

**NC3 Services**

**Main components of a charter**

**Information Security**

**Informations générales**

Version: 4

Document state: Draft

Document: Main components of a charter- Information Security

Date: 07/02/2013

SMILE Representative:

Table of Contents

[1 Purpose of the charter 3](#_Toc26456917)

[2 Commitment of the management 3](#_Toc26456918)

[3 Scope and sanctions 4](#_Toc26456919)

[4 Use of information systems 4](#_Toc26456920)

[5 Password Management 4](#_Toc26456921)

[5.1 Responsibility of employees 4](#_Toc26456922)

[5.2 Creating passwords 5](#_Toc26456923)

[5.3 Durability of passwords 5](#_Toc26456924)

[5.4 Saving passwords 5](#_Toc26456925)

[6 Use of electronic equipment 6](#_Toc26456926)

[6.1 BYOD 6](#_Toc26456927)

[6.1.1 Responsibilities 6](#_Toc26456928)

[6.1.2 Duties 6](#_Toc26456929)

[6.2 Use of desktops 6](#_Toc26456930)

[6.3 Using a Laptop or Smartphone 7](#_Toc26456931)

[6.3.1 Common rules of a Laptop or Smartphone 7](#_Toc26456932)

[6.3.2 Rules specific to Laptops 7](#_Toc26456933)

[6.3.3 Smartphone specific rules 7](#_Toc26456934)

[6.4 Software Installation 8](#_Toc26456935)

[6.5 Using the remote access of the company 8](#_Toc26456936)

[7 Use of Internet Services (Web) 8](#_Toc26456937)

[8 Email Management 9](#_Toc26456938)

[8.1 Creating an account 9](#_Toc26456939)

[8.2 Using e-mail 9](#_Toc26456940)

[8.3 Prerogatives to sending an email 10](#_Toc26456941)

[8.4 Saving emails 10](#_Toc26456942)

[8.5 Erasing large unprofessional emails 10](#_Toc26456943)

[8.6 Defended use of emails 10](#_Toc26456944)

[8.7 Use of the electronic signature 11](#_Toc26456945)

[8.8 Using encryption 11](#_Toc26456946)

[8.9 Security and Security Events 11](#_Toc26456947)

[8.10 Template and signature 11](#_Toc26456948)

[9 Management of keys and badges 11](#_Toc26456949)

[10 Clean Office / Clean Desk 11](#_Toc26456950)

[11 Disposal 12](#_Toc26456951)

Information about this document

This document is an aid to the creation of an Information Security Policy / Charter. It outlines the best practices and guidelines to be followed by employees of an organization. The information contained in this document is not exhaustive and should always be personalized to the recipient organization, knowing that a good practice can be accepted, adapted or even rejected according to the context.

Here are two important good practices:

* write what you want to do, then do "EVERYTHING" what you have written;
* It is better to write less and apply the whole, than to be exhaustive and to apply only part of it.

# Purpose of the charter

This charter is a code of good practice that allows the information system to be used in the best conditions of safety, in a trusting and responsible manner and with respect for others.

It also outlines the rights and obligations that arise from the reciprocal engagement between the employee and the company.

# Commitment of the management

Our company implements this Policy / Charter, in order to define the information security rules to be respected by all people working for it.

We commit ourselves to support all actions that fall within the framework of information security and to provide the means necessary for their implementation.

Everyone working in our organisation must follow this approach:

* taking cognizance of and applying the present measures in its respective field of activity;
* by informing the different parties, such as colleagues and external contacts, of the rules applicable to them.

Not respecting the information security measures will be punished...

<la\_direction>

# Scope and sanctions

This charter applies to all employees of the company, regardless of status, and more generally to all persons, permanent or temporary, using the company's IT resources.

It will also be communicated and signed by the persons falling within the scope mentioned above.

Intentional or repeated non-compliance with the rules of this charter, gross violations of the Penal Code, privacy laws, and non-compliance with intellectual property rights may lead to disciplinary sanctions which will take into account the risks incurred and the damages suffered.

In the case of serious violations of laws and legislation, the management may be brought to the courts.

