user name" field.
- Type in your account password in the "Password" field.
- Follow the instructions and keep in mind that you cannot reuse and old password again.
- When you have typed in your new password, be sure to click the button that says 'Change password', not the 'continue' button.

3.7 NRC layered security

3.7.1 Layered and 2 Factor Authentication

NRC has a multiple layer approach to security:

1. **User account password**
 - a. When you start an NRC computer, you must have a password to be able to enter a user account. No one should be able to just switch on a computer and go straight in to a user account.
2. **User ID and password to access resources**
 - a. System requires 14 character minimum length password / passphrase protection that is changed every 3 months.
3. **Pledge**
 - a. Second layer Software based authentication.

3.7.2 Why we use 2-factor security

An authentication mechanism can use several factors like *what you know* (a password you remember), *what you have* (a smartcard, an OTP generating software solution) or *what you are* (biometrics, retina or fingerprint scans for example). A two-factor or multi-factor authentication system (also known as 2FA, two step verification or TFA) uses at least two of these factors.

The way NRC utilize this for on-line access is to rely on Pledge. You start by entering your user ID and password normally. After that the system creates a unique one-time password (OTP) using the pledge software on your computer or on your mobile device. You type the code and get access to the system. Your Pledge is the "*what you have*" -item as the OTP is directed to that particular device and cannot be created by others.

This eliminates the possibility for someone to access NRC resources by simply using your User ID and password, and essentially makes the system safe from hacking by trying to brute force break your password.

3.8 Patching of Hardware / Firmware

[See Annex](#) regarding Firmware and patching of firmware.

3.9 HO supplied equipment

Never update or flash firmware on any of the equipment supplied to your mission from the head office (or ISP) unless you have been specifically instructed to do so.

3.10 AV protection

3.10.1 What are Viruses?

You can read more in-depth about viruses and malware in the [“What are viruses” annex](#).

3.11 Anti-Virus Software

As part of your layered security, you should have some form of Anti-Virus software installed on all machines. This can be commercially supported editions such as Kaspersky, McAfee, Symantec, F-secure, Webroot, Trend Micro, etc. You can also choose to use a ‘free edition’ of available Anti-Virus protection such as: Microsoft Security Essentials, Avast, AVG, etc.

Always check the license agreement if you consider using ‘free’ applications in an NRC mission. The author - even though it is not commercially sold – commonly copyrights most free antivirus software.

Sadly, there is no "best" anti-virus program. Each may miss something that the other's catch. That is one of the reasons we have listed several, there is no “best one”.

If you do install more than one AV software, you will quickly find that they will conflict with each other, and will cause unpredictable results. It is not recommended to run more than one AV software on a computer at a time.

3.11.1 Update the Anti-Virus Database

Your first step should be to update the virus signature database that came with the installation. New viruses are created every day, and the databases that the anti-virus programs use are being updated as well. You need to get the latest database update for your software before deploying.

Most of the programs have update functions that will locate, download and install the latest databases automatically, make sure that this function is enabled.

3.11.2 Run Regular Scans

It is recommended to periodically run scans of the hard disk(s). When you first install the software, you should run a full scan. Then, depending on how heavily used your machine is, you should run a scan periodically as well. Some programs will allow you to schedule such a scan to happen automatically.

3.11.3 Keep Windows Up-To-Date

Windows Update regularly, enable the automatic update feature.

All software has bugs; some of those bugs are used to create the exploits that virus writers take advantage of to create viruses that can infect your system. As these bugs are found, Microsoft fixes the affected components in the operating system, and makes those fixes available for download and install using Windows Update.

Remember that windows XP will lose all official support in April 2014, as Microsoft will stop producing updates and will no longer support the OS. You should plan to upgrade or decommission any computer running windows XP before January 2014. Contact HO ICT for assistance if you need help in this undertaking.

3.12 In case of virus infection

In case of a virus outbreak, the first steps are:

1. Disconnect the infected computer from the network (to prevent further infection).
2. Inform the user what has happened, and find a replacement computer (if possible) for the user to continue to work on as you take the infected computer in to custody.
 - a. No emails should be sent from the infected computer.
 - b. No removable media should be connected to the computer (to prevent further infection).
3. Inform the office that there is a virus outbreak, to let the other users know to be vigilant for strange behavior of possible infection.
 - a. In case of Skype based viruses, ask your users to shut down Skype until the infection has been contained. Also, consider informing people on the users contact list that a Skype virus might have been sent from the users Skype account.
4. Inform Head Office ICT what has happened, for advice and/or reporting purposes.

Once the immediate danger has been contained:

The best action is to completely reformat the computer in question and re-install operating system and software to be 100% sure. This is cumbersome and time-consuming, but assures that the virus is removed.

Remember to **delete existing partitions** during the windows re-install, and create a new partition to make sure that you remove any boot sector viruses. If you re-use the existing partitions, you run the risk of still having viruses on the hard drive.

Alternatively

If you for whatever reason cannot re-deploy the computer, you must remove the hard drive from the infected computer and run a full virus scan on the hard drive as an externally connected drive with a computer that has a good AV solution.

3.13 Personvern

- Access to data and log's
- Routines for deletion incl how long data should be stored
- Routines and how to handle potential non-acceptable use etc

DRAFT

4 Networking

NRC has as part of a global initiative started to move away from having individual network configurations and hardware to homogenize the network hardware equipment and standardize the network configuration for all the offices. This not only removes many of the network planning and hardware procurement needs from the individual missions, but also assures a consistent global standard, which assures a higher level of security, ease of management and also paves the way for the missions being able to use the online resources based out of Oslo more effectively.

4.1 The components of HO supplied network equipment

See [networking component](#) annex for description of components

4.2 Network component cabling Guide

See [cabling guide](#) annex for a complete overview of standard layout

4.3 Standard network configuration

- Fortinet FW LAN :10.100.X.1
- Steelhead Riverbed 10.100.x.9 and 10.100.x.10 (Primary and management interface)
- Trapeze WLC2 10.100.x.11 with a network mask of 255.255.255.0 , making the Fortinet FW LAN IP 10.100.x.1 the Default Gateway of the LAN
- The Public IP address for the Fortinet Firewall is provided by the ISP

4.4 Available addresses

The addresses that are available to be used for static IP addresses are 20-40 (10.100.xx-20, 10.100.xx.21, 10.100.xx.22, etc.).

Feel free to use these addresses as you see fit, as they are reserved and not given out by the DHCP.

4.4.1 Reference

Standard IP's used on the network

- 10.100.xx.1 – Firewall
- 10.100.xx.9 – River Bed
- 10.100.xx.10 – River bed
- 10.100.xx.11 – Wireless Network Controller
- 10.100.xx.12 – Wireless Network Controller
- 10.100.xx.20-40 – Available for use
- 10.100.xx.50-254 – Used by DHCP for devices on the network

4.5 Local ISP/Landline

In some missions, there is a possibility to use a local ISP for land based internet service to the mission (WiMax, Microwave, Fiber Optics, etc.).

When researching for local internet provision, the ISP must be able to provide:

- A live/real IP address
- 99% uptime (not be dependent on city power, or have down time because of equipment failure or maintenance)
- Offer contention ratio 1:1 connection

4.6 VSAT

The NRC standard for VSAT is using our global ISP Astrium.
The standard technology used is C-Band VSAT.

4.6.1 Procurement of VSAT services

Please contact HO ICT office for guidance and assistance in procuring a VSAT solution.

4.6.2 Astrium procurement process

See annex [Astrium procurement process outline](#)

4.6.3 Network guides

[Perform a trace route](#)

[How to change WAN IP address](#)

5 Communication and collaboration tools

5.1 Email

Each person in need of an email address will be assigned an official NRC email address.
Personal email addresses (Gmail, yahoo, Hotmail, etc.) are **not allowed** to be used for work or work related communications.

E-mail is primarily a mean of exchanging messages, not an archive. If the message contains information and/or attachment that is worthy of preservation, the information should be stored in the document management system.

Information stored in the mailbox is deleted without consideration when the staff member leaves NRC.

5.1.1 Email etiquette

Many are overwhelmed by the sheer volume of incoming e-mails, of which many we could do well without. Every one of us is responsible for not wasting other colleagues' time unnecessarily.
In general, e-mail messages cannot be considered as confidential. Messages to recipients can be compared to post cards, which may be read by outsiders with some effort and insight depending on messaging systems involved in the transport. Internal messages within NRC are confidential to the extent of the recipient's eventual delegated access to another colleague.

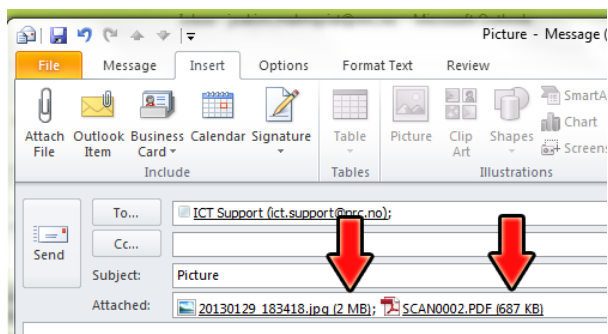
5.1.2 Size of email attachments

Large file attachments negatively affect overall system performance. In areas where the internet connection is slow large attachments are difficult to download.

Compress images whenever possible and review the file size of any attachment before sending it.

A file that exceeds 10MB in size is considered very large even by modern standards; a file that exceeds 1MB in size can take ages to download for a recipient at one of our Field Offices.

Once you attach a file to outlook it is clearly indicated (next to the attachment) what size it is, if it is bigger than 1-2 MB, consider alternative ways of delivering the materiel.



5.1.3 Mobile email

Currently NRC uses the software DME ([read more about DME here](#)) to assure that emails can be read, sent and stored securely on mobile devices. DME assures that the communication between the client and the email server is secured, as well as encrypt the stored emails on the device so that if the device is lost or stolen the information cannot be read. The DME application can be downloaded on iOS, Android and Windows Phone 8 OS, but is not free. If you need a user to have email access on a mobile device, contact HO ICT for licensing and pricing.

5.2 Email Resources

There are 3 kinds of addresses above the standard email addresses that you can create in outlook with NRC

1. Contact group (formerly known as distribution lists)
2. Group email
3. Shared email address

Address Type	Can be used by	Available	Good for
Contact Group	Only the creator	Only on creators PC	Personal use
Group email	Everyone	Everywhere	Large distribution lists
Shared Address	Pre-determined users	For selected users	Generic email addresses

5.2.1 Contact group

A contact group is a list of email addresses that you yourself can create in your outlook. You basically give the list a *name*, and add people from your email address book, and you can now use this to send emails to many people at once. (An address doesn't have to be in your Address Book to be added to the Contact Group. You can add an external address by simply copying and pasting it in, or typing it in manually).

Example: I create a group called 'it people' and assign all my IT contacts to this contact group. The next time I want to send an email to this group I simply type 'it people' in the address field, and the email will go to all people in this list. This is a very useful tool, which can be edited very easily by you yourself. The backside is that only you can use it, it is not available to anyone else.

Read more about how to create a contact group here
(<http://office.microsoft.com/en-001/outlook-help/create-and-edit-a-contact-group-formerly-distribution-lists-HA010354963.aspx>)

5.2.2 Group Email

A group email address is a contact group that we create at HO. This address is available for anyone to be used globally, but can only contain email addresses within NRC.

The standard format for a group email is CC (country code) – Name. So if you want to create an address for all ICLA people in Afghanistan, you could call it AF-ICLStaff@nrc.no. It's important to remember that this address can be used by anyone in any mission as it is publically recognized by the email system.

