1. DEFINITIONS

TERM	ACRONYM	DEFINITION
User	-	Agent who uses any equipment or information technology system covered by the terms of this Policy, whether a direct employee or service provider;
Disposal	-	Elimination of expired, obsolete, and/or duplicate physical or digital documents. Preferably, physical documents must be destroyed through processes that allow paper recycling and prevent document readability.
Document		A unit composed of information and its medium, produced or received as a result of an activity, preserved to serve as evidence, testimony, and research.
Backup	-	A backup copy of data from a device or storage system that can be accessed when recovery is needed.
Information Management Table (IMT)	IMT	A tool that establishes the retention period of company documentation throughout its archival phases, considering its value and responsibility for storage, identifying vital records and contingency plans.
Taxonomy	-	Structure used to classify and store all documents generated or received by Brazilian Nickel S/A during its activities.
Responsibility Matrix	-	Instrument that defines who is responsible for performing and supporting document management in each area/program to ensure implementation and maintenance of the documentation process.
Confidential Information	-	Information intended for specific individuals, whose unauthorized disclosure could cause damage and/or risk to finances, company image, or project execution, accessible only to designated employees.
Restricted Information	-	Information accessible to employees within a specific department or workgroup.
Internal Information	-	Information that may be accessed and disclosed internally.
Public Information	-	Information that may be accessed and disclosed both inside and outside the companies of the Brazilian Nickel S/A Group.
Information Management System (DMS/ECM)	GED	Technology that facilitates control, storage, sharing, and retrieval of existing information, such as SharePoint or ECM systems.
Information Management Products and Services	-	Any initiative aimed at storing, cataloging, and managing corporate content (e.g., knowledge bases, portals, action plans, lessons learned).
Group	-	All companies are directly or indirectly controlled by the companies. The term “subsidiary” and/or “controlled companies” is as defined by the Brazilian Corporations Law (Law No. 6,404/76).
Information Assets	-	Tangible and intangible assets of Brazilian Nickel S/A, comprising the information itself (of any nature), information technology equipment, hardware, personal data, systems and software, as well as techniques, know-how, and any other information related to Brazilian Nickel S/A and its activities.
Security Incident	-	Any confirmed or suspected event that compromises or may compromise the confidentiality, integrity, availability, or authenticity of the Company’s Information Assets. This includes unauthorized access, loss, leakage, destruction, improper alteration, unavailability, operational failures, anomalous behavior, misuse of credentials, cyberattacks, malware, or any situation that poses a risk to business continuity, personal data, corporate information, or critical organizational assets.
Artificial Intelligence	IA	Any system, model, or technology capable of performing tasks that would normally require human intelligence, using computational methods such as machine learning, natural language processing, computer vision, or predictive models to analyze data, identify patterns, generate content, support decisions, or execute actions autonomously or semi-autonomously.
Enterprise Resource Planning	ERP	Integrated business management system that centralizes and automates the processing and consolidation of an organization's data and operational processes, including areas such as finance, accounting, procurement, inventory, human resources, and operations.
Antivirus	-	A system designed to protect against computer viruses.
Malware	-	A malicious file designed to damage or exploit devices and/or IT services.

Enterprise Content Management	ECM	Systems and practices for managing the lifecycle of unstructured information.
Honeypots	-	Networks used to test cybersecurity attacks, designed for research and data collection from attackers.
Graphics Processing Unit	GPU	A hardware component designed to process and accelerate operations related to graphics and image rendering in computers and mobile devices.
General Data Protection Law	LGPD	Law No. 13,709/2018 is the Brazilian legislation that regulates data processing activities and focuses on creating a legal security framework, with standardized regulations and practices to promote the protection of personal data of all citizens.
PIPEDA (Canada's Personal Information Protection and Electronic Documents Act)	PIPEDA	Canadian federal privacy law governing personal data handling.
European Union General Data Protection Regulation	GDPR	EU regulation on data protection and privacy.
UK data protection legal framework.	UK GDPR / DUAA	The British data protection regulatory framework consists of the UK GDPR, the Data Protection Act 2018, and the Data (Use and Access) Act 2025, which together govern the processing of personal data by public and private organizations in the United Kingdom. The regime establishes legal bases for data processing, data subject rights, security obligations, and international transfers, and applies to any organization that processes data of individuals located in British territory.
Applicable Data Protection Laws	-	Data protection laws applicable to the operations of the Brazilian Nickel S/A Group, including the LGPD, GDPR, PIPEDA, UK GDPR / DUAA, as well as any other rules, regulations, or guidance from relevant supervisory authorities on the protection of personal data in force in the jurisdictions where the Company operates, which may vary depending on the country of operation.
European Union Artificial Intelligence Act	EU AI Act	Regulation (EU) 2024/1689 is European Union legislation that governs the development, commercialization, and use of artificial intelligence systems, classifying them according to their risk level and establishing proportional obligations for providers and operators that act in or impact European territory.
Applicable Artificial Intelligence Laws	-	Laws governing the development, deployment, and use of artificial intelligence systems in accordance with the operations of Brazilian Nickel S/A, including the EU AI Act, as well as other rules, regulations, and guidance from competent authorities on artificial intelligence in force in each jurisdiction where the Company operates, which may vary depending on the country of operation.

2. OBJETIVOS

I. The purpose of this policy is to define the principles, guidelines, and actions related to the governance of data, documents, and corporate information across all companies within the Brazilian Nickel S/A Group, as well as to ensure the proper and appropriate use of the Internet, Intranet, Extranet (controlled access for suppliers, partners, clients, or service providers), IT assets, and Computing and Communication Resources, with the aim of ensuring the security, compliance, integrity, publication, and availability of all information resources necessary for the execution of the Group's processes..

II. This policy also aims to describe the acceptable use of computer systems and equipment within the company, as well as all of its Information Assets. These rules exist to protect employees, the company, its clients, and suppliers. The improper use of computer systems and equipment exposes the company to risks, including virus attacks, compromise of systems and network services, and legal issues.

III. Finally, this regulation also aims to establish hardware specifications for desktops, laptops, and complementary devices for use in the Brazilian Nickel S/A operational environment in which technology provides support.