# Use of information systems

The means available to employees of the company are intended for professional use. Nevertheless, the company recognizes a right of private use, when it is justified by an acceptable interest, if the use remains within reasonable limits and if the employee behaves responsibly. The use of professional resources in a private capacity must follow the principle of “due diligence” and must respect the following rules:

* it is forbidden to use the resources of the company for purposes that could harm the integrity of natural or legal persons or for the image of the organisation;
* the legislation in force is known to all and applied;
* the use of resources in a private capacity must not cause any disturbance or dysfunction of the work of other users;
* employees may not, without prior authorization, exceed the rights and authorizations attributed to them, that is to say, modify, reproduce, destroy or read information that is not intended for them;
* collaborate with people in the IT department to help identify and correct problems or anomalies that may arise;
* the equipment made available to the personnel will be used, handled or stored with the necessary care to avoid any deterioration;
* it is forbidden to connect removable media from or having been connected to external sources, to any company device, without having performed the usage control implemented by the IT department;
* employees may not, without prior authorization, remove material or information from the company compound.

# Password Management

## Responsibility of employees

The employee is personally responsible for the proper protection of his password. The password is secret, and is personal information that should never be transmitted.

## Creating passwords

Passwords used within the company are strictly personal and must comply with the following minimum rules:

* have a minimum length of 10 characters;
* be composed of uppercase, lowercase letters and numbers.

A derogation exists however, for the systems not accepting these constraints (PIN code of a Smartphone, for example).

It is strictly forbidden:

* to keep beyond the first use, the passwords attributed by default by the system manager concerned;
* use easy-to-guess passwords (user name, pet name, date of birth, phone number, etc.);
* use words from a dictionary (also foreign), names of cities, countries or even months;
* use the password assigned by the IT department;
* use a password based on the user's ID;
* use the same password for multiple systems;
* give a password to a colleague, a supervisor or the IT department;
* write the password down without protecting it in the proper way;
* send or disclose a password by email, phone, Internet, etc.

It is advisable to create the password as follows:

* choose a phrase from a poem, film or other well-known source;
* then take the first or the second letter;
* change, for example, the letters "S" to the number "5", "l" to "1" or "o" to "0".

Example: *« It is difficult to change a well-anchored opinion! »* gives : *« 1idtcawAo! »*

To avoid using the same password for each system, you can change it by playing multiple letters or inserting non-alphanumeric signs:

"2idtcawBo!", "3idtcawAo?", "3idtc,awAo?"

## Durability of passwords

Passwords must be changed on a regular basis:

* All administrator password must be changed every 6 months to a minimum;
* All other passwords must be changed at least every year;
* At the slightest hint of compromise, the password of the affected system must be changed immediately.

## Saving passwords

Passwords:

* of the "administrator" type, or
* by their nature to be used by more than one person, or
* giving access to encrypted documents,

are saved in a list provided for this purpose and under the responsibility of the IT manager.

This list must only exist in paper form, enclosed in a sealed envelope and be deposited in a fireproof cabinet. The persons entitled to access and use this list are designated by the IT manager.

"Normal" passwords can also be saved by programs designed for this purpose (KeePass, for example).

# Use of electronic equipment

## BYOD

BYOD access is granted to employees with a motivated business need to access the company's services using private or personal equipment.

Access to the Company's services may be limited or blocked in the event that anomalies are identified.

It is the responsibility of the employee to ensure that his device is compatible with the technical constraints of the proposed mobile access. Neither the employer nor the service provider can be forced to support the device.

### Responsibilities

* The employee is solely responsible for the mobile access made available by the employer and his personal equipment. The employer can not be held responsible for any personal damage caused (hardware, software, data loss).

### Duties

Employees who have BYOD access commit:

* not to modify the operating system of their device (e.g. no jailbreak, etc.)
* not to change, share or replace the specific configuration of the device;
* do not communicate access to a third person:
* delete all data on the device when closing the BYOD access.

## Use of desktops

Employees who have at their disposal a desktop computer commit themselves to:

* protect access to the computer with a password that meets the requirements described above;
* block access to the computer before leaving the workstation, even for a very short period of time;
* take all appropriate measures to ensure the security of information stored on the computer;
* Do not leave the computer to third parties except IT personnel for maintenance purposes;
* do not install software without authorization from the supervisor, except authorized ones;
* manage the computer using common sense;
* protect all information stored on a local disk. When a network disk exists, the data stored directly on the machine is the responsibility of the user. In particular, he guarantees the confidentiality, integrity and availability of information stored locally;
* Label explicitly with the mention "private", the private data stored locally.

## Using a Laptop or Smartphone

### Common rules of a Laptop or Smartphone

All instructions valid for desktop computers are to be respected for Laptops and Smartphones. In addition, the nomadic nature of these requires special attention from the employee who is responsible for it.