How to request a group email:

A group email address at HO level must have no less than 7 email addresses (otherwise it is too small to put the work in to, and you can just as easily just manually put in the individual email addresses). It also has to be planned to be used regularly and by many, otherwise it is a lot of work for very little benefit.

Send an email to ICT Support (ict.support@nrc.no), in the email explain that you would like to create a group email address, include the suggested name of the email address in the correct format (CC-Name@nrc.no), and then list the users by name and user ID.

Example:

“South Sudan would like to create the address:
SS-EDUAweil@nrc.no

Sven Svensson – 103222abcd
Bjorn Bjornsson – 103222efgh
Reinar Reinartsson – 103222ijkl
Etc.”

5.2.3 Shared Address

A shared address is a generic email address that can be accessed by several people (it's not associated with one specific person).

With a standard email address you generally open up your outlook (and specific profile) and work with emails (sending / receiving) as a single person, but with a shared mailbox you would have an additional mailbox also being available inside your outlook profile as well as your primary account.

A generic address could be a shared address for recruitment, info, bids, etc.. You would still use the same format as with a group email “country code-name”, so the bids one for South Sudan could be SS-Bids@nrc.no, for recruitment in Cote d'Ivoire could be CI-Recruitment@nrc.no, etc..

If someone sends an email to a generic email address it would show up in several peoples outlook under the shared account folder, and can be read and replied to as a standard email. In most cases the email would be received in the generic email box, and then forwarded to the relevant person.

There should always be a generic info request and contact address existing in each mission (CC-Info@nrc.no), this is the address that should be used as reference in public postings in newspapers, used as a generic contact address on publications, and so on.

There should not be too many of these existing in a mission, try to keep it to as few as possible (cc-info, cc-bids, cc-recruitment).

How to request a shared address:

Send an email to ICT Support (ict.support@nrc.no), in the email explain that you would like to create a shared email address, include the suggested name of the email address in the correct format (CC-Name@nrc.no), and then list the users that should have access to it.

Example:

“South Sudan would like to create the shared address:
SS-info@nrc.no

Accessed by:

Sven Svensson – 103222abcd
Bjorn Bjornsson – 103222efgh
Reinar Reinartsson – 103222ijkl
Etc.”

5.3 Internet Messaging

5.3.1 Skype

Skype is a voice-over-IP service and instant messaging client owned by the Microsoft Skype Division. It is the consumer version of Microsoft Lync.

As this is a very popular IM option many users want to use it, and it is part of the [additional software recommendation](#) list

It is a good idea to advise the user to create a new Skype ID especially for using at NRC as it is important to separate private communication and professional communication, and the contact list very quickly grows. Remember that it is against the NRC ICT policy to use your official NRC address to register social media accounts unless you are representing NRC publicly in this media.

5.3.2 Lync

Microsoft Lync (formerly Microsoft Office Communicator) is a instant messaging client used with Microsoft Lync Server or Lync Online available with Microsoft Office 365. They are replacements for Windows Messenger which was used with Microsoft Exchange Server.

Microsoft Lync is an enterprise software; unlike Windows Live Messenger and Skype, they have a different feature set that is targeted toward corporate environments.

Basic features include instant messaging, Voice Over IP, and video conferencing inside the client software. Advanced features integrate with many other Microsoft software:

- Availability of contacts is based on Microsoft Outlook contacts stored in a Microsoft Exchange Server
- Contact lists can be retrieved from a local directory service, like Microsoft Exchange Server

- Microsoft Office can show if other people are working on the same document
- All communication between the clients is done through a Microsoft *Lync Server* server. This makes communications more secure, as messages do not need to leave the corporate intranet, unlike with the Internet based Windows Live Messenger. The server can be set to relay messages to other instant messaging networks, avoiding installation of extra software at the client side.
- A number of client types are available for Microsoft Lync, including mobile clients.
- Uses SIP as the basis for its client communication protocol
- Offers support for TLS and SRTP to encrypt and secure signaling and media traffic.
- Allows sharing files.

Lync is the preferred way of communication via IM in the NRC workplace between NRC staff
You can only use Lync if you have a @nrc.no email address.

5.4 When to use which IM tool

- When you are communicating with other NRC staff, you should always use Lync.
- Skype should only be used for external or private conversations.

5.5 Using Public Wi-Fi

The number of free public Wi-Fi hotspots is growing, but not every hotspot can provide the protection of a professional network. A laptop, tablet or smartphone's default settings and firewalls may not be enough to keep safe from threats while traveling. Here are some basic tips in assuring that a user stays safe while traveling:

1. Turn off sharing

A user may share a document library, printers or files, or even allow remote login from other computers on the network at the office or in the home. Unless they disable these settings before connecting to a public Wi-Fi network, anyone else in the vicinity may be able to hack into their PC.

a. Windows

Open the advanced sharing settings of the Homegroup section of the Network and Internet settings in the Control Panel. From here, toggle file and printer sharing as well as network discovery to off, This will assure that the computer is not visible to anyone connected to the same network.

b. Mac

Go to System Preferences, then Sharing, and make sure none of the options are checked.

2. Avoid Automatically Connecting to Wi-Fi Hotspots

A smartphone or tablet may be set to automatically connect to any available Wi-Fi hotspot. Not only will this allow a device to connect to public networks without your express permission, it may also be automatically connecting to malicious networks set up specifically to steal information. Most modern smartphones and tablets have this option disabled by default, but this isn't always the case, and it's a setting that should always be double-check.

- Open the Wi-Fi section of the phone's (tablet) settings app. If you don't see an option to disable auto-connecting, you're already safe. Otherwise, turn this setting off.

3. **Force use of HTTPS**

Regular websites transfer content in plain text, making it an easy target for anyone who has hacked into the network. Many websites also offer the use of HTTPS to encrypt the transfer data, but you cannot rely on the website or Web service to automatically enable this feature.

- a. A good tool to use is the browser extension [HTTPS Everywhere, from zscaler](#). With this plugin enabled, almost all website connections are secured with HTTPS, ensuring that any data transfer is safe from prying eyes.

DRAFT

6 Procurement

This chapter lists what to be aware of when carrying out ICT related procurement. Please refer to the NRC Logistics Handbook for information on how to handle the actual procurement including relevant processes.

6.1.1 General guidelines for procurement of new equipment

6.1.1.1 *Who gets a computer?*

Consider users who do not need constant computer attendance to be potential shared users.

A shared user is someone who shares one physical computer with one or more other users.

Each shared user should have their own (password-protected) account on a designated computer, where their desktop, email, settings, files and folders, etc. are stored and protected.

6.1.1.2 *Locally roaming users*

Locally roaming users are users who only use computers periodically (writing weekly reports, occasional documents), or only use the computer to work with email.

These users can use any available computer to access their email via webmail or work with Word or Excel. Locally roaming users should use the 'guest' account when logging on to a computer, or can have a dedicated account on a shared computer.

6.1.1.3 *Laptop or desktop*

Laptops are primarily for mobile users.

If a user is not intended to travel with their computer they should use or share a desktop computer.

A laptop should never be bought for a user out of convenience. Desktops are cheaper, easier to maintain and repair, and harder to steal.

6.2 New Desktops

New desktops should be of a reputable brand (HP, Lenovo, Dell, etc.) and come with at least 1-year warranty on parts and labor.

You should ultimately aim to choose one brand and model, and stick to the same model when procuring more computers in the future. As such, it is important that you pick a model and brand that you know will be around for the near future, and for which spare parts and services can be easily secured. This makes service and support easier, as you do not have to figure out new issues with different models.

Always aim to buy your equipment from a certified dealer if possible, and consider a service agreement with the vendor if you procure a large number of desktops. Your computers should have an expected lifecycle of no less than 3 years.

In today's market, you can also consider buying smaller desktops such as the [Intel NUC](#), or the [Lenovo ThinkCentre M series](#) (among others). These desktops have a very small footprint and low power consumption. You can always talk to HO logistics or the roving ICT adviser if you need guidance or help with selecting a model and specifications.

Minimum standard specs

- Intel Core i5 or better
- 85% Energy Efficient PSU
- 4 GB DDR3 minimum
- SATA HD
- integrated video card with DVI
- gigabit Ethernet card

- Wi-Fi card 801.11 b/g/n (Optional depending on setup)
- Window 8 Pro
- 19" WXGA Digital Flat Panel with DVI
- Mouse should be optical and USB
- Keyboard should be USB

6.3 New Laptops

New laptops should be of a reputable brand (HP, Lenovo, Dell, etc.) and come with at least 1-year warranty on parts and labor.

You should ultimately aim to choose one brand and model, and stick to the same model when procuring more computers in the future. As such, it is important that you pick a model and brand that you know will be around for the near future, and for which spare parts and services can be easily secured. This makes service and support easier, as you do not have to figure out new issues with different models.

Always aim to buy your equipment from a certified dealer if possible, and consider a service agreement with the vendor if you procure a large number of desktops. Your computers should have an expected lifecycle of no less than 3 years.

Consider how the laptops will be used, and in what environment they will be running.

Large laptops (17" and above) are not very portable, though they are easier to carry around than a desktop computer. The cheaper ones are usually low-powered and useful for people that just want to do basic work on a bigger screen but do not plan to carry it around.

Midsized laptops (13"-16") these laptops are all-around, affordable laptops for the average user. They have a pretty big range in price and power, so you can almost always find what you're looking for. They're great for people that want a simple laptop but want a lot of USB ports, a CD drive, fair battery life and some power. They're more portable than large laptops, but still will carry a noticeable heft in your backpack at around 2-3 KG's.

Ultrabooks (Usually 14" and smaller) you can get an ultrabook, which is a super slim, super light, moderately powerful machine built for the average user. These are great if you are willing to sacrifice, a few USB ports and a DVD drive in the name of portability. They weigh about 1-2 KG's, carry enough power for all your basic activities, and usually have a great battery life. These are built for people that travel a lot, and are not the best choice for everyday deskwork.

Small laptops and netbooks (Usually 12" and below) These are ultra cheap, ultra portable, and ultra low power. They're really only good if you're looking for extreme portability, and are willing to sacrifice quite a bit of power to do so. Don't expect to do more than simple web browsing and email on these machines, and even then, you can expect it to have a bit of lag to it. These models are not recommended for everyday work.

6.3.1.1 Ports

When it comes to the ports in your laptop, you're going to be much more limited than on a desktop, so it's important you know what you're getting. How many USB ports is needed? Does the model you're looking at have USB 3.0? Does it have an SD card slot for camera photos? DO you need Ethernet, or a VGA, DVI, or HDMI port for connecting an external monitor? This can fluctuate a lot from laptop to

laptop, and the smaller your laptop, the fewer ports it's going to have (ultrabooks are particularly low on ports, since they're so thin). You can always get a USB hub if you need more ports at home, or a USB SD card reader for your photos, but just know that the more ports you actually have on the computer, the more versatile it's going to be.

Screen Quality

Check both the screen's resolution (higher is usually better) and its quality; it should be easy to see the difference when compared with the screen on a cheap laptop.

Heat Production

Laptops can get very hot, especially if you are using them (improperly) on your lap. This is going to be something you can only really read in reviews, but keep an eye out for laptops that overheat even when they are used properly on a desk. Make sure that the laptop has rubber feet on the bottom that gives heat room to escape when set on a flat surface, and that it has good fan placement and airflow to keep everything running at a safe temperature.

