INFORMATION SYSTEMS POLICY

The Board of Directors of Barna Steel, S.A., on behalf of the entire Celsa Group ('**Celsa Group**'), in the context of its general and non-delegable power to determine the general policies and strategies of Celsa Group, has approved the *Information Systems Policy* (the '**Policy**').

I. Purpose

Broad sweeping information technology and information flows are important factors to consider having an adequate internal and external communications network in the company, which requires establishing measures to protect the company's assets and the correct performance of its productive activity. Celsa Group's internal operating rules establish that the IT and other resources provided by the company are provided as work tools. All users must use the Celsa Group corporate network and its data without engaging in activities that may be considered illicit or illegal, that infringe the rights of the Company or of third parties, or that may violate morality or the rules of etiquette of remote networks.

The purpose of this Policy is to ensure that technological resources are used appropriately, to set out clear rules about the possible use for personal purposes of email, internet,and other facilities such as telephones, in the office or remotely, and to inform users about the monitoring of these activities and the reasons for doing so. Any violation of the Policy may be considered misconduct and subject to appropriate disciplinary action. If you are unsure whether something you intend to do may be in breach of this Policy, you should seek advice from your manager or consult the IT ServiceDesk manager or the Ethics and Compliance Committee.

II. Scope

This Policy applies to Celsa Group and all group companies, taking into account their specific characteristics. Celsa Group will work to ensure that the policies of its Group companies are in line with this Policy. In the case of activities performed by Celsa Group outside Spain, this Policy will be adapted to the more restrictive local legislation applicable.

III. General Principles

By means of this Policy, Celsa Group assumes and promotes the following general principles that should guide all its activities:

a) Direct our efforts toward the prevention of errors, as well as to their correction, control and management.

b) Promote continuous training and awareness of information security.

c) Ensure that the Company complies with the requirements established by legislation on information security.

d) Establish systematic actions for controlling, monitoring and preventing incidents.

e) Guarantee the confidentiality and authenticity of information, protecting data and information systems against improper access, cyber-attacks and unauthorised modifications.

f) Act appropriately and jointly to prevent, detect, and respond to cyber incidents that could affect information security.

IV. General Content

a) User IDs and passwords

Most Celsa Group information systems require password use. All users agree not to share their user IDs and password for access to Celsa Group's information systems with anyone else. If you suspect that someone else knows your ID and access credentials, you must change your password. Users will be solely responsible for any actions carried out with their user ID.

The IT ServiceDesk will provide the necessary assistance in managing passwords. In this respect, every user must change the password of any computer or mobile phone device on a regular basis, as well as establish a sufficiently secure password.

b) Computer use

Desktop or laptop computers will be used exclusively for business purposes, subject to the following exceptions:

Users may make limited use of the Company's computers for sending personal emails outside of their working day or during break periods within their working day and in accordance with the Policy. The subject line of the message must include the word 'Personal'.

Users may make limited use of the Company's computers for browsing the internet for personal reasons, outside their working day or during rest periods within their working day and always in accordance with all the terms of the Regulations implementing the Policy.

Misuse of the internet and email can pose serious risks to Celsa Group companies, such as the introduction of viruses, infringement of copyright laws, or imputation or defamation of third parties. Moreover, email, often viewed as an informal method of communication, should be considered equivalent to an official paper letter from the Company. Negligent use of Company email or the internet can have serious consequences and the Company therefore imposes strict limits on professional or personal use.

The Company reserves the right to refuse permission for personal use in individual cases if it deems it appropriate to do so.

c) Viruses

Users must let the IT ServiceDesk update any anti-virus systems and cooperate in their maintenance and updating to prevent any incursion that could destroy or corrupt information or data on the Celsa Group network.

Users must not connect any of the Company's computers or laptops to clearly unsecured networks, or install 4G internet access devices without authorisation, as this could cause a breach in the security of the systems with the risk of introducing viruses and other types of malwares. Breach of this rule could be considered a serious offence.

d) Email

All communications made by Celsa Group professionals within the scope of their responsibility by any means must respect the ethical principles established by Celsa Group, including, of course, communications made via email.

