Information Technologies and Telecommunications Policy

This his Policy defines the general conditions for the use of Information and Telecommunications Technologies.

Under this term are grouped together: the connection to the Internet, electronic mail, communication systems and, more generally, all the IT resources made available to the user by the company (PCs, Smartphones, etc.).

This policy specifies the rights and obligations that the employer and the user are required to respect in order to establish a proper use of ICT, in compliance with the legal and regulatory provisions in force.

These principles of use are based on the principles of mutual loyalty and trust.

1. PRINCIPLES

FIELD OF APPLICATION

This policy applies to all Company personnel, regardless of their status (employees, temporary staff, trainees, service providers, etc.), and more generally to all persons having access to the Company's IT resources, whether permanently or temporarily, on the Company's premises or outside by remote access from the network administered by the Company.

TERMINOLOGY

The term "user" therefore refers to any person who, regardless of his or her status, is required to create, consult and use the IT resources made available by the Company and/or the Eramet Group.

APPLICABLE LAW

Laws and regulations define the rights and obligations of persons using computerised means.

It is reminded that any person present on French soil must respect French legislation, in particular:
- the law of 20 June 2018 n° 2018-493, implementing the European Union regulation of 27/04/2016 known as RGPD (general regulation on the protection of personal data)
- the law n° 78-17 of 6 January 1978 relating to information technology, files and liberties;
- legislation relating to computer fraud (articles 323-1 to 323-7 of the Penal Code).

It should also be noted that there is a group agreement in force on the right to disconnection from the Internet for each employee.

THE RIGHT OF ACCESS

To access the network, each user receives an individual password and login.
They are responsible for protecting their password by ensuring that it is not divulged and that it meets a sufficient standard of security in terms of number of characters and complexity with regard to the instructions and procedures issued by the IT department.
This identifier and password must remain personal and must not be shared.

THE PURPOSE OF ACCESS

The use of computer resources and the use of Internet services and the network to access them are authorised within the framework of the users' professional activity.

The user must ensure the proper use of these computer resources and therefore has a duty to maintain their integrity, as in the case of any other tool made available to him/her in the course of his/her work.

2. MODALITIES OF IMPLEMENTATION

Organisation

The Human Resources Department and employee representative bodies undertake to deploy this policy locally within the applicable legal framework and to inform all employees of its implementation.

The Information Systems Department undertakes to follow the procedures described in this policy. All employees undertake to follow the rules described in the Policy.

Governance

The Eramet Group's Human Resources Department is responsible for deploying the Policy and ensuring compliance with commitments on the proper use of IT tools throughout the Eramet Group. This document is kept up to date jointly by the Employee Relations Department and the IT Department.

Method

GENERAL SAFETY RULES

All users are responsible for the use of the computer resources and network to which they have access. They are also responsible, at their own level, for contributing to the general security of their resources and indirectly to that of their company. Thus, the user must not modify the security parameters of his equipment.

The use of these resources must be rational and honest in order to avoid saturation or diversion for personal use.
Finally, it is up to users to respect the rules of confidentiality protection. In particular, it is forbidden to read information held by other users, even if they have not explicitly protected it. This rule also applies to e-mail-type conversations that are not sent directly or in copy to the user.

SPECIAL SAFETY RULES

The user must apply the company's safety instructions, procedures and recommendations, particularly in the following areas:

Data protection

The User must keep himself/herself informed and comply with the procedures relating to the classification, storage, transmission and destruction of information as well as the security of passwords.

The User must systematically lock his computer as soon as he leaves his workstation so that the content cannot be accessed.

The user must report to the IT department any attempt to violate his account and, in general, any anomaly that he may notice.

If the user has to send confidential data, he must take care to send it only to persons authorised in the context of their activity and after having verified their identity. Encryption solutions are made available by the company. It is up to the company to contact the IT department.

The user must not use personal services (dropbox, personal email...) to exchange or store professional data.

Rules for workstation

The user is responsible for the equipment (PC, laptop, smartphone, tablet, etc...) and tools entrusted to him. He undertakes to protect them so that they are not lost or stolen. They may not be transferred, lent or transmitted to third parties. He undertakes to refrain from modifying the established configurations.

Updates must be carried out within the deadlines that will be communicated by the IT department.
In the event of loss, breakage or theft, the user must urgently contact the IT department of the Company and/or the Eramet Group.