A Webcam

Make sure your laptop comes with a built-in webcam. Most should, but not all will, and this is an easy component to forget.

A Lock

If you plan on locking the laptop to a desk, check and make sure your laptop has a hole for a desk lock.

6.4 Printers and scanners

Read about printers in the [printer section](#)

6.5 How to properly send out a RFQ

All guidance in procurement can be found in the NRC Logistics Handbook, available on the intranet.

6.6 Inventory documentation

There has to be a documented inventory of all your ICT equipment. Currently NRC does not offer a tool for this, so you are free to use whatever works the best for you, most commonly an Excel workbook is a good suggestion. The inventory should be used primarily to keep track of what equipment you have, serial numbers, model numbers, warranty information, etc., but can also include serial numbers of software, location of the equipment, who the equipment is assigned to (name, department, title, etc.).

It is recommended to keep inventory of all sorts of equipment ranging from computers, handsets, printers, scanners, networking equipment to mobile phones. Be sure to keep the inventory updated and if any changes are made to hardware or software make sure that the inventory reflects these changes.

Your inventory should also **include any software** paid for by the NRC mission, including serial number and reference when the software was procured and which computer it is installed on.

6.6.1 Naming convention and tracking variables

You should have a naming convention to ID / label all your equipment.

A good suggestion is to take the name of the country, the office, the item category and a number.

If you are in South Sudan (SS) in the Juba Office (JUB), and have a desktop computer (DSK) name it: SS-JUB-DSK-001. If you are in Somalia (SOM), in the Mogadishu office (MOG) and have a laptop (LPT), name it: SOM-MOG-LPT-001.

Using a system like this you can simply look at a label and know what office it belongs to, what it is and which mission it belongs to.

6.6.1.1 Suggested tracking variables:

- **ID**
 - This is where you put your ID (e.g. KEN-NBO-PRT-023)
- **Category**
 - What it is (e.g. Computer, Laptop, Printer, etc.)
- **Model**
 - Model name of the equipment (e.g. EliteBook, LaserJet, etc.)
- **Manufacturer**
 - (e.g. Dell, HP, D-Link, etc.)
- **Year of manufacturing**
- **Serial Number**
- **User**
 - Who the equipment is assigned to
- **Main Location**
 - What office the equipment is located in
- **Department**
 - Department of location (e.g. Finance, ICLA, etc.)
- **Status**
 - Condition of the equipment (New, Used, Broken, in storage etc.)
- **OS**
- **Office Ver.**
- Version of MS Office (e.g. Office 2007, Office 2010 Pro, etc.)
- **Portal Launcher**
 - If launcher is installed, and which version
- **Outlook Launcher**
 - If launcher is installed, and which version
- **AV**
 - If and which version of AV is installed
- **Pledge**
 - Which version of Pledge is installed
- **Java**
 - Version of Java
- **Adobe Reader**
 - If installed and if so which version
- **Team Viewer**
 - If installed and if so which version
- **Lync**
 - If installed and if so which version
- **Software summary**
 - If there is any additional software installed (SPSS, Mopenzi, Adobe Acrobat, etc.)
- **Admin password**
 - If there is an admin password, what is it
- **Comments**

7 User Management

7.1 New person entering the office

7.1.1 Before a new arrival

- Inform IT in good time that someone is coming so that a computer can either be prepared or procured
- Each new arrival must - if not already existing - have a @nrc.no email address to be able to utilize the ICT systems and communicate.
- Inform IT if any previous data is necessary to be transferred to the new user's computer. Either from previous user whose position is being replaced, or common data necessary for the position.
- If any supplementary equipment is needed (Laptop bag, external screen, mouse, external keyboard, hard drive, USB key, camera, etc.); make sure that this equipment is procured in advance before the arrival of the new user.

7.1.2 New arrival

- If the new person needs a computer from IT, they need to come to the IT office and fill out the Handover Document for Equipment form. ([example equipment acceptance form](#))
- No equipment will be handed over without proper documentation. ([example equipment acceptance form](#))
- If the equipment needs to be sent to the field or handed out by a 3'd party: said person must sign the handover form and becomes responsible for assuring that proper documentation is filled out when handing over the equipment to the new user. Documentation should be returned to OPS for filing.
- Each new person needs to have a briefing from IT
 - Presenting the NRC ICT Policy
 - How to connect to the network and subsequently the internet and email using the Outlook launcher and the portal launcher.
 - Email
 - How to access webmail
 - How to change the email password and explain the frequency of password change
 - Make sure that the user creates a password for their computer account
 - How to access the intranet
- Computer inventory should be updated to reflect the change of ownership of computer
- If emails from a previous user was supposed to be delivered IT should aid in making the PST file accessible from users outlook
- IT needs to inform HR of new arrivals email address (send to HR Representative)

7.1.3 Changing position

- Make sure that the title is changed in the AD to reflect the new position by sending the change information to ICT Support (ict.support@nrc.no), referring to the name, user ID, previous title and new title.

- Make sure that any rights associated with Intranet Services, Document Management System, Agresso, etc. is changed /added/removed according to the position.
- If the person is switching department, make sure that any ICT equipment that belongs to the previous department is returned, and new equipment is issued or changes ownership to the new department.
- Make sure the inventory reflects any changes in equipment, location of said equipment and title change.

7.2 Hand out of equipment

Before any computer equipment is handed out ICT department must assure:

- That the computer has the latest edition of all NRC proprietary software
- That all updates, patches and fixes have been applied
- That the condition of the equipment has been properly documented and is reflected in the inventory
- That the proper handover documentation is filled out ([example equipment acceptance form](#))
- That the staff member understands the [responsibility associated with using NRC equipment](#)

7.3 Person exiting the office

When someone is permanently leaving the office

- Paperwork and an inspection of the state of the equipment needs to be done.
- User should be ready to hand over the computer no later than on the morning of the last day.
- Make sure that documents exists that supports the fact the equipment initially signed out from IT / OPS has been handed back.
 - This should include any form of equipment such as ;
 - Computers
 - Satellite phone
 - Mobile phone
 - Cameras
 - Peripheral equipment (bags, cases, mice, keyboards)
 - Etc.
- Make plans in advance, for what needs to be done with potential data remaining on the computer handed back. IT will help move and store data needed to be handed over to the successor or manager (within reason), but only if IT is informed prior to handing the equipment back.
- Once returned to IT; the user account will be permanently erased from the computer with no possibility of getting it back. No data will remain from the previous user unless specifically requested.
- It is the responsibility of the department manager to inform IT of what to do with the data on the returned computer; IT will not keep unsolicited copies of backups without having been instructed to do so.
- Departments should return equipment to IT for reconditioning and service even if said computer is supposed to remain in same department.
- Departments are not to keep computers stored in lockers or drawers in their offices.
- All unused computers should be stored in the IT department.

- If specific computer is needed to return; IT will earmark the computer and return it upon request.

7.4 Each user

- Each user should have an individual account created on a designated computer.
 - This account must be password protected.
- Account should be named after the users (either first name, or first and last name) to easily help identify who the account belongs to.
 - Not a generic name such as 'Finance' or 'Admin'.
- Each user account should contain a setup of the intended user's email account through MS Outlook as well as Pledge, installed and registered with the account of the intended user.
- A [locally roaming user](#) should either have a properly named account set up on a shared computer or use the guest account on a computer.

7.4.1 No generic accounts

It is prohibited to use a generic account for the ICT systems, all User ID's must be for one person only, and cannot be shared or named with the title of the function of the position.

7.5 Removal of equipment containing data

Any equipment that contains any form of data storage (internal hard drives, flash drives, memory cards, smart phones, portable hard drives, etc.) needs to be securely erased before being disposed of / donated / or shipped to another mission.

Be sure to use a specific tool that is especially written to permanently erase residing data traces.

When you delete a file of a storage device, the operating system does not really remove the file from the disk; it only removes the reference of the file from the file system table.

The file remains on the disk until another file is created over it, and even after that, it might be possible to recover data by studying the magnetic fields on the disk platter surface.

Before the file is overwritten, anyone can easily retrieve it with a disk maintenance or an undelete utility.

There are several problems in secure file removal, mostly caused by the use of *write cache*, construction of the hard disk and the use of data encoding. It is necessary that you use a software that assures that all traces are permanently eliminated.

One suggestion is using 'Eraser' (<http://eraser.heidi.ie/>) which is a freeware solution available for download.

8 Computer Management

8.1 Minimum hardware requirements

Standard minimum specification when procuring a computer is:

- Dual core Intel processor
- 4GB RAM (minimum)
- Wi-Fi capability B/G/N
- Windows 8 Pro (operation system)
- Microsoft Office 2013 (Std. Edition or above)

8.2 General

It is generally prohibited for an individual user to install software, screensavers, games, media players, 'apps', etc. onto NRC computer equipment. All software has to be legally obtained and licensed to The NRC Mission, illegal and trial copies are strictly forbidden.

8.2.1 Copy of NRC's software

With most software, there are licenses, which states NRC's right of use.

The licenses are NRC property, and do not follow the individual user, hence, all copying of NRC's software is prohibited.

8.3 Standard NRC software setup

- Windows 8 Pro edition (32 Bit or 64 Bit edition)
- MS Office 2013
 - Standard edition or above.
 - 32 bit version, not 64 bit version as it is incompatible with some of NRC security software solutions
- Java (latest edition available)
- NRC Portal launcher
- NRC shield protected outlook launcher
- Pledge
- Adobe Acrobat Reader (latest edition available)
- Microsoft Security Essentials (Antivirus protection)
- Lync

8.4 Additional software recommendations

- [7Zip](#) (freeware compression software)
- [CCleaner](#) (cleaning software)
- PDF Creator software (e.g. [Cute PDF](#))
- Team Viewer (Remote access support tool)
- Skype (IM software)

9 Personal responsibility of NRC equipment

All computers and related ICT equipment and accessories are NRC property and are provided to the staff members for a period of time as deemed appropriate by the mission. As a condition of their use of the computers and ICT equipment, staff members must comply with and agree to all of the following:

- Prior to being issued NRC equipment, staff members will sign the appropriate documentation and agree to all outlined policies.
- Staff members should NOT attempt to install software or hardware or change the system configuration including network settings without prior consultation with the ICT Dep.
- Staff members are expected to protect equipment from damage and theft.
- Each staff member is monetarily responsible for any hardware damage that occurs outside NRC premises and/or software damage (including labor costs).
- Staff members will not be held responsible for computer problems resulting from regular NRC-related use; however, staff members will be held personally responsible for any problems caused by their negligence as deemed by the management.
- Staff members will provide access to any laptop computer, equipment, and/or accessories they have been assigned upon the management's request.

9.1 Warranty

Just about all products on the market today come with a standard manufacturer's warranty, which typically covers your purchase for one year. The majority of minor malfunctions occur within this first year. If your equipment is under warranty, always contact the manufacturer or the supplier to see if they will help you fix your problem.

You of course have to be sensible with what you are asking for, and what the cost for the repairs are worth. If you are trying to exchange a broken part that costs \$25 but the shipping costs you \$120 then perhaps the better way is to simply buy the new part and have it shipped to you. You might also be located in a place where it is difficult to send items, or where there simply isn't any service provider available, then you have to evaluate if it is worth your time and effort to have the item repaired or if it is simply cheaper and quicker to procure a new item instead.

When you procure new equipment, always ask about the warranty so that you are prepared if something would happen. If you have 3^d party repairs made you will most certainly void any warranty, this is also the case if you yourself buy replacement parts and try to fix it yourself.