In the case of a permanent or temporary allocation of a device, the employees concerned is expected to:

* follow the same instructions as desktop computers (previous chapter);
* take all appropriate measures to ensure the physical security of portable devices made available, including the prevention of theft or physical damage;
* do not connect to computer networks whose level of trust is unknown;
* perform backups when storing data on his mobile device;
* ensure that no one can see any confidential information when the device is used in a public place;
* do not use private WiFi in the company;
* disable the means of wireless communication (Wifi or Bluetooth), including automatic device search, when not in use;
* use the Bluetooth security mode that encrypts traffic in both directions.

### Rules specific to Laptops

In addition to the rules mentioned above, employees who use Laptops commit to:

* use an anti-theft cable if it is essential to leave the Laptop unattended in public places;
* take the laptop as hand luggage when traveling;
* use a specific user account with restricted rights, to access the Internet via his Laptop in public places such as hotels, railway stations, terminals, etc. ;
* Do not hinder the operation of the antivirus and firewall, and check that they are activated and regularly updated.

Laptops are given to persons who, by their attributions, are invited to travel or to participate in fairs or seminars in Luxembourg and abroad.

### Smartphone specific rules

In addition to the rules mentioned above, employees who use smartphones commit to:

* be aware of the main risks associated with Smartphones, which are in this case the loss, disclosure or destruction of information that is generally facilitated by the reduced size of the device;
* protect access to the smartphone with a personal PIN code;
* update with new software versions as soon as they are available.

Smartphones are given to people who, by their attributions, are invited to travel or to participate in fairs or seminars in Luxembourg and abroad.

## Software Installation

It is prohibited to download or install software that is not authorized by the IT department.

## Using the remote access of the company

Employees and third parties authorized to use the remote access of the company are responsible for contracting the services of an Internet service provider and for supporting the associated costs.

Moreover :

* they are responsible for ensuring that unauthorized users cannot use their rights or personal infrastructure to connect to the company's network;
* When a connection to the company is established, the user must in no case establish other connections with other remote sites, to avoid that the user's computer serves as a bridge for software malicious;
* the computer used to connect to the DMZ, must have an always updated antivirus;
* by using remote access from the company, the user must understand that his computer is an extension of the company's network. It is therefore subject to the same rules and regulations that apply to the equipment of the company. The computer must comply with the company's security policy;
* in the case of telework, for example, the employee must ensure that no third party has access to the company's assets through his remote access, that he does not engage in any illegal activity, and does not employ any other person access for commercial or other interests. The user is responsible for the consequences of any abuse;
* an idle connection for 30 minutes is automatically closed. The user must then reopen a new session. The use of techniques that allow to leave the connection open is strictly forbidden (periodic ping, etc.);
* All connections have an uptime of max. 24 hours. Beyond this, the user must reopen a new session;
* The programs used to manage remote communication can only be those that have been approved by the company's IT department.

# Use of Internet Services (Web)

The use of the internet must be done according to the following rules:

* the use of the internet and access to the sites must be done in compliance with the own usage policy specific to the various sites and networks used, and in compliance with the legislation in force.
* the user will pay particular attention to phishing. He will ensure that he is on the site he wants and not on a counterfeit. When he enters sensitive information, he will make sure that the connection is secure, including the presence of a padlock on his browser and that the URL of the page starts with HTTPS;
* It is forbidden for any user to surf sites that are offensive, racist, pornographic, pedophile, defamatory, violent, or that would harm others;
* the use of the internet for private purposes is tolerated, however it must comply with the conditions stated above and must not cause any trouble or malfunction of the work of other users;
* Downloading for private purposes, or that could harm the information system is prohibited. In case of doubt, you must abstain.

# Email Management

## Creating an account

For employees who have an email address specific to the company, the accounts are created when the employee takes office or when an external consultant intervenes for a mission of significant duration that requires one.

The name of an email is: [First\_name… .Last\_name @ …](mailto:Prénom.Nom@eco.etat.lu)

The initial installation is done by the IT department on the employee's workstation.

Access to emails is controlled by a user name and password that meets the requirements described above.

## Using e-mail

The company's e-mail processing system is mainly for business use.

In accordance with the law, every employee of the company has a right to privacy at work. The use of emails for personal reasons is therefore tolerated in reasonable quantities, provided that its use does not interfere with the proper performance of the daily tasks of the employee and the company. All private mail must show the mention "private" in its subject.