Software/hardware rules

It is forbidden to introduce any new hardware, programmes or software outside those supervised by the IT department, except with their authorisation. The same applies to so-called "Free" software.

Rules for removable medias

The use of a USB key, hard disk, CD/DVD is authorised provided that the user carries out an antivirus check targeted by the IT department and that this meets a professional need.

The storage of data on these types of media must be intended solely for short-term transfer and not for archiving or backing up data. The data must be stored on the file services provided by the Company (File Server, Sharepoint, etc.).

When not in use, removable media must be stored in secure locations.
The connection of personal removable media is prohibited.
The use of the workstation as an electrical recharging station, e.g. of a mobile phone, is not allowed.

Data backup rules

All business data stored on the workstation or equipment must also be stored on a company network resource. Data on the PC hard disk should be kept to a minimum.

It is the user's responsibility to sort the documents he receives (by email or other means) and to store them without delay in the location provided by his department/team (file server, sharepoint, etc.).

Protection against "Fraud" and "Phishing" and anomalies

The user must be particularly vigilant with regard to messages from outside the company whose sender is unknown or whose content is suspect. In case of doubt, he should contact his IT department.

Users are reminded that the origin of an email is never certain and that the name of the sender displayed is never a guarantee of its correct identity. The content of a sensitive email must be confirmed by telephone if necessary.

It is forbidden to make abnormal manipulations that could lead to the introduction of parasite software or viruses.

Safety Safety rules relating to telework and in mobility situations

The user must ensure in all circumstances that his working environment is adequate to preserve the integrity and confidentiality of the data. He will use the security screen filters to limit the risks.

The user must not use public equipment or networks (hotel, cybercafé...) for professional purposes.

Rules for managing arrivals/departures/absences with respect to data

The user has a duty of anticipation in the transmission of his data.

Thus, in the event of departure from the company or in the event of an anticipated prolonged absence, he must ensure the transmission of professional data, for the smooth running of the service, to the persons concerned.

It is forbidden for a user to delete all his professional data from the network and his workstation.
If he has not prepared his departure, the Company reserves the right to take action on the various files, folders, directories and e-mails of a professional nature. Any personal data stored on computer resources that has not been recovered after the user's departure from the Company will be destroyed.

Special rules for mobile phone

Like the workstation, the downloading of applications must be limited to applications authorised by the Company or the Group.
In the event of loss or theft, the user must immediately notify the IT department so that the telephone and its contents can be permanently erased without delay.

Special rules for messaging

An email address will be provided to users as part of their duties. This email address will be closed upon the user's departure and the email box will be destroyed after the employee's departure.

It is the user's responsibility not to redirect all or part of the emails from the professional letterbox entrusted to him/her to an email system outside the Eramet Group, for any reason whatsoever.

He must limit the number of recipients of his e-mails to the strict minimum.
It is recommended that documents be shared by sending by email only the link to the said document exchanged on a sharing tool provided by the IT department (e.g. a Sharepoint).

To prevent the risk of viruses, it is requested to check the origin and authenticity of messages, and it is advisable, when in doubt, to destroy messages from a stranger that contain an attachment, without reading or extracting it.

For specific application rules that have not been described above, it will be the responsibility of the user to comply with the relevant memos or procedures that may be issued to ensure the proper functioning of the IT means.

COMPLIANCE WITH LEGISLATION

Intellectual Property legislation

Obligations in terms of property rights require the user to respect copyright and intellectual property rights and not to copy, modify, distribute or use information, documents, works (texts, images, photographs, musical or audiovisual works, logos of the Company and/or the Eramet Group), software and associated licences for which he does not hold the required rights (rights of use, modification, reproduction, etc.).

Users must only use the software covered by the licence agreement of the Company and/or the Eramet Group in accordance with the terms of the licence.

All employees are prohibited from taking copies of Company and/or Eramet Group data out of the Company, except in the case of formal authorisation for use limited to the strict framework of their work, or in the specific cases of backup or maintenance operations carried out by the IT department.

Compliance with legislation on the rights of individuals and respect for privacy

It is strictly forbidden to consult, distribute or download sites, images or files, particularly those of an offensive or defamatory nature, which serve to provoke violence or racial, religious or sexual hatred, paedophilia and violence against children.