Always make a judgment to what the complete cost of replacing or fixing something will end up being. Your time, transport, shipping, and even the cost of not having the functional equipment available to those who need it has to be part of your calculation of the best way forward.

9.2 When to fix it yourself, and when not to...

If you are fully confident in that you can perform the repair, and have the spare part and expertise, perform the repair yourself, but when you are feeling that you are out of your depth, always ask your manager if they agree with your assessment. You are not a printer repair expert, so if the problem is

anything above jammed paper or a stuck toner, seriously consider calling in a professional to avoid making the problem worse than it is.

If you have the opportunity, see if there are any companies in your area that offer contractual repair services. If you have many printers, copiers, etc. that have regular issues it is more cost effective to outsource the repairs and maintenance, than it is for you to try to manage it yourself.

Never perform repairs yourself that you are not sure that you can manage before you start doing them, there are many guides and message boards online that will give insight how to best deal with many common repair issues, and remember; if you break it beyond repair trying to repair it – then you are economically responsible for replacing the equipment.

9.3 Printers

- Printers at NRC are for work related printing only
- If you have big printing needs (more than 200 copies of something), contact the ops department to raise a PR to have a local printing company perform the printing to save time, cost and toners.
- To the furthest extent try to print double sided copies
- If available, use the 'economy mode' to save on paper and toners (usually found in the settings of the printer)

Only use color printers where it is needed, otherwise use black and white laser printers.

9.4 Ink vs. Laser

Ink Jet printers should only be chosen if there is a specific need to print images of high quality or an individual user needs to have a printer/copier/scanner for themselves out of security reasons. Even though Ink Jet printers are cheaper and more convenient at face value, the running cost (ink), low volume capability and tendency to break makes it an inferior choice to a laser 9 times out of 10. A laser printer is faster, can handle higher workloads, is cheaper per printed copy, and often have networking capabilities available as a standard option.

- Many "intelligent" ink cartridges contain a microchip that communicates the estimated ink level to the printer; this may cause the printer to display an error message, or incorrectly inform the user that the ink cartridge is empty. Some inkjet printers will refuse to print with a cartridge that declares itself empty, even though it is not.
- Many inkjet printers have lower initial purchase prices than laser printers, but the cost per page when using original ink is usually significantly higher compared to a laser printer.
- Inkjets use solvent-based inks which have much shorter expiration dates compared to laser toner, which has an indefinite shelf life.
- Inkjet printers tend to clog if not used regularly, whereas laser printers are much more tolerant of intermittent use.
- Inkjet printers require periodical head cleaning, which consumes a considerable amount of ink, and will drive printing costs higher especially if the printer is unused for long periods.

- Inkjet printers have traditionally produced better quality output than color laser printers when printing photographic material. However, laser technologies have improved dramatically over time, and are practically equal to ink today and fully acceptable office needs

When procuring printers, first have a look at what is available as far as black & white as well as color laser printer goes, and plan to share printers across the network instead of assigning individual printers to single users.

When looking at printers, compare:

- Initial cost
- Cost per page
- Total cost of ownership
- Print speed
- Duty cycle
- Paper tray capacity
- Double sided printing capability
- Network connectivity options

9.5 Printer placement

If you are procuring a printer, always in first hand plan to procure a network printer that many people can share, and always try to find the most strategic place to keep it. Having a network printer on someone's desk will create unnecessary traffic and interruptions to the user whose desk the printer resides. Try to place the printer somewhere it will not create a traffic jam, as people tend to stand by the printer waiting for printouts. Stay away from door openings, or heavily trafficked areas.

If you have several offices sharing a printer, consider placing the printer in a hallway to give equal distance from all users' desks. By forcing the user to walk over to the printer, you eliminate *convenience printing*, as many will opt to read on screen instead of having to get up and walk over to the printer to get their printed material.

With a sufficiently sized printer, one network printer can service several departments, enabling you to buy a more capable machine, with a higher duty cycle, bigger paper trays and faster printouts, than having several smaller printers spread across the office.

10 Power supply and protection

10.1 Ensuring ground (earth) from start to endpoint

10.1.1 Why grounding is so important?

Earthing/grounding of electrical systems is required for a number of reasons, principally to ensure the safety of people near the system and to prevent damage to the system / equipment itself in the event of a fault. The function of the protective conductor, or earth, is to provide a low resistance path for fault current so that the circuit protective devices operate rapidly to disconnect the supply.

One of the biggest advantages of grounding electrical currents is that it protects your equipment as well as generators, your office and everyone in it from surges in electricity. If lightning was to strike or the power surges for whatever reason, having your electrical system grounded will mean all of that excess electricity will go into the earth — rather than frying everything connected to your system.

It is VERY important that all your equipment and electrical outlets are properly grounded.

10.1.2 Standardize the plugs you use to ensure the grounding path

It is very common practice to have several kinds of electrical plugs in the office; the problem with this is that you will most likely break the path of the ground current using a series of cables with different connectors.



It is simple, quick and cheap to procure loose electrical connectors to standardize your office electrical provision. By buying quality, replacement plugs you, not only assure that all your plugs are of the same model and standard, but also ensure that the ground path is not broken.

10.1.3 Power strips

Low quality power strips should be replaced with high quality power strips, preferably models that have an on/off switch, as well as replaceable fuse - if there is ever a short circuit or over voltage spike. Since all connectors should be standardized plugs, there is no need to have multi-plug capable junk models.

Good example



- Thick quality power chord
- Proper ground circuite

Bad example



- Flimsy plastic
- Multitude of sockets models

- Quality housing
- On / Off switch
- Standardized plugs (in this example US plugs, but yours should obviously be according to the standard of the country you operate in)
- Exchangable Fuse for spike protection
- Thin cable
- Proper grounding is questionable
- Clearly a cheap model built with little to no quality standard assurance

It is also important that users stop using the power strips as their personal charge stations. Make sure that there is sufficient amount of plugs available for all intended equipment, and advice the managers to tell the users that they are not allowed to unplug cables as they see fit.

One suggestion could be that the office supply a couple of multi-model-plug power strips in a common area where users are allowed to charge their cellphones, computers, mp3 players, etc. Perhaps even make it an official rule that you are not allowed to tamper with the cables in the office at all, but only at the common area charge stations.

This would assure minimal wear & tear of the equipment, and guarantee that all equipment is connected and properly grounded.

The power strip pictured above having an On/Off switch also assures that once the power strip in question is shut down, the user can assure that the power has truly been turned off, so that monitors and printers will not stay on after closing. This aid in prolonging the life of equipment and assuring that no unnecessary equipment is running after closing hours.

10.2 UPS

For desktop computers an Uninterruptable Power supply (UPS) is recommended to protect the equipment and aid the user in saving open documents and correctly shut down the computer in case of power loss.

A UPS is a piece of equipment that contains a small battery that provides a computer with a few minutes' worth of electricity in case of a power outage. The UPS is designed to aid in closing the computer down correctly, not to continue to work for as long as the battery continues to feed electricity. If the battery is continuously drained the longevity of the UPS will quickly diminish, and the UPS will stop to function as he batteries are worn down

10.3 Stabilizers

A stabilizer should be in front of all electrical equipment regardless of what or where the equipment is located. A stabilizer is a cheap protection unit that takes fluctuating electricity, "cleans" it, and makes it 'stable'. It also protects from spikes and low voltage. It is highly recommended to always keep all equipment behind a stabilizer.

11 Hardware maintenance and cleaning equipment and its components

11.1.1 Procedures

When you are carrying out cleaning of ICT equipment the following procedures should be observed:

- You must consider health and safety regulations before attempting to clean any ICT equipment.
- You must turn off power sources and disconnect the electricity before cleaning begins.
- You should always follow manufacturer and organizational guidelines on cleaning equipment.
- You must make sure that your hands are dry when working with electrical equipment.
- Never spray or squirt any liquid onto any equipment component. If a spray is needed, spray the liquid onto a cloth and then use that cloth to rub down the component.
- You can use a vacuum to suck up dirt, dust, or hair around the computer on the outside case. However, do not use a vacuum for the inside of your computer as it generates a lot of static electricity that can damage the internal components of your equipment.
- When cleaning a component or the computer, turn it off before cleaning.
- Be cautious when using any cleaning solvents; some individuals may have allergic reactions to chemicals in cleaning solvents and some solvents can even damage the case. Try to always use water or a highly diluted solvent.
- When cleaning fans, especially the smaller fans within a portable computer or laptop it's suggested that you either hold the fan or place something in-between the fan blades to prevent it from spinning.
- Spraying compressed air into a fan or cleaning a fan with a vacuum may cause damage or back voltage to be generated.

11.1.2 Frequency and methods

Depending on the environment that your equipment operates in determines how often you should clean your equipment. If your equipment already has a layer of dust is a fair indicator of that you are not cleaning it often enough.

11.1.3 Desktops Computers

The outside/cover of the computers should be swept cleaned by the cleaning staff on a daily/weekly basis, this includes the monitor, keyboard as well as the physical computer. If this is not being done; talk to the appropriate manager and ask them to include dusting the desktops as part of their routines.

The desktops should be physically opened and cleaned either through vacuuming or blower no less than once every 6 months. If the desktop is in a particularly dirty environment the frequency might have to be increased. Use best judgment and common sense to set frequency of internal cleaning.

When cleaning the motherboard from dust, dirt, or hair is to use compressed air. When using compressed air, hold it in the up-right position; otherwise, it is possible chemicals may come out of the container that could damage or corrode the Motherboard or other component within the computer. Also, ensure when using compressed air that you always blow the dust or dirt away from the motherboard, or out of the case.

Do not use a standard electricity powered vacuum as it can cause a lot of static electricity that can damage the computer. When using the vacuum it is vital that you stay a couple inches away from the motherboard and all other components to help prevent contact as well as to help prevent anything from being sucked into the vacuum. Ensure that you do not remove any small components with the vacuum such as jumpers.

11.1.4 Laptops

As the condition of laptops depends on how and where they are being used you have to use best judgment and common sense to set the frequency of internal cleaning. They should be cleaned out thoroughly no less than once a year. In very dirt environments and frequent usage in the field it might be best to physically open up the laptop and remove dust, hair and other particles. If the laptop is commonly used in a fairly clean environment it might be enough to simply use the blower to clean out the insides through the air intakes and exhaust. Sometimes you might have to remove the keyboard and clean it out thoroughly. Be careful not to let the fans spin from the airflow of the cleaning as it might create reverse current.

11.1.5 Printers

Printers need to be cleaned out just as computers need to on the inside as well as on the outside. The heavier use of the printer the more frequent the cleaning should be performed. Under normal conditions a printer should be cleaned every 2 – 3 months.

There are 2 forms of cleaning you can do on a printer:

Physical cleaning; as in opening the printer up, removing cartridges and using a combination of blower and cloth to remove dust and excess toner powder. First, make sure to turn off the printer before cleaning it. Dampen a cloth with water or rubbing alcohol and wipe the case and each of the buttons or knobs on the printer. As mentioned earlier, never spray any liquid directly onto the printer.

Self-Cleaning; access the self-clean options by moving to your control panel, then clicking on the printer, then clicking on the button/ tab for “maintenance” within which there should be an option to clean your cartridge/toner. Once the printer has finished cleaning the cartridge/toner it often then spits out a printed page for you to check. This process is repeatable as many times as you can bare to get the cartridge back to full functioning, not usually much more than once or twice generally.

11.1.6 Scanners

Clean a flatbed scanner's surface by spraying a window cleaner onto a paper towel or cotton cloth and wipe the glass until clean. As mentioned earlier, never spray a liquid directly onto the component.

