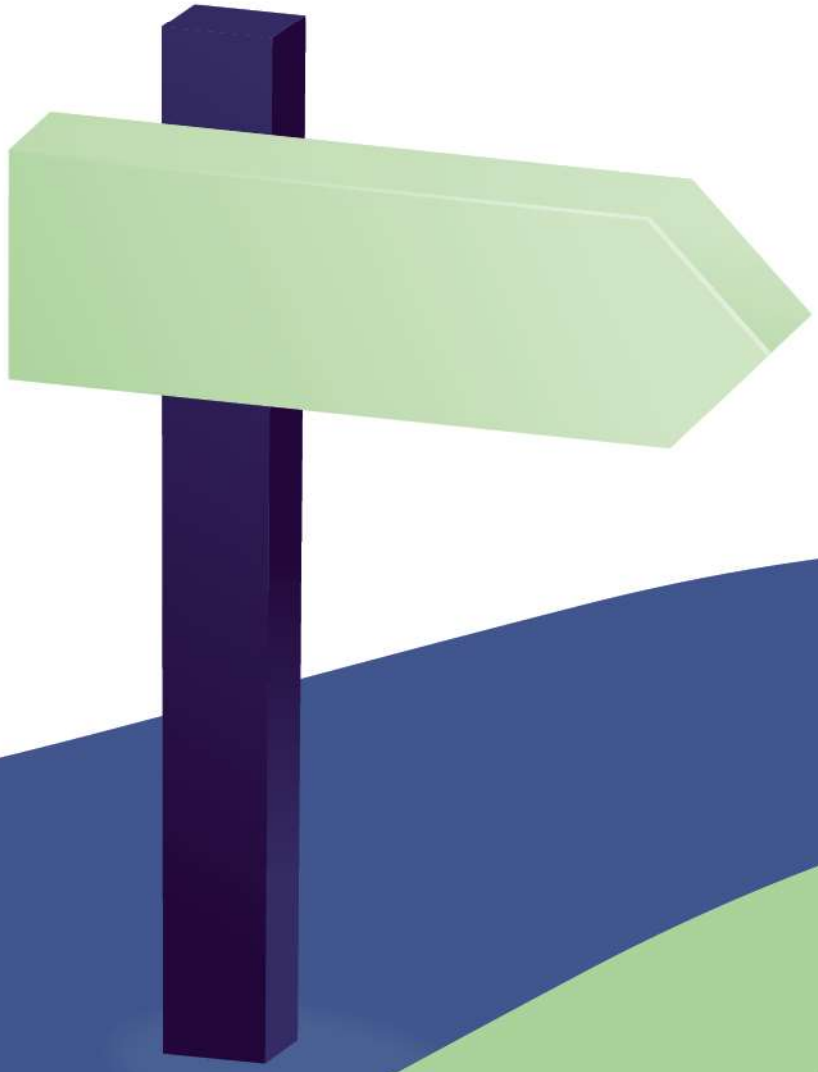
ErametManagementSystem

September 2023

POLICY

Digital usage Policy



eramet

OUR LONG-TERM OBJECTIVES

This Policy defines the general conditions for the use of Information and Communications Technologies by Group employees.

The term "Information and Communications Technologies" or ICT refers to a set of technological tools and resources used to transmit, record, create, share, or exchange information. These include Internet connections, e-mail, communication systems and, more generally, all the IT resources made available to users by the company (PCs, mobile phones, smartphones, etc.).

This policy sets out the rights and obligations that the employer and user are required to respect to ensure the proper use of ICTs in compliance with the legal and regulatory provisions in force.

These principles of use are based on loyalty and trust.

This Policy applies to all the staff of each Eramet Group company, regardless of their status (employees, temporary workers, trainees, service providers, etc.), and more generally to all persons who have permanent or temporary access to the Group's communication tools or IT resources, either on the company's premises or remotely from the network administered by the company.

It applies to tools made available to employees by the Group and to personal tools that the Group has authorised for professional use.

1. ERAMET GROUP COMMITMENTS

As part of its Digital usage Policy, the Eramet Group undertakes to:

EXCOM and Board of Directors

- **Provide** employees with the ICT tools they need to carry out their tasks.
- **Encourage** the use of ICTs by Group employees to improve performance and efficiency.
- **Promote a legal and regulatory framework that** enables balanced use of ICTs (right to disconnect, IT security rules, etc.), while also providing a secure framework for the Company.