Users must not send, forward, distribute or retain email messages containing abusive, aggressive or offensive language. When composing an email, users agree not to make use of expressions that are considered inappropriate in reference to matters of a personal nature and in particular about race, colour, religion, beliefs, gender, age, nationality, sexual orientation or disability, or those that contain or imply attitudes of harassment at work or sexual harassment. Similarly, those containing them should not be resent or distributed.

The performance of Celsa Group's networks may be affected by sending large attachments in emails such as video clips, large images or large quantities of attachments, junk or spam emails, viruses' hoaxes, chain or pyramid messages, and other types of messages sent and received that are not related to the operation of the business.

In this regard, users must delete their electronic communications and attachments after a reasonable period of time has elapsed and it has been ascertained that they are of no use or that it is unnecessary to store them on the Company's equipment. Celsa Group reserves the right to monitor the performance of its networks and may delete any elements whose storage is not considered necessary or may recover those files incorrectly deleted, if either of these actions is considered appropriate.

Users must not generate or send emails that are not related to their professional activity in the Company and must, in turn, demand the same behaviour from all other users.

Users may not use email accounts with domain names owned by Celsa Group in their personal online activities, nor may they register with social networks, online services or other non-professional resources with these users.

Users may not use passwords previously used by Celsa Group in their personal online activities, nor may they use passwords previously used by Celsa Group in their personal online activities, social networks, online services or other non-professional resources

e) Internet browsing

Users must not, under any circumstances, access web content of an inappropriate or offensive nature, or store or distribute such material to the internet or by email using the Company's computers. Examples of inappropriate or offensive content include racist material, pornography, sexually explicit images of all kinds, as well as text and other related materials, promotion of illegal activities, intolerance of others, gambling or betting on the internet.

f) Use of business telephone devices for private use

This Policy applies to both fixed lines and mobile or 4G devices. Users may use Company telephones for private use only in an emergency or for essential calls for which authorisation should be sought in the first instance from their line manager.

For private use, the use of services that generate an additional cost to the Company, such as calls to chat lines, SMS subscriptions, etc., as well as the use of services with associated costs through the Company's 4G devices, is not permitted.

The use of business telephone devices has, in addition to the limitations set out in this section, all those applicable to them in relation to similar functions that can be executed on 'smart' telephones and those equivalent to computers and PCs, as well as those relating to computer viruses, email and any other that are similar due to their nature.

g) Protection of company portable devices; computers, smart phones, tablets or other

To protect the information and devices owned by Celsa Group, all mobile devices will have a remote management system (MDM) that allows, among other things, to protect them from external attacks, in particular cyber-attacks, installing remote work applications, providing remote support and applying automatic configurations such as corporate email. In any case, the management and processing of the MDM tool will be controlled by the IT department for the purposes described above, in accordance with the legal provisions in force.

h) Geolocation of devices

Users are aware that the devices owned by the company may be equipped with geolocation systems. The installation of these devices is primarily intended for use in cases of user emergencies, such as

accidents, as well as for recovery in cases of loss or theft of equipment. The activation of the action protocol in these cases will be expressly authorised by the Chief People & Organisation Officer.

i) Use of a private mobile phone during working hours

The use of private telephones during working hours must be kept to a minimum; the detailed regulation of their use will be established in the Regulations implementing the Policy.

j) Monitoring of communications

The Company may keep records and audit the use of telephones, landlines and mobiles, fax machines, computers or other devices owned by the Company, including email systems, internet and other systems, the regulation of which will be set out in the Regulations implementing the Policy.

If there is sufficient evidence or suspicion of the commission of an unlawful act or conduct contrary to the rules, principles or Code of Ethics and Professional Conduct of the Celsa Group, the Company may keep records and monitor telephone calls, faxes, computer files and internet use as well as emails sent, received and stored, subject to the legal limitations and safeguards provided for in the applicable legislation, with the prior authorisation of the Chief People & Organisation Officer.

All users will be informed of the content of this Policy and its implementing regulations so that they are aware of these monitoring possibilities.

k) Social media

The rules of this Policy and its Regulations concerning the use of computer equipment, emails and internet browsing are fully applicable to users' access to social media during work time and/or with the media or equipment owned by the company.

V. Specific content contrary to this Policy

The following practices will be considered contrary to this Policy and its implementing regulations in view of the danger they pose to the integrity of the security of Celsa Group's information systems. These practises are considered serious or very serious offences within their scope.