3. SCOPE

IV. O The scope of this policy applies to all employees, service providers, and other users involved, directly or indirectly, in the generation, receipt, storage, processing, consultation, organization, and archiving of documents and information generated or received by any department, unit, or company of the Brazilian Nickel S/A Group, in Brazil or abroad.

V. This policy covers the use of all IT systems, applications, devices, and equipment managed by the Group or by third parties that store, process, or transmit data and information, regardless of the format in which they are presented. This includes computer networks, hardware, software and applications, mobile devices, and telecommunications systems. It also includes information processed by other organizations in their business relationships with the company, such as clients, suppliers, service providers, and institutional partners.

4. DUTIES AND RESPONSIBILITIES

VI. All employees, service providers, and other users of the Group's data and information must be aware that the information generated and handled through the systems is the property of Brazilian Nickel S/A.

VII. All employees, service providers, and other users of the Group's systems, data, and information must be aware of the guidelines set forth in this Policy, especially the rules that directly and specifically affect them.

VIII. The effective security of Brazilian Nickel S/A's assets is a collective effort involving the participation and support of all company employees.

IX. In addition, there are several parties responsible for the acceptable use and management of data and information. This includes specific responsibilities of Brazilian Nickel S/A, Employees in General, Managers, the Information Technology department, the Legal department, and third-party service providers. Each of these is described in this policy.

4.1. Institutional Roles of Brazilian Nickel S/A

- Ensure that all data, documents, and information are maintained in secure environments.
- Assume responsibility for providing data security and management tools.
- Ensure data monitoring and protection through standards, policies, and guidelines in accordance with the General Data Protection Law (LGPD) (Federal Law No. 13,709/2018).
- Act in a timely manner in the event of a data security risk, taking legally appropriate measures.
- Enforce sanctions and disciplinary measures in cases of data breaches and violations of this policy.

4.2. Legal Department Obligations

- Provide legal advice to managers, employees, third parties, the Board of Directors, and the IT department regarding compliance with the LGPD.
- Guide the correct procedures in cases involving sanctions and disciplinary measures for data breaches and violations of this policy.
- Study and provide legal counsel in the event of litigation or breaches involving the Group's data or information.
- Identify legal risks related to the security and governance of Brazilian Nickel S/A's data, documents, and information.

4.3. Manager's Obligations

- Ensure that this standard is applied and, in case of doubt, request validation of the correct procedure from the Information Technology department.
- Guide employees and service providers on proper procedures for the use and management of Information Assets, as well as on proper compliance with the guidelines established by this policy.
- Identify violations of this policy, report them to the Information Technology department, and apply appropriate disciplinary measures, in accordance with guidance from the Human Resources and Legal departments.
- Specify who is authorized to access the documents and information under their responsibility.
- Ensure that all formal records received are stored in accordance with the standards established by the Data Security and Governance Policy.

4.4. Employee's Obligations

- Immediately report to IT any detected data or information leak or theft.
- Be aware of and act in accordance with the Data Security and Governance Policy, protecting information owned by Brazilian Nickel S/A, sent or stored in any physical or electronic medium;
- Handle relevant information and processed personal data with care, using such information only for purposes appropriate to your role and activities.
- Be responsible for the preservation, security, and reliability of Brazilian Nickel S/A information.
- Ensure that all documents and information under your responsibility are handled in accordance with the rules and procedures for document and information management.

- Request updates to document and information management tools from the IT department whenever necessary.
- Protect and control information stored on removable media and workstations.
- Return, in perfect physical condition, all information assets in your possession belonging to Brazilian Nickel S/A, upon request or upon termination of your activities.
- Use information and/or personal data only for the period necessary to fulfill its purpose and/or in accordance with the retention period required by applicable legislation.
- Take the necessary precautions when disclosing information about the Group, regardless of the medium (landlines, email, mobile phones, radio communications, among others).
- Verify that third parties or contractors have signed the appropriate confidentiality agreement with Brazilian Nickel S/A before sharing documents and information of the institution.

4.5. Obligations of Third Parties and Service Providers in General

- Be familiar with and act in accordance with this policy, protecting information owned by Brazilian Nickel S/A that is sent or stored on any physical or digital medium (paper or electronic).
- Ensure the confidentiality of relevant information to which they have access and not use it to obtain advantages for themselves or others, protecting it from unauthorized access.
- Use data and information strictly within the contractually defined scope and in compliance with data protection legislation.
- Maintain the confidentiality of the information to which they have access as a result of providing their services.
- Ensure that all documents and information under their responsibility are handled in accordance with the rules and procedures related to Document and Information Management.
- Return, in perfect physical condition, all information assets in their possession belonging to Brazilian Nickel S/A, upon request or upon termination of their activities.

4.6. Obligations of the Information Technology Department, Information Security Analysts, and System Administrators

- Ensure that all equipment and systems are kept up to date and fully operational throughout their lifecycle to achieve the company's objectives.
- Ensure that software and applications not approved by the organization are not installed on company-owned hardware or other equipment.
- Install antivirus/anti-malware applications and all business applications deemed necessary for users to perform their duties.
- Monitor and protect data in accordance with the rules and guidelines set forth in this policy and in the applicable Data Protection Laws.
- Identify security risks related to data and/or technology equipment.
- Develop, maintain, and disseminate policies, standards, procedures, and tools related to information management and data governance.
- Guide employees and service providers on proper information management and data governance procedures, as well as compliance with this policy.
- Provide technical support and validate operational procedures developed by the Group's areas.
- Coordinate Information Management and Data Governance actions to ensure compliance and standardization of document processes.
- Conduct audits, whenever necessary, to verify proper storage of documents and information.
- Support the definition, development, and configuration of tools for document and information management.
- Train and support Group employees in information management and data governance methodologies and technologies.
- Select, approve, and request the hiring of suppliers, partners, and service providers related to data governance and security.
- Take responsibility for developing and updating data security and management tools, such as procedures, flowcharts, and standards.
- Provide appropriate materials for storage, as well as trained personnel to perform the activity.
- Ensure compliance with and broad dissemination of this Policy and related regulations.
- Perform preventive, predictive, and corrective maintenance on systems, software, applications, programs, devices, and IT equipment managed by the company.
- Establish appropriate procedures for the reduction or destruction/disposal of media and equipment.
- Manage, protect, and test backup copies of critical business data and information.
- Assign each account or access device (computers, systems, databases, and other Information Assets) to an identifiable responsible individual.
- Implement a continuous vulnerability management process focused on monitoring, remediation, eradication, and defense.
- Create and implement processes for managing access to restricted IT environments, such as data centers, rack rooms, and sensitive equipment areas.
- Develop a Disaster Recovery Plan (DRP) for fast and effective restoration of data and information lost due to disasters.
- Manage information security incidents, ensuring proper handling.
- When providing equipment to employees, ensure they sign the Equipment Responsibility and Usage Agreement, and ensure the return of assets upon termination of employment.