Each Employee

- **Comply** with the general IT security rules defined by the Group, as well as local regulations.
- **Comply** with current legislation on public order and morality.
- **Comply** with the specific security rules defined by the Group in terms of data protection/backup, protection against fraud, phishing and other anomalies, use of removable media, etc.
- **Report** any misuse and/or dangerous use of ICT tools, whether in a professional and/or personal context.
- **Ensure** strictly professional use of the ICT tools provided.
- **Training** in the ethical use of ICT tools.
- **Report** any potentially dangerous events or content, as well as any suggestions for improvement.

It is the responsibility of each manager to ensure that he or she gives all employees the means to meet these commitments.

2. IMPLEMENTATION METHODS

The Eramet Group Human Resources Department is responsible for deploying the Policy and ensuring compliance with commitments on the proper use of IT tools throughout the Group.

This Policy is part of the Eramet Management System and therefore applies to all Group companies and sites. It may be adapted locally by the Human Resources Department if required by the applicable legal framework. The Information Systems Department undertakes to follow the procedures described in this Policy.

All employees are required to follow the rules described in this Policy.

To implement its Digital usage Policy, Eramet uses the following resources:

→ **Deploy a framework within the Group that complies with the legislation governing the use of ICTs. All employees must be familiar with and apply these rules.**

- Intellectual property legislation: respect for copyright and intellectual property rights; prohibition on copying, modifying, distributing or using information, documents, works (texts, images, photographs, musical or audio-visual works, company and/or Eramet Group logo), software and associated licences for which he/she does not hold the required rights - rights of use, modification, reproduction, etc.).Copies of data belonging to Eramet may not be taken out of the company except with **formal authorisation** for use strictly within the scope of the employee's work, or in the specific case of back-up or maintenance operations carried out by the IT department.

- Legislation on personal rights and respect for privacy: strict prohibition on consulting, distributing, or downloading sites, images or files that are abusive, defamatory, used to provoke violence or racial hatred, religious or sexual, paedophile or child abuse, and more generally contrary to applicable law in the employee's country

- Legislation on personal data (GDPR): any user who processes or accesses personal data relating to the company's and/or the Eramet Group's internal staff or to third parties (customers, partners, candidates, etc.) must comply strictly with the applicable regulations and the established guidelines associated with the processing. In particular, he/she shall take care to comply with the purpose of the processing, confidentiality, protection, and storage period of such data.

- Respect for public order and morality: it is forbidden to consult, distribute, or download sites, images or files of a pornographic nature, gambling, weapons or violence of any kind.

→ **Clearly define the rules governing employee access to ICT tools.**

- Access rights: to access the network, each user is given a password and an individual identifier. These must remain personal and must not be shared. Each user is responsible for protecting their password, ensuring that it is not divulged and that it meets a sufficiently high security standard in terms of number of characters and complexity, in accordance with the guidelines and procedures issued by the IT department.

- The purpose of access: users must ensure that the ICT resources made available to them are used correctly and have a duty to preserve their integrity. System administrators have certain privileged access rights to administer and control these systems. They must respect a strict confidentiality clause.

→ **Clearly define the rules to be respected in terms of IT security.**

- Prohibition on employees engaging in actions that jeopardise IT security.

→ **Clearly define the way in which Group employees use the Information Systems.**

- Make professional use of the communication tools and information systems entrusted to them by the company.

- Do not store personal data (photos, music, videos, etc.) on a professional shared storage space (file server, SharePoint space).

- Do not post confidential information on the Internet (social networks, websites, forums, mailing lists, etc.).

- Do not express personal opinions that could damage the company's reputation or be prejudicial to it.

→ **Establish a system for monitoring the rules set out above**

- The IT security systems put in place by the Eramet Group and/or the Company record traces of information passing through the network.

- To preserve the security, integrity, and confidentiality of the Information System, and to ensure compliance with applicable regulations and this Policy, the use of hardware or software resources and exchanges via the network **may be analysed and monitored in compliance with applicable legislation**.

Compliance with the principles and rules governing the use of ICTs is integrated into the control, inspection, and audit processes.