To clean the outside of the scanner, the same towel or cotton cloth can be used.

11.1.7 Screen / Monitor cleaning

Unlike a computer monitor, the LCD or flat-panel display is not made of glass, therefore requires special cleaning procedures.

When cleaning the LCD screen it is important to remember to not spray any liquids onto the LCD directly, press gently while cleaning, and do not use a paper towel as it may cause the LCD to become scratched.

To clean the LCD screen we recommend that you use a non-rugged microfiber cloth or soft cotton cloth. If a dry cloth does not completely clean the screen, you can apply rubbing alcohol to the cloth and wipe the screen with the damp cloth. Rubbing alcohol is used to clean the LCD before it leaves the factory.

It is recommended to use a blower and clean out the insides from dust particles once every 6 months in normal office conditions, more frequently if the screen is in a dusty environment.

11.1.8 Networking equipment cabinets

The frequency of cleaning the network equipment cabinet depends on the environment of the location of the equipment. In some places the air filter of the cabinet will keep the inside clean enough. It is however recommended that you shut down the equipment at least once every 6 months and vacuum or blow the cabinet clean and use a cloth to clean out all of the equipment as well as wipe the cables clean from any dust particles that might have accumulated.

If the equipment is located in a very dirty environment the frequency might have to be increased. In some extreme cases the cleaning should be done every 2-4 weeks. There should never be a layer of dust on the equipment, and be sure to frequently clean the air filters to assure free airflow through the cabinet.

11.1.9 Networking equipment

Wi-Fi Routers, access points and other peripheral network equipment can usually be kept clean with a cloth as they commonly have fan less passive cooling. Be sure to at least blow clean these items once every 12 months. If they are in a particularly dusty environment this frequency might have to be increased, use best judgment and common sense to set the best frequency.

11.1.10 Cleaning tools

Although many companies have created products to help improve the process of cleaning your computers and equipment, you can also use household items to clean their computers and peripherals. Below is a listing of items you may need or want to use while cleaning your equipment.

11.1.11 Cloth

A cloth is the best tool used when rubbing down equipment; although paper towels can be used with most hardware, it's recommended using a cloth whenever possible. Use a cloth when cleaning components such as the outside of the case, a drive, mouse, etc. You should not use a cloth to clean any circuitry such as motherboard or insides of equipment since they can generate static that can damage electronics.

11.1.12 Water or rubbing alcohol

When moistening a cloth, it is best to use water or rubbing alcohol. Other solvents may be bad for the plastics used with your computer.

11.1.13 Portable Vacuum – Blower

Sucking or blowing the dust, dirt, hair, and other particles out of a computer can be one of the best methods of cleaning a computer. Over time, these items can restrict the airflow in equipment and cause

circuitry to corrode. Do not use a standard vacuum as it can generate a lot of static electricity that can damage your computer.

The best go-to equipment is a blower or a portable computer vacuum.



Portable Blower



Computer Vacuum

11.1.14 Cotton swabs

Cotton swabs moistened with rubbing alcohol or water are excellent tools for wiping hard to reach areas in your keyboard, mouse, and other locations.

11.1.15 Foam swabs

Whenever possible, it is better to use lint-free swabs such as foam swabs

12 Annexes

[Work Description for ICT Officer](#)

[Laptop Acceptance Form](#)

[Trace Route guide](#)

[Astrium procurement process](#)

[How to change WAN IP address](#)

[Networking Components](#)

[Cabling Guide](#)

[What are viruses?](#)

[General Threats](#)

[Support flowchart](#)

[Firmware and patching](#)

1. Job Description ICT Officer

JOB TITLE: ICT Officer
DUTY STATION:
CONTRACT PERIOD:
STARTING DATE:
REPORTING TO: OPS Manager

1. BACKGROUND

THE NRC PROGRAMME

<Complete with paragraph detailing programme background and scale>

2. ROLE, TASKS AND RESPONSIBILITIES

JOB PURPOSE

Working with ops manager, and head office ICT personnel drive the use of technology in the organization, provide effective IT systems, help develop and implement IT standards and policies, and provide technology support and solutions to meet the needs of the organization.

The ICT officer will manage the overall technology infrastructure for NRC including planning, implementation and management of the software applications and hardware infrastructure that support NRC operations. ICT officer will be involved in systems administration including general computer support, upgrades, software installations, license management, network and printer support, deployment of equipment, manage inventories, end user support. Provide user training in use of common business applications, and training staff in using NRC ICT systems.

TASKS AND RESPONSIBILITIES

Equipment

- Configure and deploy new and refurbished workstations, laptops and peripheral equipment.
- Install, troubleshoot, repair, update and maintain workstations and laptops.
- Install, maintain, and troubleshoot printers/copiers as well as manage toner requests.
- Setup and support audio/visual equipment for presentations and trainings on and off site.
- Install and configure peripherals including scanners, external drives, monitors and other peripheral hardware.
- Removal/disposal of non-functional equipment.
- On a regularly schedule clean equipment from dust and particles.

Software

- Provide software and system troubleshooting and support.
- Install, maintain, troubleshoot, and update operating systems and user applications.
- Proactively schedule software upgrades and patching.

- Assure that all software on NRC equipment is licensed and keep record of licenses.
- Track license and support contracts to include notification of renewal timeframe to management.

Network

- Monitor network to ensure network functionality and availability to all system users.
- Install, maintain, troubleshoot, and repair cabled, wireless and other network infrastructure.

Security

- Maintain local and server based anti-virus software.
- Inform and train users and management in how to adhere to NRC global and local security ICT policies.
- In case of virus infection clean out affected equipment.

Users

- Ensure computer is set up prior to new hire start date and any related moves.
- Handle the relocation of computer equipment as a result of offices or personnel changes.
- Request and setup new user accounts and email accounts.
- Troubleshoot, and repair user accounts and email accounts, assist in resetting passwords.

Systems Planning

- Participation in research and recommendation of improved infrastructure processes and technologies to include growth planning.
- Provide procurement assistance including, but not limited to, researching solutions, engaging with potential vendors, making recommendations for product purchases and evaluating bids.
- Test new equipment and applications and provide thorough feedback.

Management of Vendor Services

- Work directly with vendors to schedule repairs and maintenance.
- Request and evaluate services with vendors and service providers.
- Work with ISP and other outside vendors to ensure dependable operations.
- Work with vendors to and vendor supplied systems to track service requests through to completion.

Training

- Train new and current employees on computer software and ICT systems.
- Create materiel and presentations for trainings and reports.
- Assess user capacity and suggest trainings and areas in need of improvement.

Routine Administrative Tasks

- Create and maintain inventory, which may include hardware, software and various items such as laser printer cartridges and peripheral equipment.
- Maintaining documentation of processes, procedures, and troubleshooting guides.
- Monitor and report ICT expenses.

- Assist with preparation of operating budgets based on estimated and actual expenditures for ICT systems and support needs.
- Keep ICT equipment, storage area and work area clean and organized.

Supported technologies include but are not limited to: wired and wireless networks, storage systems, Microsoft Active Directory, Windows OS, MS Office suites, Citrix, end user workstations, laptops and various proprietary and commercial software applications and hardware.

Must be able to work independently to troubleshoot, perform root cause analysis, identify and isolate technical issues.

Must be willing to take ownership of the issue analysis and resolution efforts and commit to 'doing what it takes' to resolve technical issues regardless of the effort or timeframe required.

The person in this position will also be responsible for managing and completing various IT projects. This includes the assessment of applications and technology, formulating and presenting solution options to various levels of management, influencing and advising the selection process, and overseeing implementation of NRC ICT systems and key project deliverables.

Must have strong communication skills, written and oral, be able to communicate effectively, produce reports, and present solutions.

May be required to work extended and /or non-core business hours, as and when required by the needs of the organization. This may include evening, weekends and holidays.

4. ADDITIONAL INFORMATION

DUTY STATION AND LIVING CONDITIONS

Signed

(Employer)

(Employee)

By signing this job description, the employee accepts them as well as the NRC Guiding Principles on Sexual Harassment and the General Code of Conduct for all NRC's field personnel attached to this document.

2. Laptop Acceptance Form

I understand that all laptop computers, equipment, and/or accessories provided to me are the property of the NRC.

I agree to all of the terms in the NRC ICT Policy, the NRC's ICT Policy, and I will return the equipment to the ICT department in the same condition in which it was provided to me.

I understand that I am personally responsible for any damage to or loss of any laptop computer and/or related equipment and accessories. In case of damage or loss I will replace or pay the full cost of replacement of the damaged or lost equipment with equipment of equal value and functionality subject to the approval of the management.

I will not install any additional software or change the configuration of the equipment in any way without prior consultation with the ICT department.

I will not allow any other individuals to use any laptop computer and/or related equipment and accessories that have been provided to me by the NRC.

I understand that a violation of the terms and conditions set out in the NRC ICT policy will result in the restriction and/or termination of my use of the NRC's laptop computers, equipment, and/or accessories and may result in further discipline up to and including termination of employment and/or other legal action.

Name _____

Signature _____ Date _____

Phone _____ Model _____ NRC ID # _____

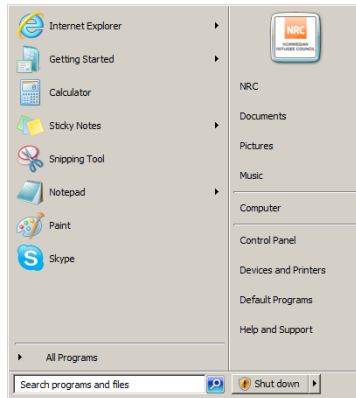
Items Loaned / Condition – If used or damaged please make additional comments

Item	Loaned				Condition			
Computer	Yes	<input type="checkbox"/>	No	<input type="checkbox"/>	New	<input type="checkbox"/>	Used	<input type="checkbox"/>
Power Supply & Cord	Yes	<input type="checkbox"/>	No	<input type="checkbox"/>	New	<input type="checkbox"/>	Used	<input type="checkbox"/>
Laptop Bag	Yes	<input type="checkbox"/>	No	<input type="checkbox"/>	New	<input type="checkbox"/>	Used	<input type="checkbox"/>
Mouse	Yes	<input type="checkbox"/>	No	<input type="checkbox"/>	New	<input type="checkbox"/>	Used	<input type="checkbox"/>
Keyboard	Yes	<input type="checkbox"/>	No	<input type="checkbox"/>	New	<input type="checkbox"/>	Used	<input type="checkbox"/>

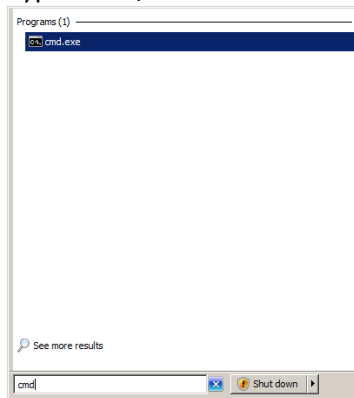
Comments: (overall condition, scratched, dented, bent, missing keys, missing parts):