4.7. Obligations of the Data Protection Officer ("DPO")

- Support the Information Technology Team in the procedures for analysis, investigation, and proposal of solutions in matters involving personal data.
- In accordance with Article 48 of the LGPD, when applicable, notify the National Data Protection Authority ("ANPD") and the data subject(s) of the occurrence of a security incident that may pose a risk or cause significant damage to the data subjects, in compliance with the guidelines of the Incident Management Policy.

5. GUIDELINES

5.1. General Guidelines

X. The guidelines set forth herein aim to establish a standard to be adopted by the recipients of this Policy, in order to ensure the security of Information Assets, assigning to all the responsibility and commitment for its implementation. All exceptions must be approved by the IT team and the responsible Manager.

XI. Company data must only be stored on official company devices that have been backed up and approved by the IT team.

XII. The Information Technology Department, together with the DPO and CFO of Brazilian Nickel S/A, shall be responsible for developing the responsibility matrix to designate those accountable for supporting document management in each area of the company.

XIII. Sharing is only permitted through platforms such as SharePoint and Teams, when licensed and approved by Brazilian Nickel S/A. This ensures secure data transfer and compliance with the principles of purpose, adequacy, and necessity for the recipient of the information/data.

XIV. Updates to policies, standards, or procedures related to Information Governance and Management may only be officially disclosed when prepared or validated by the Information Technology Department.

XV. This policy must be updated annually by the Information Technology Department, or whenever necessary.

XVI. To process generated or received documents, document and information management tools must be approved and validated by the Information Technology Department in conjunction with the areas that generate the documentation.

XVII. The contracting of products and services related to Document and Information Management by any department or Group entity without proper approval from the Information Technology Department is prohibited, subject to applicable disciplinary measures.

XVIII. Any exception to this Policy must be approved in advance by the IT team through the request form available on the Corporate Financial Portal on the Intranet.

XIX. Any request to amend this policy must be evaluated and approved by the Information Technology Department through Change Management (Corporate Financial Portal), and reviewed jointly with the DPO and CFO of Brazilian Nickel S/A.

XX. Brazilian Nickel S/A information must be handled in strict compliance with the Data Retention and Disposal Policy, ensuring that its retention, storage, and disposal occur in accordance with the deadlines, criteria, and requirements established therein, in order to ensure legal compliance, protection of personal data, and mitigation of risks related to misuse or improper retention of records.

XXI. Users are assigned rights and duties to support and monitor compliance with this Policy, and all must report any non-compliance, risk, or information security incident to the Information Technology Department via email at suporte.ti@brnickel.com and/or itsupport@brnickel.com, as applicable.

5.2. General Us and Ownership of Information Assets

XXII. The systems and equipment made available by the company (including servers, desktops, notebooks, tablets, network equipment, telephones, smartphones, projectors, software, applications, business systems, databases, storage media, and any other tangible or intangible assets provided by the Information Technology Department), even when assigned to employees, are the property and responsibility of Brazilian Nickel S/A. The handling of these assets represents only temporary custody, not possession or ownership, and any reproduction or retention by users is prohibited.

XXIII. Systems and equipment must be used exclusively for professional activities intended to serve the interests of Brazilian Nickel S/A.

XXIV. The use of company equipment for performing activities and storing personal files is not permitted for Users. However, personal use for non-corporate purposes is only allowed with company authorization, through the request form (Corporate Financial Portal) and via email at suporte.ti@brnickel.com and/or itsupport@brnickel.com. Additionally, such use must only occur during appropriate breaks that do not affect work productivity. Respecting company policies, prioritizing professional tasks, and setting time limits for personal activities are also important practices.

XXV. Any use of technological resources must be responsible, avoiding overloading equipment and maintaining the security and confidentiality of company data.

XXVI. It is essential that employees are aware of the organization's specific policies on this matter and assume personal responsibility for any damage or issues caused to company equipment.

XXVII. In the event of theft, robbery, or loss of any equipment or device, the employee responsible must immediately report it to the police authority of the respective state and country where they are located. Subsequently, they must submit the report to the Information Technology Department, detailing the incident.

XXVIII. To ensure the protection, integrity, and proper maintenance of Information Assets, the Information Technology Department is responsible for continuously monitoring equipment, systems, and network traffic through specialized tools and corporate information security and management platforms (such as monitoring, logging, and event correlation solutions), in accordance with the organization's Information Security policies and guidelines.

XXIX. Users must not use company systems and equipment for illegal, unethical, harmful, or unproductive purposes, as this exposes the organization to risk. Under no circumstances is any employee authorized to use Brazilian Nickel S/A systems and equipment for any illegal activity, in accordance with local, state, and federal laws.

XXX. The installation of systems on Group equipment will only be permitted if expressly authorized through the request form (Corporate Financial Portal), available on the Intranet. In such cases, the employee must ensure that the software or application is not pirated and that it is used exclusively for activities related to their work routines. For portable computing devices, including laptops, tablets, and smartphones, the user must also consider access to data stored on the device and the networks available for connection.