Compliance with any provision of public order and any provision not contrary to good morals

It is strictly forbidden to consult, distribute or download sites, images or files, particularly those of a pornographic nature, gambling, weapons, violence of any kind.

Compliance with legislation on personal data ("PDSR")

Any user who processes or accesses personal data relating to the internal personnel of the Company and/or the Eramet Group or to third parties (customers, partners, candidates, etc.) must strictly comply with the applicable regulations and the established guidelines associated with the processing. In particular, it will pay particular attention to respecting the purpose of the processing, confidentiality, protection and retention period of such data.

HOW TO USE INFORMATION SYSTEMS: INTERNET, MESSAGING, SOCIAL NETWORKS...

The user must make professional use of the information systems entrusted by the company within the framework of his professional activities and in compliance with the general principles and rules specific to the various sites that offer them, as well as in compliance with the legislation in force as mentioned above.

Exceptionally, use for extra-professional purposes is tolerated with regard to compelling family obligations and the necessities of everyday life for the use of the Internet and messaging.

Such use must be made outside working hours (during breaks). It must not impede the speed of

the network (risk of saturation), nor endanger the integrity of the network.

Electronic messaging

Email messages sent using the IT tools provided by the company are presumed to be professional. For personal use, messages must be explicitly identified in their subject line by the mention "personal".

Directories and files

Consequently, the user is asked to explicitly identify with the word "personal" the directory in which he can place personal files on his hard disk. He should not place professional files in this directory.

Users are reminded that this is a tolerance and that the Company does not guarantee that this directory will be backed up.

It is still forbidden to store personal data (photos, music, videos, etc.) on a shared storage space (file server, SharePoint space).

Social Networks & Internet Publishing

The user must not transmit confidential information on the Internet (social networks, sites, forums, mailing lists...), not engage in actions that jeopardize computer security, not express personal opinions that could damage the reputation of the company or harm it. It must comply with the laws and regulations in force.

PURPOSE AND FRAMEWORK OF CONTROLS

The IT security systems set up by the Eramet Group and/or the Company record the traces of the information passing through the network.

In order to preserve the security, integrity and confidentiality of the Information System, the use of hardware or software resources and exchanges via the network can be analysed and controlled in accordance with applicable legislation.

Thus, the following analysis and control systems are implemented for security purposes, to diagnose malfunctions or to check the conformity of workstations and implemented systems:

To the information system

The security configuration of the systems generates records (logs) - date and time, identifier used for the connection, services accessed - which can be traced and used for the purposes mentioned above.

At the workstation

A system for analysing and blocking malicious code, viruses and intrusions is in place.
The security configuration of workstations (including smartphones) generates records (logs) - date and time, identifier used for connection, messages generated by security devices (antivirus...) - which can be traced and used for the purposes mentioned above.

For the Internet

A system is set up to filter access to dangerous sites and/or sites that are contrary to legislation and morality.
The information recorded, for each Internet access, is notably the following: Address of the sites consulted (URL), User (login), type of flow (HTTPs, HTTP, FTP), and the volume of data received and transmitted. They can be traced and used for the purposes mentioned above.

For mailbox

A blocking / quarantine system is set up for dangerous emails.

The information recorded includes the sender, the recipient(s), technical information identifying the message, links and attachments linked to the email.

For the telephone

The information recorded at the business telephone infrastructure level is as follows: the telephone numbers called, the duration, date and time of the call, and the billing elements.

Information from analysis, monitoring and recording devices can be used in the following cases:

- On request of the authorities (administrative, judicial or police)
- In case of incidents or abusive use (virus, intrusion, saturation of resources, breakdowns...)
- In case of proven or suspected malicious acts.

ACCESS TO DATA

You are reminded that any letters or files created or received using the IT tool provided by the employer for the purposes of the position are presumed to be of a professional nature.
The company may therefore access messages, directories and professional files at any time, even without the presence of the person concerned.

Concerning emails and directories characterised as "personal", there is no obstacle to:

- These documents are checked by automatic security tools (i.e. antivirus...)
- The IT department may exceptionally access these elements when there is a proven risk, in particular of security, continuity of service or liability, in order to take protective measures, in the presence or not of the User and having informed the User.

With regard to emails characterised as "personal", network administrators are not prevented from accessing "email" messages and their content when there is a proven risk in terms of security or continuity of service.