3. Trace Route guide

1. Click the start button



2. Type 'cmd', and click the icon that appears at the top of the list



3. At the command prompt type 'ipconfig /all' and hit enter, the needed information will appear as shown

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\User>ipconfig /all

Windows IP Configuration

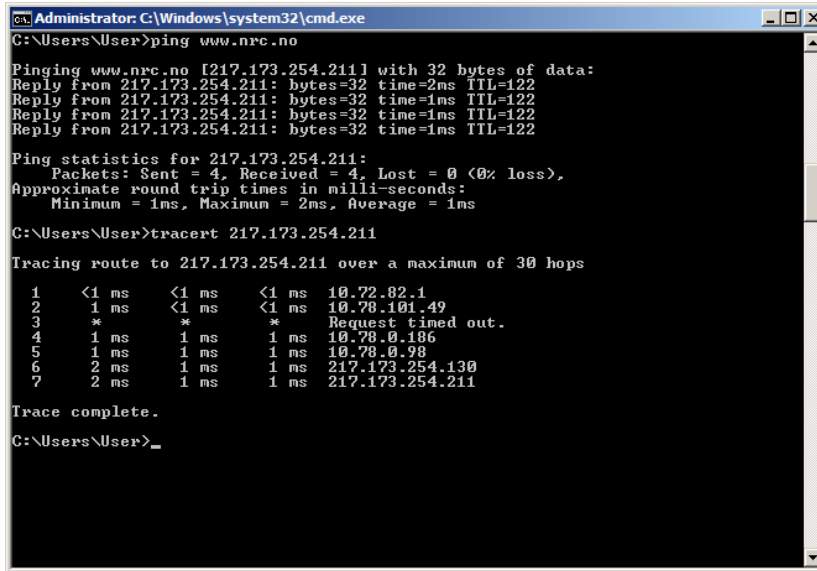
    Host Name . . . . . : 103220eljo
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : kunder.tconet.net

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : kunder.tconet.net
    Description . . . . . : Intel(R) 82567LM-3 Gigabit Network Connection
    Physical Address. . . . . : 18-A9-05-20-21-D8
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::f4eb:4232:894f:38f6%12(Preferred)
    IPv4 Address. . . . . : 10.72.82.213(Preferred)
    Subnet Mask . . . . . : 255.255.254.0
    Lease Obtained. . . . . : 15. september 2011 08:39:06
    Lease Expires . . . . . : 16. september 2011 00:39:06
    Default Gateway . . . . . : 10.72.82.1
    DHCP Server . . . . . : 10.72.82.1
    DHCPv6 IAID . . . . . : 270051589
    DHCPv6 Client DUID. . . . . : 00-01-00-01-12-F2-6A-3A-18-A9-05-20-90-4D

    DNS Servers . . . . . : 217.173.247.196
                          217.173.247.197
    NetBIOS over Tcpip. . . . . : Enabled
```

- Next step is to ping and run a trace route to a known IP address
At the command prompt type 'ping www.nrc.no', followed by 'tracert 217.173.254.211'



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\User>ping www.nrc.no

Pinging www.nrc.no [217.173.254.211] with 32 bytes of data:
Reply from 217.173.254.211: bytes=32 time=2ms TTL=122
Reply from 217.173.254.211: bytes=32 time=1ms TTL=122
Reply from 217.173.254.211: bytes=32 time=1ms TTL=122
Reply from 217.173.254.211: bytes=32 time=1ms TTL=122

Ping statistics for 217.173.254.211:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\User>tracert 217.173.254.211

Tracing route to 217.173.254.211 over a maximum of 30 hops:

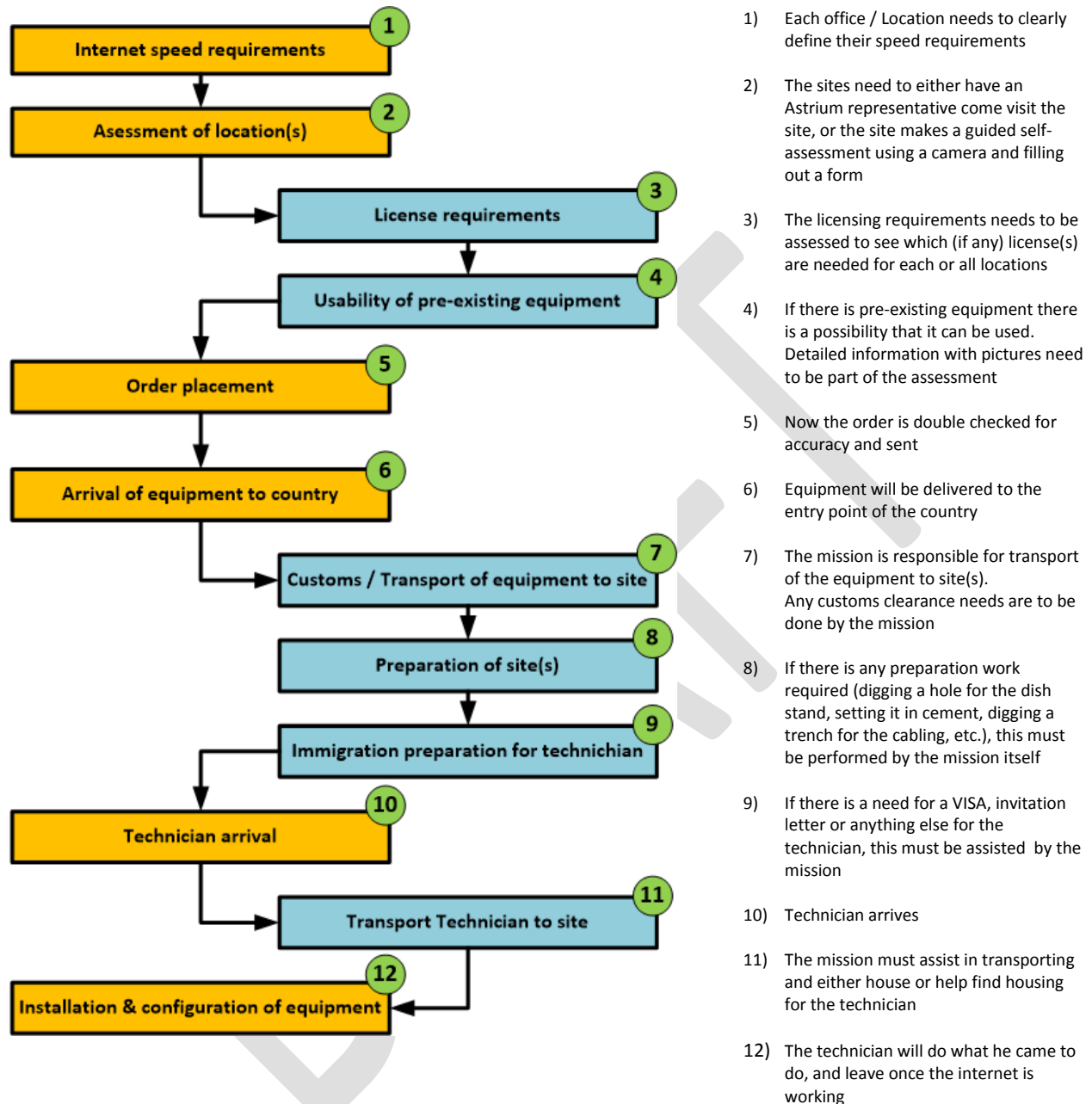
  0  <1 ms    <1 ms    <1 ms    10.72.82.1
  1  <1 ms    <1 ms    <1 ms    10.78.101.49
  2  *          *          *          Request timed out.
  3  1 ms     1 ms     1 ms     10.78.0.186
  4  1 ms     1 ms     1 ms     10.78.0.98
  5  2 ms     1 ms     1 ms     217.173.254.130
  6  2 ms     1 ms     1 ms     217.173.254.211

Trace complete.

C:\Users\User>
```

- You have now got all the information that you need to relay to the technician

4. Astrium procurement process



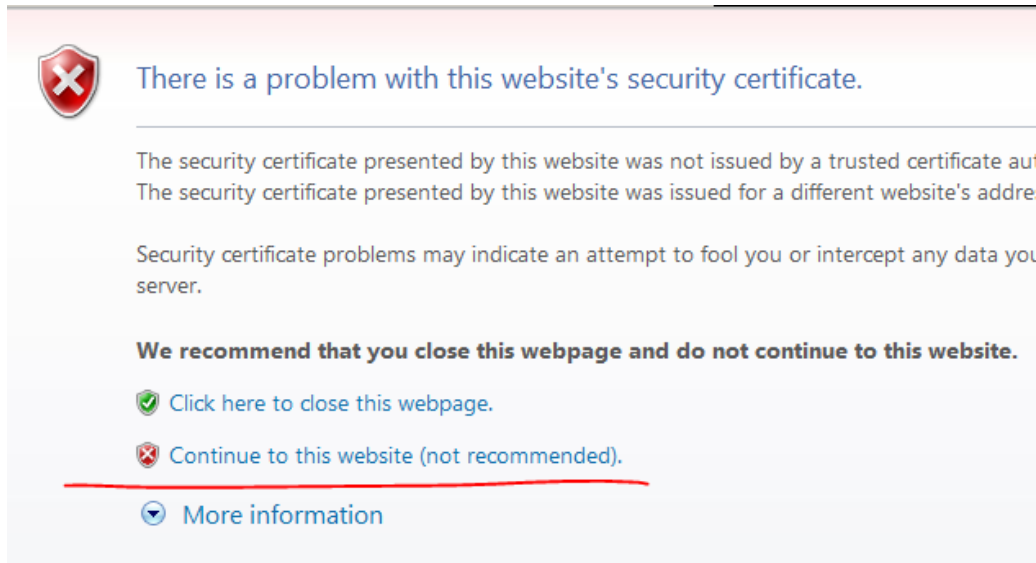
Step	Costs	Work required from the mission
1 Internet Speed Requirements Before any decisions or planning happens, the mission needs to define what internet speed they require at each site. Once this has been done Astrium will have all the information that they need to move on with designing the order, inquiring about licensing, etc.	None	A clearly defined list of internet speeds

2	<p>Location Assessment</p> <p>Each of the locations needs to have an assessment made. Either Astrium or one of their working partners can do this.</p> <p>The goal of the assessment is to assess where the best location for placing the 2.3 Meter dish is, assure that there is a free line of site, and that it is the best place as far as weather and other factors goes.</p> <p>Self-assessment</p> <p>In some cases the assessment can be done by staff at the location(s). A guide will be sent together with a questionnaire. Using a digital camera; pictures must be taken according to the guide, and the questionnaire filled out. The result will be sent to Astrium and either approved or sent back with further questions or instructions.</p>	<p>Potentially transport to site</p> <p>Potentially house the Assessor</p> <p>Anything else that might be required if the location has difficult circumstances (access to food, water, etc.)</p>	<p>If the locations are in difficult to reach areas, if there are no available hotels, or other circumstances that makes the job difficult there needs to be assistance from the mission to aid in getting the assessor to the location and if required aid with lodging.</p> <p>If the assessor needs to come from another country, the mission will have to assist in getting a VISA, written invitation, or whatever else might be required.</p>
3	<p>License(s)</p> <p>Since Astrium is not locally represented in some of the countries there might be a need to get a license from the local government to be able to have a VSAT connection. Once the internet speed requirements, and number of sites required has been established Astrium will find out what the potential cost and needs for license(s) are.</p> <p>Any License cost will be paid by the mission</p>	<p>Any cost related to licensing is the responsibility of the mission to pay.</p>	<p>Astrum will aid in finding out the needs for each individual country. If there is a licensing need, there will be administration work for the mission to obtain said license.</p>
4	<p>Pre-existing equipment</p> <p>If there is pre-existing equipment there is a chance that it can be used.</p> <p>There are two parts to the setup:</p> <ol style="list-style-type: none"> 1) The actual dish 2) The electronic parts (BUT head, modem, cable, anchors, etc.). <p>In some cases all equipment can be used, in some cases none of the equipment. This will be part of the site assessment</p>	<p>None</p>	<p>None</p>
5	<p>Order placement</p> <p>Once all requirements has defined, the site(s) has been assessed, the licensing has been solved, the mission is now ready to place the order</p>	<p>None</p>	<p>Make a final approval of the order, and fill our required paperwork.</p>
6	<p>Equipment Arrival</p>	<p>None / Included in price</p>	<p>None</p>