XXXI. All employees who use IT assets (desktops, notebooks, telephones, mobile phones, projectors, servers, wireless networks, monitors, UPS devices, emails, virtual conference rooms (Teams®, Zoom®, Skype®, Google Meet®, etc.), intranet systems, and other technological tools) must be aware that their use must be responsible, ethical, and aligned with internal guidelines, ensuring the protection of information, the integrity of equipment, and compliance with applicable corporate policies.

I. Examples of unacceptable activities related to the use of systems and networks include:

a. Violations of the rights of any individual or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including but not limited to the installation or distribution of "pirated" products or other software products not properly licensed for company use;

b. Making unauthorized copies of copyrighted material, including but not limited to scanning and distributing photographs from magazines, books, or other copyrighted sources, copyrighted music, and installing any copyrighted software for which the company or end user does not have an active license;

c. Accessing data, servers, or accounts for any purpose other than conducting company business, even if authorized access exists;

d. Exporting software, technical information, and technologies in general;

e. Introducing malicious programs into the network or server (e.g., viruses, worms, trojans, phishing, email spam, etc.);

f. Disclosing account passwords to third parties or allowing third parties to use one's account, including family members when work is performed from home;

g. Using company-owned computing equipment to actively participate in the acquisition or transmission of material involving bullying, sexual harassment, violence, hate, racism, xenophobia, discrimination, pornography, or child

pornography;

h. Using company equipment and systems to make fraudulent offers of products, items, or services;

i. Making explicit or implicit statements about product or service warranties, except as part of normal job duties;

j. Engaging in security breaches or network communication disruptions (security breaches include, but are not limited to, accessing data for which the employee is not the intended recipient or logging into a server or account the employee is not expressly authorized to access, unless such activities fall within the scope of their regular duties);

k. Performing port scans or security/vulnerability scans without express company authorization;

l. Performing any form of network monitoring that intercepts data not intended for the employee's host, unless such activity is part of the employee's duties;

m. Circumventing user authentication or the security of any host, network, or account;

n. Introducing honeypots, honeynets, or similar technology into the company network;

o. Interfering with or denying service to any user other than the employee's host (e.g., denial-of-service attacks);

p. Using any program, script, or command, or sending messages of any kind, with the intent to interfere with or disable a user's terminal session, by any means, locally or via the Internet/Intranet;

q. Attempting to access or obtain personal data of employees, clients, suppliers, and business partners, unless such activity is part of the employee's duties or tasks.

II. If, through an internal investigation, misuse of Information Assets is proven, the User who acted with intent or negligence shall be held liable and may be penalized in accordance with the disciplinary measures established in the Company's Internal Regulations or with the penalties provided for in contract, as applicable.

5.3. Documents and Information Management Tools

5.3.1. Document Flow

XXXII. In order for documents from each area to be handled in accordance with best practices in document management, the information flow must be properly mapped, standardized, redesigned, and automated, whether carried out by the IT team in conjunction with a contracted specialized provider, if necessary.

XXXIII. II. The assessment of the document flow consists of identifying, analyzing, describing, and recording the document process in each area of Brazilian Nickel S/A, with the objective of standardizing how these processes operate and identifying actions for their continuous improvement.

XXXIV. III. The Information Technology Department shall be responsible for providing the necessary resources, as well as a qualified team, together with a contracted specialized provider, to map and redesign the document flow, considering the priorities defined by Brazilian Nickel S/A.

XXXV. IV. The parameterization, creation of workflows, and/or automation of document flows must be carried out with the agreement of the Information Technology Department, which will be responsible for approving the solution.

5.3.2. Corporate Taxonomy

XXXVI. The taxonomy aims to organize, categorize, and classify the information generated in each of the Group's processes. This taxonomy will be configured in information management technologies to store documents, with the purpose of facilitating their search and retrieval.

XXXVII. The taxonomy of each unit must be structured hierarchically, considering the company's processes, subprocesses, and activities, in order to ensure a systemic view of all information generated by the organization for the execution of its activities.

XXXVIII. The terms used to structure the taxonomy are classified from general to specific topics or from the whole to its parts, in order to facilitate logical navigation of subjects within the document.

XXXIX. The elements that make up the taxonomic structure should preferably be described in English format, adopting the following standard: ***yyyymmdd_BRN_Subject***.

XL. The Information Technology Department shall be responsible for providing the necessary resources, as well as a qualified team, together with a contracted specialized provider, for the development and updating of the taxonomy for each area, whenever necessary, in accordance with the priorities established by Brazilian Nickel S/A.

XLI. The areas must periodically assess the need to update the taxonomy and inform the Information Technology Department so that the necessary actions can be taken.

XLII. The Group's areas may suggest changes to the structure whenever deemed necessary, in order to ensure alignment between the taxonomy and the needs of information users.

5.3.3. Information Management Table

XLIII. Every department responsible for generating or receiving physical or digital documents necessary for the execution of Brazilian Nickel S/A's processes must have an Information Management Table prepared in accordance with the Document and Information Management methodology.

XLIV. The INFORMATION MANAGEMENT TABLE must contain, at a minimum, information on how each Brazilian Nickel S/A document is handled, its confidentiality classification, and how long it is retained.

XLV. The retention period, in addition to applicable laws and regulations, must consider the disposal of information that has already fulfilled its purpose, in accordance with Articles 15 and 16 of the LGPD, as well as other applicable laws and regulations in force, and any exceptions must be documented, justified, and approved.

XLVI. The INFORMATION MANAGEMENT TABLE of each unit/area must be approved by the manager of each unit in conjunction with the Group's Legal Department.

XLVII. The Information Technology Department shall be responsible for providing the necessary team for the development of the Information Management Table for each unit/area, considering the priorities defined by the Group.

5.3.4. Operational Standards

XLVIII. This consists of the description of how to perform a specific task, with the objective of regulating and standardizing the manner in which tasks are carried out.

XLIX. Document management procedures and the related work instructions describe the methodology for handling the document collection, detailing the activities required to classify, organize, name, index, file, and move physical and digital documents through their respective stages.

L. The Information Technology Department shall be responsible for providing the team to develop the procedures and work instructions necessary for the implementation of document management in each area/program, considering the priorities defined by Brazilian Nickel S/A.

