الشركة الوطنية للصناعة و المناجم
SOCIÉTÉ NATIONALE INDUSTRIELLE ET MINIÈRE

HEAD OFFICE

Nouadhibou, Jully18, 2023

HO Memo number 134

The user charter for the proper use of Information Technology resources and services at SNIM

This text is an addendum to user agreement under its clause 30. It is above all a code of good conduct and aims at clarifying the users' responsibility to establish an appropriate use of the resources and services related to Information Technology.

1. Definitions

The term "Resources" shall referred to portable or fixed physical equipment made available to users or installed in the workspace: Computer, printer, scanner, photocopier, projector, radio, telephone, switch, access point, camera, cabinet, biometric reader, access control device, etc.

"Resources" also refers to files and databases, in addition to intermediate or central equipment that the user will be able to access, via the various telecommunication networks, using the equipment and/or available services.

The term "Services" refers to software systems: directories, software and various applications used in the day-to-day management of the various business lines of the SNIM and subsidiaries, email, intranet, Internet, video conferencing, CCTV, remote connection product (VPN), etc.

The term "User" shall refer to persons having access to or using resources and/or services

The term "company" refers to SNIM and all its affiliates or third party connected to SNIM's network

2. Access to Resources and Services

The use of the resources and services is only authorized in the exclusive scope of the professional activity of the users.

The use of the resources and access to the services is subject to the authorization of the Information Technology Manager. This authorization is strictly personal (limited to the person asking) and cannot be assigned in any case, even temporarily, to a third party. This authorization may be withdrawn if the need is no longer justified.

Any authorization shall end when the professional activity justifying it has ceased, even temporarily. This termination must be notified to the Information Technology department by the head of the structure of the user.

3. Rules of use, safety and alert

The use of the resources and services must be rational and fair and in compliance with the rules of the charter of ethics and the company's code of conduct, in order to avoid their deterioration or misuse for non-professional purposes.

Each user is the sole responsible of any activities done with the resources and service accessed by his identifier.

Every user is also responsible, at his level, to contribute to the general security of the company's information systems and telecommunication networks. In this context, the user is required to alert the Information Technology department of any event that may impact, directly or indirectly, the security.

In particular,

The user must:

- Attend training and/or information sessions on the use and security of Information Technology resources and services.
- Implement the safety and proper use recommendations communicated to him.
- Ensure the protection of his information. He is responsible for the rights he gives to other users and it is of his responsibility to protect his data using various means of backup available to him.
- Report to the relevant departments of the Information Technology any attempt to breach his account as well as any abnormality he might notice;
- Get approval from the Information Technology department prior to any software installation or configuration modification;

- Choose safe passwords, renewed periodically and kept secret. These passwords must under no circumstances, be communicated to third parties.

The user must not:

- Allow other users, even those authorized, to access through the resources and services of which he is the only holder.
- Attempt to access resources and/or services to which he is not authorized
- Use or attempt to use accounts other than his own or hide his true identity;
- Attempt to read, modify, copy or destroy data other than those belonging to him. In particular, he must not modify trace file or files containing credentials or usage history.
- Leave his workstation or those shared with other users without logging out, and must not leave resources or services accessible from his account.

4. Privacy rules

Users' access to information and documents stored on Information Technology systems (application databases, server shares, files on PCs or files attached to emails, etc.) must be limited to those owning these accounts.
In particular, it is forbidden to read information held by other users even if they have not explicitly protected them.
This rule also applies to telephone conversations, videoconferencing and emails for which the user is not the direct recipient or in copy.

5. Software usage right rules

Any software installation within the company, from broadcast media (DVD, USB, etc.) or downloaded from the internet, must be done only based on a license right granted by the software publisher or an authorized distributor. It is therefore, strictly forbidden to carry out any data breach or illicit acquisition ways.
The use of installed software must strictly adhere to their license rights.

6. Information Technology systems integrity preserving.

The user undertakes not to voluntarily cause disruptions to the proper functioning of information systems and telecommunication networks, either by unusual handling of the equipment, or by the introduction of unauthorized hardware or software.

7. Internet and email usage rules.

The user must show attention and maturity in the use of Internet services and emails.
In particular:

The user must know that:

- It is strictly forbidden to engage in any conduct relating to:
  - The use of account and/or equipment hacking techniques: Identity theft, infiltration attempt, vulnerability exploitation, etc.
  - The use of Cyberattack vectors: Generating and/or distribution of fishing emails (spam, scam), CSRF, XSS, denial of service, etc.
- The email address is professional and therefore, the company reserves the right to access the exchanges made and/or their content in the circumstances it deems necessary.

The user must not:

- Visit websites that broadcast content related to violence, racism, terrorism, blasphemy, plagiarism, trafficking of illicit products, pornography, pedophilia, etc.
- Go to video games websites, movie and television channels, etc.
- Steal information for malicious use: Data traffic, scam, etc.
- Give his professional email address on the internet except for professional necessity.

SNIM cannot be held responsible for the consequences of breaches committed by a user who did not comply with these different rules.

8. Analysis and control of the use of resources and services

The use of resources and services may be analyzed and controlled at any time, for various reasons.

The user must not, in any manner, evade these controls, and must apply the resulting instructions and recommendations.

The user should also be aware that SNIM's Information Technology systems record timestamped traces of user activity.

9. Enforcement and non-compliance

This policy applies to any person who accesses SNIM's Information Technology resources and/or services, and, in particular to SNIM's staff and connected entities (Subsidiaries and Foundation, etc.)

The charter will be notified to the relevant staff who are required to strictly respect it. Failure to comply may result to legal proceedings in addition to disciplinary actions.

الجيد

Board member and CEO,

Le Directeur Général

Mohamed Vall MOHAMED TELMIDY