	The equipment will be sent to the entry point of the country. The electronics will be sent from Norway, the hardware will be sent from Germany.		
7	Customs and Transport The mission will have to get the equipment out of customs, and transport the equipment to the site(s).	Cost of customs clearance. Cost of transport of equipment to site.	The mission will have to get the equipment out of customs, and transport the equipment to the site(s).
8	Preparation of site If there is any requirements of preparation work for the new equipment it will have to be done by the mission. If there is no previous equipment there will need to be a hole dug and cement poured for the place where the dish will be located. Astrium will guide and assist in this matter.	Cost of labor and material.	Mission will with guidance from Astrium either perform the required work themselves or outsource it to a qualified company.
9	Immigration prep work If there is a need for VISA, introductory letter, etc. the mission will have to assist in preparing this for the arrival of the technician.	Depends on need of border entry, or movement inside of the country.	Admin for immigration.
10	Technician arrival If technician comes from another country, and not form a local partner, the mission might need to aid in airport pickup. This depends on the country	Potential cost of transport	Potential pickup at airport
11	Transport to site(s) Technician needs to go to site. If there is a lot of distance, or if the transport is difficult the mission will need to assist.	Potential transport costs	If the technician cannot get to site by normal means the mission will need to assist.
12	Installation and setup. The work required depends on circumstances, but is estimated to be between 3 – 5 days, this of course is an estimated number and might vary depending on local situation.	Potential room and board if the site is located in a difficult area.	Mission might need to assist with room and board if the site is located in a difficult area.

5. How to change WAN IP address

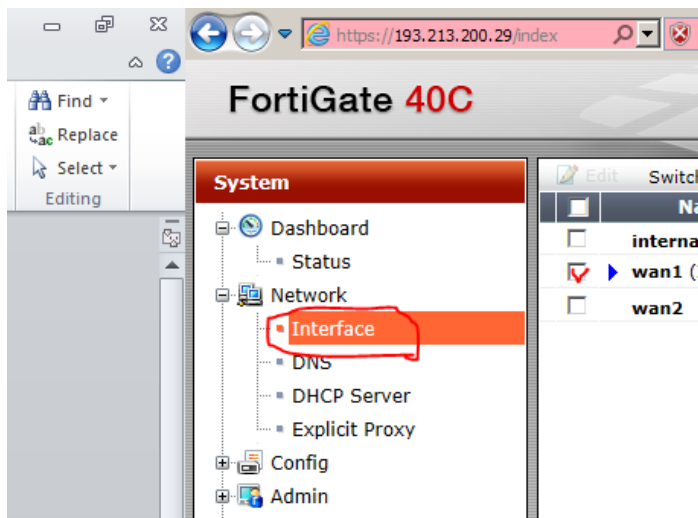
1. In your browser window, go to the address <https://10.100.x.1> (where x is the subnet of your office, if you are unsure, ask HO ICT)
2. When you get prompted about the security certificate; click “continue to this website”



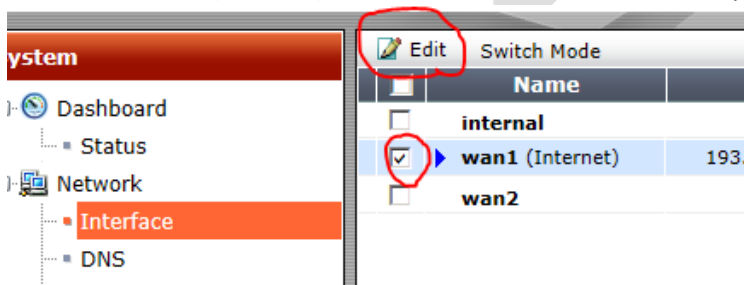
3. Fill in the username & password (if you don't know it, contact HO ICT), and click 'login'

A screenshot of a login interface. At the top, it says "Please login...". Below this are two input fields. The first is labeled "Name" and contains the text "network". The second is labeled "Password" and contains seven dots. To the right of the password field is a red button with the word "Login" in white text.

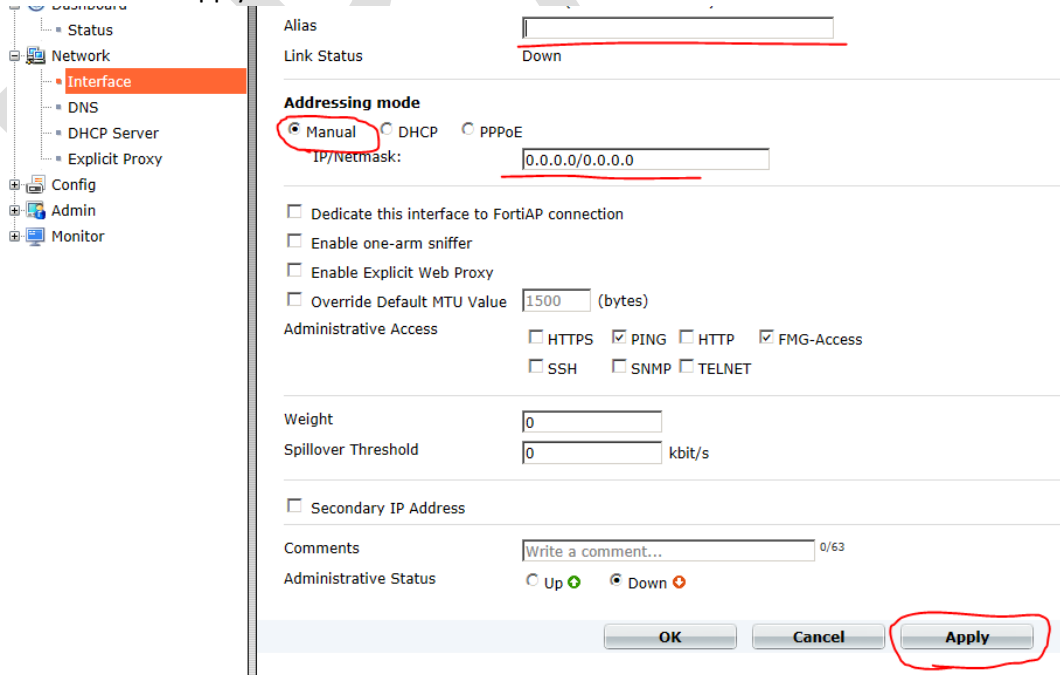
4. Click the 'interface' link in the left menu



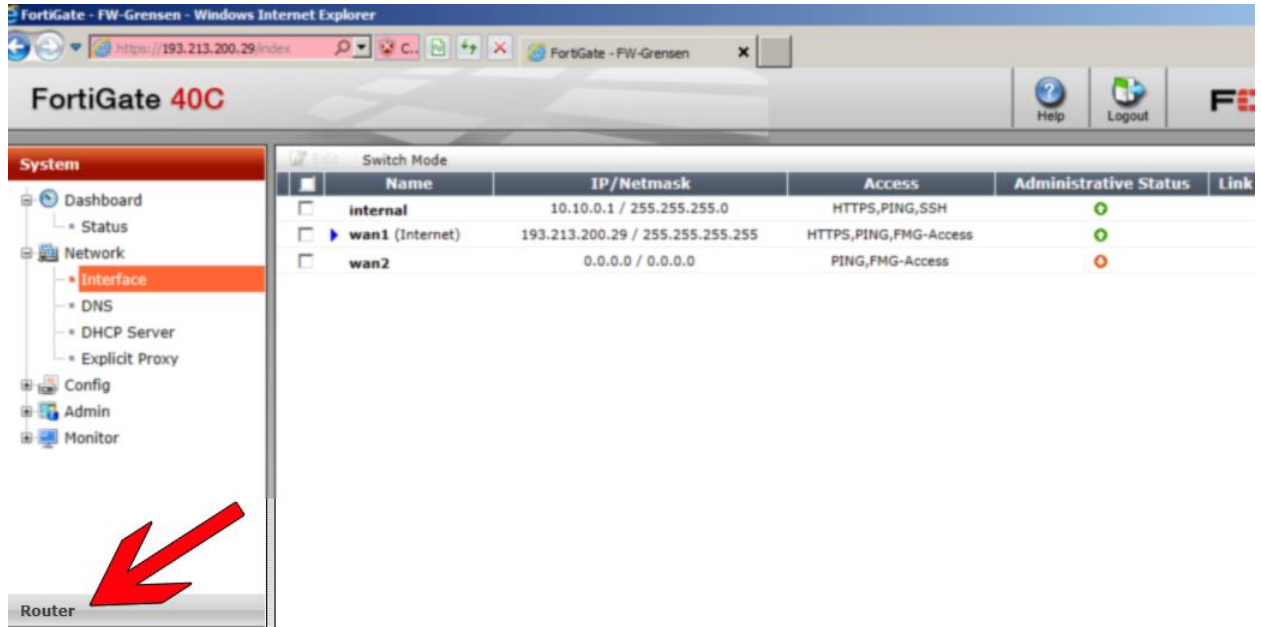
5. Check the 'wan1 (internet)' box, and click the 'Edit' link on top



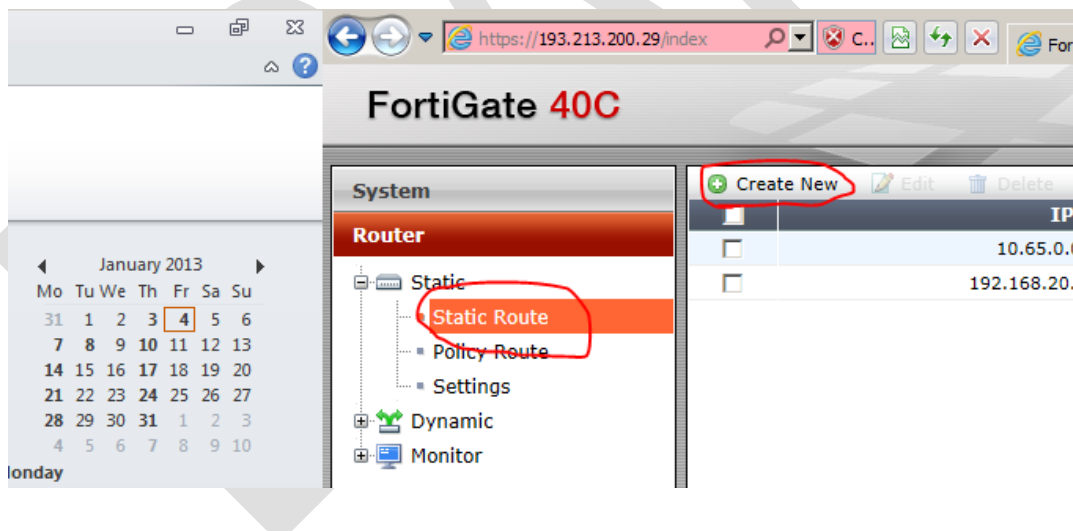
6. Click the 'manual' option, and put in the IP address and subnet mask (provided by your ISP) and then click the 'Apply' button



7. Find the 'Router' icon at the bottom of the webpage



8. In the 'Router' menu, click the 'Static Route', and then click the 'Create new' button.



9. Change the 'Gateway' to your ISP's gateway address, leave "destination IP / Mask" as is, click 'OK'.

FortiGate 40C

System

- Router
 - Static
 - Static Route**
 - Policy Route
 - Settings
 - Dynamic
 - Monitor

New Static Route

Destination IP/Mask: 0.0.0.0/0.0.0.0

Device: wan1 (Internet)

Gateway: 0.0.0.0

Comments: Write a comment... 0/63

Advanced...