LI. The Group's areas/programs may develop specific technical procedures, subject to approval by the Information Technology Department.

5.4. Information Processing Requirements

The specific operational requirements related to how the Group handles documents and information are defined below:

5.4.1. Information Classification

LII. It is the responsibility of managers, within their respective areas of activity, to specify who may access the documents and information under their responsibility.

LIII. The classification of all documents necessary for the execution of Brazilian Nickel S/A's processes must ALWAYS be recorded in the INFORMATION MANAGEMENT FRAMEWORK, in accordance with the confidentiality classification criteria.

LIV. **Classification of Confidential Information:**

a) The confidential classification is assigned to documents and information intended for specific individuals within Brazilian Nickel S/A. This classification is generally associated with documents whose information leakage may represent a financial or reputational risk to the Group.

LV. **Classification of Restricted Confidential Information:**

a) The restricted or confidential classification is assigned to documents and information necessary for the execution of Brazilian Nickel S/A's business processes, which are disseminated within the scope of each management area that produces them.

b) Restricted information may be made available only to internal groups within each management area or among specific management areas.

c) Documents containing personal data (based on the LGPD) must have restricted access, in accordance with the principles of the law.

LVI. **Classification of Corporate Information Confidentiality:**

a) The corporate classification is assigned to information that may be known by all employees of the Group, as it does not present potential risk. Corporate information may be made available within Brazilian Nickel S/A without confidentiality restrictions.

LVII. **Classification of Public Information:**

a) The public classification is assigned to Brazilian Nickel S/A information that does not present potential risk and whose disclosure to the external public adds value to the institution's image. Public information may be made available to the external audience, which is the target of the information, in accordance with the competencies established in Brazilian Nickel S/A's communication and disclosure policies.

LVIII. All systems used to store data and information at Brazilian Nickel S/A must be configured in accordance with the confidentiality classification criteria defined by the departments, in order to prevent unauthorized access.

LIX. Proper classification of documents within the taxonomy structure must be carried out for the recording and evidencing of process execution, to facilitate electronic storage and ensure the quick search and retrieval of documents and information.

5.4.2. Production, Receipt, and Circulation of Documents and Information

LX. Documents generated or received by departments or programs must be published at the time of their generation/receipt in the technologies provided by Brazilian Nickel S/A for Document and Information Management. Only approved tools and applications may be used to handle the data.

LXI. Technical documents must be received, identified, and coded in accordance with the relevant standards. When applicable, suppliers should be advised to use the Group's document templates or standard document identification.

LXII. Departments should use standardized document templates whenever possible for document production.

LXIII. The circulation of documents and information should, whenever possible, be carried out using technologies approved for this purpose. If documents are sent by email, confidentiality and secrecy criteria must be observed.

5.4.3. Document Registration

LXIV. To register documents in information management technologies, it is necessary to define indexing standards required to ensure the search and retrieval of documents, information, and content.

LXV. Indexing standards define how documentation is recorded in the technologies, according to the needs of each unit/department.

LXVI. It shall be the responsibility of the team designated by the Information Technology Department to define document indexing standards in conjunction with the departments.

5.4.4. Document Printing

LXVII. A document should only be printed if it requires a physical signature and it is not possible to use an electronic signature or digital certification, or in cases where the format makes electronic access or reading difficult. However, it is important to emphasize that even when a document is printed, it must still have restricted access, and everyone must work together to ensure that documents are not left "forgotten" on devices or desks.

LXVIII. Documents that do not legally require a seal or signature should preferably be processed electronically, avoiding excessive printing.

LXIX. Each employee is responsible for the proper custody, transport, and storage of the documents they print, ensuring compliance with the information classification and protection against unauthorized access.

LXX. Files sent for printing must be collected immediately from the printer tray, avoiding being forgotten or accessed improperly by third parties.

5.4.5. Organization of Documents and Information

LXXI. It shall be the responsibility of the departments that generate documentation to register and publish new documents in information management technologies.

LXXII. The existing legacy collection in digital format will be migrated to the technologies by the team provided by the Information Technology Department, taking into account the priorities defined by Brazilian Nickel S/A.

LXXIII. The Information Technology Department shall be responsible for providing the team to assist Brazilian Nickel S/A departments in the document organization process, whenever necessary.

5.4.6. Storage, Conservation, and Preservation

LXXIV. All Group information and documents that are relevant to the institution's activities, regardless of their classification, must be stored in technologies approved by the Information Technology Department and made available for document and information management, such as Microsoft SharePoint, Teams, and Outlook, in compliance with backup and retention rules.

LXXV. Documents from units/departments must be stored in the information management technologies provided by the Information Technology Department. The evaluation of which technology will be used to store documents will be defined by the Information Technology Department in conjunction with the departments that generate the documentation at the time of document flow analysis. All files that employees need to perform their duties may be stored in the cloud system adopted by the Group, provided they comply with the guidelines set forth in this policy.

LXXVI. It is the responsibility of all employees to "clean up" the storage space on company-provided equipment and ensure that files that do not belong to Brazilian Nickel S/A are removed.

LXXVII. The company's storage resources must be used by employees in the performance of their duties. All digital files must be saved and digitized using the SharePoint cloud system adopted by the Group. The storage and management of digital files will be automated using platforms approved by the IT Department.

LXXVIII. Information owned by the Group and stored on electronic and computing devices owned or leased by the company, its employees, or third parties shall remain the exclusive property of Brazilian Nickel S/A.

LXXIX. If such information is stored in other locations not previously approved by the Information Technology Department—such as a local computer disk, external hard drive, USB flash drive, email, among others—its integrity and confidentiality will not be guaranteed. In the event of loss, the Area Manager shall be responsible for any damage or loss caused to Brazilian Nickel S/A, in accordance with the institution's Information Security Policy. Sanctions will be applied in accordance with the law and the current employment contract if the cause is evident.

LXXX. Preferably, documents that are not accepted on other media, such as large-format technical documents for reference purposes and historical documents, should be stored on physical media. Other documents, if printed, must be discarded as soon as they are used.