E-mails, like traditional letters, are subject to the rules of decency:

* It is generally considered polite to start with a greeting, and also to indicate a subject. It is the same with the politeness formula;
* the sending of attachments is also subject to rules of common sense (weight of the email according to the correspondent);
* In the event that a user receives an email that looks like spam or hoax (that is, unverified information and is often relayed by people of good will), he or she thinks and validates himself / herself this information before accepting it and possibly passing it on to other people. There are sites ([www.hoaxbuster.com](http://www.hoaxbuster.com) or [www.urbanlegends.com](http://www.urbanlegends.com)) to verify the veracity of the content of this kind of email. When in doubt, it is customary not to transmit this kind of content to one's relations;
* the user must not click on the links contained in the mails without first checking that the source is trusted
* the use of the hidden copy (Bcc, Bcc) that allows sending an e-mail without displaying certain recipients is not allowed in the organization. An exception exists, in the case of sending an email with your name in "send to:" and all other recipients in "Bcc, Bcc". In general, all recipients must be in "Bcc, Bcc" or none.
* CAPITAL writing is considered a screamed word, so avoid using it;
* before integrating additional people into "discussions" by e-mail, ask for the consent of your correspondents;
* avoid inserting unnecessary animations in emails;
* For security reasons, give preference to messages in TEXT format instead of HTML format if possible.

## Prerogatives to sending an email

E-mail is an unsafe means of communication (public communication channel), whether from the point of view of confidentiality, integrity or availability.

Employees must, before sending information by email, check whether the confidentiality of the information. Only data of the public type can be sent in the clear. Internal, restricted and confidential data must be encrypted before being sent.

## Saving emails

The e-mail system is an important work and communication tool that transmits and stores information. As such, the system is subject to backups. All e-mails in the user's accounts are saved without distinction of any personal character of the e-mail.

## Erasing large unprofessional emails

In order to ensure the availability of e-mail services, IT staff regularly check the evolution of the remaining storage space. When the availability of the email service is threatened by excessive use of resources, IT staff conduct a search for causes. Depending on the case, they may take corrective action following the procedure described below.

How to delete large or bothersome personal files:

1. IT employees request in writing that large personal files be moved or destroyed.
2. If no follow-up is given to this request, the IT department can erase these emails.

## Defended use of emails

Any inappropriate use that may jeopardize the security of the e-mail system or that may cause harm to society is prohibited.

In particular, it is forbidden to send e-mails that have repressive content by Luxembourg law. We can mention in particular:

* breach of trust (articles 491 to 493 of Code pénal) ;
* fraud (article 496 du CP) ;
* slanders, defamation and insults (articles 443 and following; CP 448 and 561-7);
* racism, revisionism and discrimination (article 454 CP);
* distribution of pornography to minors under the age of 16 (Article 385bis CP);
* Child pornography (article 384 du CP) ;
* the sending of objects protected by copyright and neighboring rights of third parties;
* sending professional secrets;
* the sending of documents whose classification prohibits any transmission by e-mail;
* Spam or sending, outside or inside the company, chain letters or joke emails.

Employees receiving emails from other company employees with prohibited content are asked to inform their supervisor or the IT department as soon as possible, since the image of the company is put at risk.

## Use of the electronic signature

Only employees who have a professional electronic signature card (linked with a company's own address) can use it for e-mail. However, all employees must adhere to the procedures in effect for signature warrants and delegations.

## Using encryption

If the use of encryption to protect the confidentiality of a content is required, it must be done with the cryptographic tools validated by the company.

## Security and Security Events

All emails sent or received by an employee of the company go through an antivirus and antispam detection. In case of doubt anyone who receives emails with linked files and who has uncertainties about the nature of these files (virus for example) should ask the IT department to check the files in question.

For information, there is a deadlock concerning certain extensions for the attached files (\*.EXE, \*.RAR, \*.ZIP, etc.).

## Template and signature

Use of the electronic signature is restricted to employees with administrative signing rights.

Each email must have a standard footer that includes:

* the surname and first name of the person;
* professional contact information;

the standard template provided by the IT department

# Management of keys and badges

Keys and badges should be like passwords, that is, personal. It is therefore strictly forbidden to lend keys or badges to another person. If any of these are lost, notify the person in charge of physical access management.

# Clean Office / Clean Desk

Removable paper and computer media containing sensitive information should not be left unattended on desks. Specifically, papers must be removed quickly from printers, fax machines or copy machines, and should not be thrown into garbage cans.

# Disposal

Any equipment that is discarded or reused in another context must be emptied of all its data in a way that is in relation to the sensitivity of the information contained therein.

Sensitive documents are shredded or deposited in a secure container.