1. Allow the use of a Company computer to someone outside the Company, i.e. someone who is not a direct or indirect employee of a Celsa Group company.
2. Use the system to attempt to access restricted areas of the company's computer systems or those of third parties.
3. Attempt to read, delete, copy or modify the email messages or files of another user.
4. Attempt to decipher passwords, encryption systems or algorithms and any other security element involved in Celsa Group's remote processes.
5. Attempt to enhance the level of one's own or another user's privileges on the system.
6. Voluntarily obstruct the access of other users to the network by means of massive consumption of Celsa Group's computer and remote resources.
7. Access to real-time discussions (Chat/IRC) as they are particularly dangerous, as they facilitate the installation of utilities that allow unauthorised access to the system.
8. Use radio/TV receivers on the Company's computers. In some countries, the use of TV receivers is illegal without a TV licence.
9. Enter data into Company computers from personal devices such as USB memory sticks, pen drives, SD cards or similar, especially in industrial environments.
10. Voluntarily introduce programs, viruses, macros, applets, Active X controls or any other logical device or sequence of characters that cause or are likely to cause any type of alteration in the computer systems of the entity or third parties.
11. Introduce, downloading from the internet, reproducing, using or distributing computer programs not expressly authorised by IT Celsa Group, or any other type of work or material whose intellectual or industrial property rights belong to third parties, when not authorised to do so.
12. Introduce obscene, immoral, offensive, racist or discriminatory content, in accordance with the laws in force in the countries in which IT Celsa Group is present.
13. Delete any of the legally installed programs.

14. Destroy, alter, disable or in any other way damaging the data, programs or electronic documents of Celsa Group or third parties.
15. Attempt to distort or doctor system LOG records.

VI. Confidentiality of information

It is forbidden to send confidential information of Celsa Group to the outside, by means of material supports, or through any means of communication, including simple visualisation or access.

Professionals, users of corporate information systems, must maintain the utmost confidentiality for an indefinite period of time and must not disclose or use, either directly or through third parties or companies, the data, documents, methodologies, keys, analyses, programmes and other information to which they have access during their working relationship with Celsa Group, whether on physical or electronic media.

No employee may possess, for uses outside their own responsibility, any material or information owned by Celsa Group.

The Regulations implementing this Policy will regulate the details of the temporary possession, use and return of any kind of information owned by Celsa Group and/or classified as confidential.

The duration of the confidentiality obligations established in this document will be indefinite, remaining in force during the term of the employment or contractual relationship with Celsa Group and after its termination.

Failure to comply with this obligation may constitute an offence of disclosure of secrets and will entitle Celsa Group to demand financial compensation from the professional.

VII. Ownership and Security of Information

Celsa Group companies are the owners of the information and rights of use and exploitation of software programs and systems, equipment, manuals, reports and all documents installed on the equipment and devices owned by them.

In that sense, all emails, messages and documents sent and/or received by professionals using the Company's email system are considered to be the property of the Company. In the same sense, so are all files of any kind that are hosted on its computer system and file system.

Professionals must not operate, reproduce, replicate or transfer systems or applications used in the organisation for purposes unrelated to the Company. Furthermore, they are obliged to comply with all measures and protocols established for the maintenance of security, control, access and use of the systems established in Celsa Group.

The workstation will be under the responsibility of the authorised professional, who must also ensure that confidential information cannot be viewed by unauthorised persons. The implementing regulations will establish the specific measures regarding the use of screens and printers for this purpose.

VIII. Governance system for reporting systems

a) Reporting of offences

Both internal and external personnel who, by any means, become aware of the commission of breaches of this Policy, as well as of any conduct that may infringe the legal and/or ethical rules established by Celsa Group, must report them to those responsible through the communication and reporting channels made available to them on the corporate intranet.

b) Data protection

Professional users of Celsa Group's information services must follow the Data Protection Policy always. The Regulations implementing this Policy will establish the obligations and responsibilities that apply to all personnel who have access to the information systems and, in particular, to personal data.

Special mention of the express prohibition of:

1) Creating files containing personal data without the express authorisation of the person responsible for the file.
2) Altering the purpose of any file containing personal data.

This Information Systems Policy was approved by the Board of Directors of Barna Steel, S.A., representing the entire Celsa Group, on 2023, July 13th.