LXXXI. Documents in physical format shall be stored in the department that generated the documentation until they are properly processed by the team provided by the Information Technology Department and forwarded for external storage, in accordance

with the flow agreed upon between the departments.

LXXXII. In the event of theft, loss, or unauthorized disclosure of information belonging to the Group, the employee who becomes aware of the incident must immediately notify their direct manager and the Information Technology Department.

5.4.7. Document Naming

LXXXIII. Electronic documents must be named in accordance with the company's specific Document Naming Operational Procedure, prior to their inclusion in information management technologies, considering the following example:

20240131-BRN-Meeting Minutes-0001.doc

- Date (YYYYMMDD)
- Company acronym
- Document type
- Subject
- Document number

LXXXIV. If the unit/department does not yet have this procedure defined, it must be requested from the Information Technology Department. The document naming standard must be developed with consideration for ease of use by users.

LXXXV. If there is a need to update the defined document naming standard, the department responsible for the documentation must request a review of the procedure from the Information Technology Department.

5.4.8. Document Consultation

LXXXVI. Documents should preferably be consulted through information management technologies, considering the access levels defined for each document, in order to minimize the risk of consulting previous or obsolete versions. When a document cannot be found in this environment, it must be requested from the team designated by the Information Technology Department, which will take the appropriate measures.

5.4.9. Document Disposal

LXXXVII. Documents must be disposed of in accordance with Brazilian Nickel S/A's internal standards and procedures. All information that is no longer necessary must be disposed of securely, taking into account the storage periods defined in the INFORMATION MANAGEMENT FRAMEWORK for each of the Group's areas/programs. Document retention periods must be considered in compliance with data protection legislation and other applicable regulations in force.

LXXXVIII. Documents may only be disposed of after approval by the manager of each unit/department responsible for the documentation, together with the Legal Department and the Executive Board of Brazilian Nickel S/A.

5.4.10. E-mail

LXXXIX. Any email containing official information, such as communications between Brazilian Nickel S/A and stakeholders; notifications, requests, or clarifications to regulatory bodies, agencies, municipalities, governments, among others; contracts with suppliers and partners, among others, must be stored in the technologies provided by the company.

XC. Any document attached to an email, whether sent or received, that constitutes a record or evidence of Brazilian Nickel S/A's processes must be included in the information management technologies. For the management of attachments, Users must use the platform approved by the IT Department.

XCI. It is the responsibility of the manager of each unit/department to ensure that all formal records received by email are stored in accordance with the standards established by the Data Security and Governance Policy.

XCII. Corporate email is a company asset and has the sole and exclusive purpose of carrying out professional activities in the interest of Brazilian Nickel S/A.

XCIII. The company may use security measures to protect the network and ensure the integrity of data and programs and may therefore inspect any file stored on the network, as well as monitor the internal use of information, browsing activities, and the sending and receiving of emails, in order to ensure compliance with this Policy.

XCIV. Employees must be cautious when opening email attachments and links received from unknown senders, as they may contain malware. In case of doubt, always contact the IT Department for guidance.

XCV. Examples of unacceptable activities related to the use of email and communication:

a) Sending messages using company email accounts without clearly stating that "comments, messages, and/or opinions do not necessarily represent the company's opinion and/or are not endorsed by the company";

b) Sending emails not related to work to internal or external recipients

c) Sending unsolicited email messages, including the distribution of "junk mail" or other advertising material to individuals who did not request it, specifically email spam;

d) Making unauthorized use of or falsifying email header information;

e) Requesting email responses to any address other than the author's own email account, with the intent to harass or collect information;

f) Creating or forwarding "chain letters" or "pyramid schemes" of any kind;

g) Providing company employee information or lists to third parties;

h) Providing third parties with personal data of employees, clients, suppliers, and business partners;

i) Sharing usernames and passwords, as well as the use of departmental email accounts by unauthorized users;

j) Accessing the emails of other Brazilian Nickel S/A users;

k) Reproducing and/or forwarding content containing electronic threats, such as viruses, spam, and other malware;

l) Accessing files with executable code (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) or any other extension that poses risks to the security of Brazilian Nickel S/A's Information Assets;

m) Sending messages intended to secretly monitor, harass, or threaten other Users, as well as to circumvent the security system or disrupt a specific service, system, server, or computer network through illicit or unauthorized means.

5.5. Security and Proprietary Information

XCVI. System-level and user-level passwords must comply with the established password policy. It is prohibited to grant access to another individual, whether deliberately or through failure to follow procedures designed to protect against unauthorized access.

XCVII. It is prohibited to use any company information for personal, educational, or private purposes, as well as to use or store personal data or data of other individuals that are not relevant to Brazilian Nickel S/A on company devices. Exceptionally, the use of such information exclusively for academic or educational purposes may be permitted, provided it is previously authorized by the area's management and the Legal/Governance team, and provided that there is no risk to confidentiality, information security, or the Company's trade secrets. In such cases, where applicable, information must be anonymized or aggregated in order to prevent the identification of personal data subjects.

XCVIII. Each employee must ensure, through legal or technical means, that proprietary information is protected in accordance with the data protection standards adopted by the company.

5.6. Contingency Actions

XCIX. All documents and information critical to the operation of Brazilian Nickel S/A or crucial to the proper functioning of its processes must be preserved. All contingency measures for the preservation of Brazilian Nickel S/A's vital records shall be executed in accordance with this policy.

5.7. Internet Use

C. Internet use at Brazilian Nickel S/A must be exclusively for legitimate purposes related to the performance of work duties.

CI. Download requests must be made directly to the support team and will be subject to evaluation by the IT team.

CII. Examples of generally unacceptable activities include:

a) Playing or participating in online or offline digital games;

b) Playing or participating in online digital gambling games;

c) Accessing offensive, illegal, pornographic, or inappropriate material;

d) Conducting personal business using company resources;

e) Transmitting any content that is offensive or fraudulent;

f) Accessing information that the employee is not authorized to access or does not need to perform their job;

g) Accessing or sharing pirated software or material;

h) Attempting to disrupt or hack other systems (internally or externally) or to produce malicious outcomes, such as damaging systems, stealing or removing data, or deploying viruses;

i) Selling or providing third parties with personal data of employees, clients, suppliers, and business partners;

j) Attempting to bypass internet controls using software, plug-ins, or other methods, as well as using programs for downloading/uploading suspicious files;

k) Using the internet to access chat rooms, social networks, download/upload movies and music, spam, and other types of access not related to daily work activities.