OK

10. Pictured below is how it should look if everything is as it should be.

FortiGate 40C

System

- Dashboard
- Status
- Network
 - Interface**
 - Static

Switch Mode

	Name	IP/Netmask	Access	Administrative Status	Link Status	Type	Re
<input type="checkbox"/>	internal	10.10.0.1 / 255.255.255.0	HTTPS,PING,SSH	⬆	⬆	Physical	15
<input checked="" type="checkbox"/>	wan1 (Internet)	193.213.200.29 / 255.255.255.255	HTTPS,PING,FMG-Access	⬆	⬆	Physical	25
<input type="checkbox"/>	wan2	0.0.0.0 / 0.0.0.0	PING,FMG-Access	⬆	⬆	Physical	0

6. Networking Components

6.1. Fortinet Firewall



The Fortinet Firewall Wan connects to the ISP equipment and performs general firewall functions between the WAN side and the LAN side of the network. It enables the VPN tunnel between the Field office Firewall WAN side and the Main Firewall in Oslo, and it is responsible for delivering DHCP addresses to the LAN side.

6.2. Trapeze WLC2



The Trapeze WLC2 is a Wireless controller that runs the configuration for the Wireless Access Points. This device controls all of the Access Points, it is where the wireless settings are stored and configured, and acts as the 'brain' behind your wireless network.

6.3. Steelhead Riverbed



The Steelhead Riverbed is a WAN optimizer that optimizes the data traffic between the field office and the HQ.

6.4. D-Link PoE Switch



This is a standard network switch, with the exception that the first four ports (Marked with a yellow stripe above them) also supplies power to the access points using Power over Ethernet (PoE).

6.5. Wireless Access points



These are 'Dumb Access Points' that cannot operate independently from the Trapeze WLC2 controller unit, and needs power to be provided from PoE.

7. Cabling Guide



Cabling Guidelines:

- 1 pcs. RED cable from your ISP router to Fortinet Firewall WAN 1 Interface.
- 1 pcs. ORANGE cable from Fortinet Firewall LAN1(or INT1) interface to Riverbed WANO_0 interface.
- 1 pcs. GREEN cable from Riverbed LANO_0 interface to D-link port 5.
- 1 pcs. BLUE cable from Riverbed Primary Interface to D-link port 6.
- 1 pcs. BLACK from Trapeze Wireless Link 1 Uplink to D-link port 7
- X pcs. WHITE from D-link PoE interface 1-4 to Wireless Access Point

8. What are viruses?

Computer viruses are self-executing, replicating programs written specifically to change the way a machine works, without the knowledge (or permission) of the user. Viruses are so called because they behave in a similar way to biological viruses. Just as biological viruses pass from person to person, replicating themselves as they go, computer viruses pass from computer to computer.

Viruses can impair and seriously damage your computer by, amongst other things; executing random text, audio and video messages, draining memory, deleting files, corrupting programs - even reformatting (or erasing the contents of) your hard disk. At best, the less destructive viruses are annoying and will slow the infected machine up, often resulting in crashes and other unpredictable behavior which can ultimately result in loss of data.

Although a virus needs an infected application to be launched in order to infect other programs or documents, they can hide themselves in your computer (often as innocent files) and replicate (make copies of) themselves until the infected application is launched.

Not all viruses behave in exactly the same way, and not all malicious programs are viruses (like Trojans). Some viruses are only active when the infected application is running, whilst others will stay active in memory until you turn off your computer. However, as the virus is resident in a file or on a disk, exiting the infected application or turning off your computer only removes the virus from memory, it does not remove the virus from the infected file or disk and the virus just lays dormant, until you to reboot your computer and/or access the infected application.

8.2. The various forms of computer viruses:

- **Boot sector viruses** infect the boot sector of a hard drive or floppy disk by first overwriting/moving the original boot code and then moving the original code to another sector on the disk, which the virus marks as bad.
- **File infecting viruses** attach/modify any executable files, sometimes replacing the original code with its own.
- **Macro viruses** are self-replicating macros that self-replicate and can spread rapidly on a computer and/or network.
- **Master Boot Record Infectors** infect a system's Master Boot Record on hard drives and the Boot Sector on floppy diskettes.
- **Multi-partite viruses** are commonly a combination of techniques of both boot sector viruses and file infecting viruses.
- **Polymorphic viruses** are difficult to detect as they use an encryption algorithm that changes, along with the viruses' appearance, change their appearance with/after each infection.
- **Stealth viruses** hide themselves from a computers' operating system and anti-virus products.
- **Viruses** (including worms) are often distributed via attachments in e-mail spam and, ironically, a great deal of e-mail spam (particularly chain letters) are virus hoaxes.

8.3. Worms and Trojans

Worms are computer programs that can copy themselves from machine to machine, extremely quickly, through computer networks.

Worms differ from computer viruses because they run independently and do not need a host file, boot sector or file transfer between machines to propagate.

- **Worms** are different types of computer worms that spread through various services - including e-mail and instant messaging clients.
- **E-mail worms** spread via infected e-mail messages in the form of an attachment or link to an infected Web site - some e-mail worms will also spoof e-mail addresses.
- **IM worms** spread via instant messaging clients, to entire contact lists, in the form of links to infected Web sites.
- **Internet worms** spread when the Internet worm scans, tries to connect and, if successful gains access to any vulnerable machines - by scanning the Internet and/or using the local operating system.
- **IRC worms** spread via IRC channels in the form of infected files or links to infected Web sites.
- **File-sharing Networks Worms** spread from shared folders via the P2P network.

9. General Threats

There are many kind of threats that we have to combat today, and traditionally one thinks of threats being defined as:

- Viruses, Worms, Trojans
- Malware, Adware, Phishing, Spam
- Hacking, snooping, cracking

Through only looking at threats from this perspective, the most common security fallacies are:

- I have Antivirus protection so I am safe!
- We are behind a firewall, so we are safe!
- All threats come from the outside!
- I have a backup, therefore what is the worst that could happen?

As much as these are the commonly perceived threats, security is primarily a management issue, not a technical issue. As much as you can protect yourselves with software and hardware, a major part of managing security risks comes through educating your users and setting up a system following NRC policies and using best practices that helps manage the flow, storage and access of information as well as being in control of the ICT equipment.

It is the ICT department's job to see to that not only all computers are protected and meet the minimum requirements of the NRC's standard setup, but also shaping the way that the users works with ICT equipment to prevent data from loss, corruption and theft.

Above loss of data through viruses and malware, you also have to assure that:

- Information remains confidential and only those who should access that information can
- No one has been able to change the information, so you can depend on its accuracy (information integrity)
- Making sure that your information is available when you need it, by managing and storing data correctly.

A big part of NRC ICT security is managing where the data physically is located, how it is being stored long term, and that it remains on NRC premises. It is also important that people simply don't walk off with data on personal computers or storage mediums, or use unsecure methods of communication spreading it outside of NRC control. The easiest way to express this is that:

"NRC data should be worked on using NRC equipment, in NRC offices, using NRC owned and licensed software, and communicating only using NRC communication systems."

This assures that the data is always in NRC control, is always being worked on using equipment that legally meets NRC licensing agreements as well as assuring that all tools necessary are available and up to standard according to NRC needs.

To do this we have the help of policies. Policies has been created globally to help guide you in setting standards, but are also there to have something to refer to if anyone disagrees to what the actual rules and regulations are as far as ICT management and how people are supposed to work.

According to NRC ICT policy, it is strongly discouraged or even prohibited to:

- Use personal computers for NRC work in the office.
- Take laptops home or even outside of the premises of NRC unless it is part of their work description and has been authorized by their manager.
- Use personal email addresses for official communication.

- Use personal removable media (hard drives, USB memory sticks, SD cards, etc.).
- Use backup media that is not encrypted.
- Use cloud storage solutions such as DropBox, SkyDrive, iCloud, etc.

DRAFT

10. Support flowchart

ICT Officer

Level 1 Support

Installation of new computers, re-deployment of equipment, software problems, Internet connectivity issues, setting up accounts, minor technical issues, broken equipment, networking issues, creation of local computer accounts, printer issues, etc.

First level of support
Everyday local issues that can be dealt with by ICT Officer, online resources, guidelines, policies.

Escalation

Head Office ICT Department

Level 2 Support

Creation of AD accounts, Networking equipment issues, Policies, Strategic questions, Email account issues, Agresso issues, SharePoint issues, VSAT, Security issues, Etc.

Second level support
Complex issues that needs assistance, guidance, or issues that are managed from HO.

Escalation

Service Providers

Level 3 Support

Service providers, Tele Computing, Portal issues, Launcher issues, ISP, Hardware manufacturers, Software companies, Etc.

Third level support
Issues that are specific to products or services that can not be solved with NRC competence or resources.

11. Firmware

Firmware refers to the applications and/or operating system that control how a device operates. It is called firmware rather than software to highlight that it is very closely tied to the particular hardware components of a device. Firmware is generally flashed into a device's ROM rather than simply being loaded into normal storage, where it could more easily be erased and lost in the event of a crash. Firmware updates are sometimes provided by a company as a way to fix bugs or introduce new functionality.

12.1.1 Why does firmware need to be updated?

Most of the equipment we use today is as much a computer as it is a device (router, switch, printer, scanner, etc.). As such, sometimes the manufacturer makes improvements to those programs that run the device (firmware). These improvements are released as firmware updates. Firmware updates generally are for correcting 'bugs' in the code that is used as the machines operating system. Sometimes the updates are to correct a functional problem and sometimes they are enhancements to existing functions that are working fine.

12.1.2 Should I always update my firmware?

Generally **if the machines are working fine then you leave them alone**, but if there is something critical like a security or compatibility flaw it is wise to update.

Before applying an update, especially in the case of firmware, you need to make sure that the update is for your exact model of device. Applying an update intended for a similar-but-different model could result in your gear becoming non-operational. The old firmware gets overwritten (replaced) by new operating instructions that aren't compatible with your model, which means your device won't work anymore. That's referred to as "bricking" your gear.

12.1.2.1 How do I find out about updates?

There are two things you can do to stay abreast of firmware updates:

- The best way to make sure you are alerted to important updates for your device is to register your purchase with the manufacturer. Fill out the registration card that comes with it or register it online at the manufacturer's website. That way, the manufacturer knows you own one of their devices and can alert you if an important update comes along.
- The other way to keep on top of updates is to occasionally visit the manufacturer's website and look up your equipment model or a list of released firmware updates. This might be the only way to learn about updates for minor issues.

12.1.2.2 Best practices regarding firmware

- Only install firmware downloaded directly from an official website or FTP site
- Only install firmware clearly labeled for the specific country/region where you purchased the product
- Firmware downloaded from an official site that is different from the country/region where the product was purchased may render the product as inoperable and void the warranty
- Firmware labeled as beta may not be as stable as the prior official release version, never use beta firmware unless absolutely necessary
- Do not upgrade firmware via a wireless connection as a network disruption can render the equipment unusable.