5.8. Use of the Corporate Network

CIII. All mobile and computing devices that connect to the internal network must comply with the information security standards implemented by the company.

5.9. Use of Removable Media

CIV. Removable media are devices that allow the reading and writing of data, such as CDs, DVDs, Blu-Ray discs, floppy disks, USB flash drives, memory cards, portable hard drives, mobile phones, among others.

CV. To minimize the risks of security incidents involving company-held information and to reduce the risk of malware proliferation on the computer network, the use of removable media is prohibited without the consent of the IT team.

CVI. Even on authorized equipment, data traffic between USB devices and computers must be monitored through reports provided by the management system, internal and external audits when applicable, and validations performed by the IT team.

5.10. Clean Desk and Clean Screen

CVII. All information used in physical form must be kept under access control and should only remain at workstations during the performance of the activity.

CVIII. After the end of the workday or when leaving the workstation, information must be stored in a secure location.

CIX. It is prohibited to leave documents on desks, in printer trays, or in any unprotected location.

CX. When disposing of documents, they must not be recycled; they must be shredded, preferably using shredders.

CXI. It is prohibited to use drafts or notes that contain personal data or confidential information.

CXII. Workstations and notebooks must be configured with automatic screen locking, ensuring the protection of information when the user is away.

CXIII. If a notebook or desktop does not have screen lock configuration, the IT department must be contacted.

5.11. Use and Acquisition of Software, Systems, Applications, and Licensing

CXIV. Software, systems, applications, and usage licenses may only be contracted after being reviewed, validated, and approved by the IT team, as communicated through the Software Analysis and Approval Form, available on the IT Services Portal on the Brazilian Nickel S/A Intranet.

CXV. Before being used in the Brazilian Nickel S/A environment, all software, systems, applications, and usage licenses must undergo an approval process conducted by the Information Technology Department. The procedure includes:

a) **Formal request:** The User or interested department must submit a request for evaluation to the Information Technology Department, describing the purpose, scope of use, and types of data involved, through the Software Analysis and Approval Form available on the IT Services Portal on the Brazilian Nickel S/A Intranet.

b) **Technical and security analysis:** Verification of data protection requirements, use of authentication technologies (e.g., MFA, SSO), integration technologies (e.g., APIs), security mechanisms, server locations, access and version controls, incident risks, and backups.

c) **Legal and compliance assessment:** Review of terms of use, licenses, intellectual property clauses, applicable legal bases, and adherence to internal policies and current legislation (including data protection, with support from the DPO).

d) **Risk classification and definition of restrictions:** Identification of the solution's risk level and definition of conditions or limits for its use by the Information Technology Team.

e) **Formal approval:** Only after technical, legal, and compliance validation will the tool be considered approved and included in the list of authorized solutions published by Brazilian Nickel S/A.

f) **Registration and monitoring:** Approved tools must be registered and subject to periodic reviews to verify ongoing compliance, security, and suitability for corporate use.

5.12. Use of Artificial Intelligence

CXVI. For the use of AI with internal data, Brazilian Nickel S/A will prioritize solutions on secure, controlled platforms with contracts that ensure the Company's data will not be used to train the provider's AI model. Therefore, only platforms previously approved by the IT team may be used, as disclosed through the software analysis and approval form available on the Brazilian Nickel S/A Intranet (Corporate Financial Portal).

CXVII. The implementation and use of AI systems must comply with the applicable Artificial Intelligence Laws, as well as regulations and guidelines issued by competent authorities in each jurisdiction where Brazilian Nickel S/A operates.

CXVIII. AI may operate as an assistive tool or make decisions with different levels of autonomy, and its use must always adhere to the principles of ethics, security, legality, privacy, and legitimate purpose.

CXIX. Before being used within the Brazilian Nickel S/A environment, all Artificial Intelligence tools must undergo an approval process by the Information Technology Department, available through the Corporate Financial Portal on the Intranet. The procedure includes:

a) **Formal request:** The User or the interested area must submit a request for tool evaluation to the Information Technology Department, describing its purpose, scope of use, and types of data involved, through the Software Analysis and Approval Form available on the IT Services Portal on the Brazilian Nickel S/A Intranet.

b) **Technical and security analysis:** Verification of data protection requirements, with support from the Data Protection Officer or equivalent role, as designated under applicable Data Protection Laws, if necessary, including security mechanisms, server location, access controls, and incident risks.

c) **Legal and compliance assessment:** Review of terms of use, licenses, intellectual property clauses, applicable legal bases, and adherence to internal policies and current legislation (including data protection, with support from the Data Protection Officer or equivalent role, as required or designated under applicable Data Protection Laws).

d) **Risk classification and definition of restrictions:** Identification of the tool's risk level, assessment of potential

adverse impacts, and definition of conditions or limitations for its use by the Information **Technology Team, in accordance with applicable Artificial Intelligence Laws.**

e) **Formal approval:** Only after technical, legal, and compliance validation will the tool be considered approved and must be included in the list of authorized solutions published by Brazilian Nickel S/A. The decision made by the Information Technology Team must be formally documented.

f) **Registration and monitoring:** Approved tools must be registered and subject to periodic reviews to ensure continued compliance, security, and suitability for corporate use.

CXX. For the evaluation of the proposed risk, the following factors must be considered:

Risk Level	Descrition	Examples	Implication for Brazilian Nickel
Unacceptable Risk	Systems that cause harm or violate fundamental rights.	Subliminal manipulation systems, mandatory social scoring systems.	Use or contracting is prohibited.
High Risk	AI that directly impacts fundamental rights, safety, health, employment, or legal processes.	Automated recruitment systems, facial recognition in security, AI in critical healthcare, credit scoring.	Requires rigorous assessment, transparency, risk mitigation, and auditing.
Risk Limited	AI with moderate impact, but without direct risk to critical rights.	Chatbots, virtual assistants, content recommendation systems, spam filters.	Requires transparency, clear disclosure to users, usage monitoring, and basic protection.
Minimal or Nulo Risk	AI that does not present significant impact on safety or rights.	Internal tools, simple automation systems.	May be used freely, without specific regulatory requirements.

CXXI. For Artificial Intelligence systems classified as High Risk (as per Item CXIV) and that fall within the high-risk categories of the European Union Artificial Intelligence Regulation (EU AI Act), the Company shall observe additional requirements, including, but not limited to:

a) **Quality Management System:** Implementation and maintenance of a quality management system, ensuring compliance throughout the entire lifecycle of the AI system.

b) **Conformity Assessment:** Conducting a conformity assessment before placing the system on the market or putting it into service, demonstrating adherence to the requirements of the EU AI Act.

c) **Technical Documentation and Record Keeping:** Preparation and maintenance of technical documentation and records (logs) generated during the operation of the AI system, in order to ensure traceability.

d) **Human Oversight:** Implementation of measures to ensure meaningful human oversight, allowing individuals to monitor, evaluate, and intervene in the operation of the AI system, as appropriate.

e) **Cybersecurity:** Adoption of technical and organizational measures to ensure that high-risk AI systems are accurate and secure, aiming to minimize errors and vulnerabilities.

f) **Transparency and Provision of Information:** Provision of clear, complete, and understandable information to users regarding the capabilities, limitations, and purpose of AI systems, in accordance with the transparency requirements of the EU AI Act.

CXXII. The Company will monitor legislative developments and guidance from competent authorities regarding the EU AI Act to ensure the continuous alignment of its policies and practices.

CXXIII. Before using AI tools, Users must assess the benefits and risks associated with each use. Among the risks, the following stand out

a) **Hallucinations, discrimination, and biases in Generative AI:** AI models may generate incorrect, inaccurate, or biased information, including unequal or discriminatory treatment of individuals or groups, as well as impacting the quality of decisions and creating reputational or operational risks.

b) **Copyright and intellectual property:** Content generated or used by AI may violate third-party rights, especially when based on protected materials or when ownership and usage permissions are unclear.

c) **Security incidents involving personal and corporate data:** Improper use of AI may result in unauthorized exposure, leakage, or improper processing of sensitive information, violating internal policies and data protection laws. Public generative AI tools (e.g., chatbots, code generators, summarization tools) may use submitted information for continuous model training, turning confidential Company data into part of the tool's public knowledge, which is strictly prohibited without authorization and guarantees that the data will not be used for training, as established in item CX. The use of such tools must consider the legal basis for processing and international data transfer mechanisms, when applicable.

d) **Outdated or inaccurate information:** Models may rely on outdated datasets, leading to incorrect conclusions in a corporate context.

e) **Lack of traceability and transparency:** Some tools do not allow full understanding of how responses are generated, making auditing, source verification, and accountability more difficult.

f) **Overreliance on technology:** Excessive trust in AI may reduce human oversight, compromise the quality of analyses, and lead to inappropriate automated decisions.

CXXIV. During the use of AI tools, the following principles must be observed by Users:

a) **Legality and compliance:** The use of AI tools must always comply with applicable laws, including data protection regulations, copyright, intellectual property, and other relevant regulations.

b) **Transparency:** Users must indicate when content has been generated with the support of AI, whenever relevant, and ensure clarity regarding the limitations, sources, and assumptions used.

c) **Human oversight:** AI must act as a support tool and not replace human judgment. Users remain responsible for decisions made based on the results provided by the technology.

d) **Security and Privacy:** It is prohibited to input sensitive personal or corporate data into non-approved tools. The use of AI must preserve the confidentiality, integrity, and availability of information.

e) **Quality and Accuracy:** Generated content must be reviewed, validated, and adjusted by the User, considering possible errors, biases, or inaccuracies inherent to AI models.

f) **Proportionality:** AI must be used only when necessary, appropriate to the intended purpose, and aligned with the legitimate interests of the organization.

g) **Minimization:** Only the data strictly necessary for the purpose of processing should be used, preferably anonymized or pseudonymized.

CXXV. All content generated by AI based on the Company's data or instructions belongs to the Company. It is the employee's responsibility to ensure that AI-generated output does not violate third-party copyright, especially if it is intended for external or commercial use. When AI-generated results are used externally, the Company must consider the need for proper and transparent attribution (e.g., "this document was generated with the assistance of AI").

CXXVI. It is strictly prohibited to:

a) insert, copy, or submit data classified as Confidential, Trade Secret, Strategic, or Personal Data of Clients/Employees into public Artificial Intelligence platforms (ChatGPT, Copilot, Gemini, Claude, Bard, DeepSeek, etc.) without formal authorization;

b) use AI tools that are not licensed or approved by the Company, as well as bypass security mechanisms, privacy

policies, usage restrictions, or limitations defined in the approval process;

c) use AI for illegal, unethical purposes or in violation of internal policies, including fraud, manipulation, discrimination, or infringement of third-party rights;

d) use AI-generated content as if it were verified results, without proper human review;

e) assign automated decision-making to AI without supervision, especially in situations that may impact individuals, clients, partners, or critical processes;

f) use AI to create misleading content, such as deepfakes, false information, or communications that may mislead third parties.

5.13. Backup

CXXVII. All procedures related to Backup and recovery of data stored on BRN servers must comply with the provisions of this Policy.

CXXVIII. Backup procedures must be updated whenever there are:

a) New applications developed;

b) New data or file storage locations;

c) New database installations;

d) New applications installed;

e) Other information requiring protection through Backup.

CXXIX. Backup copies must include files, digital systems, virtual machines, and databases stored or hosted in BRN data centers.

CXXX. For mobile devices, employees must use software approved by BRN to perform Backup.

CXXXI. Employees are recommended to keep their files in the cloud, avoiding storage in local directories or on mobile device desktops.

CXXXII. Backup copies must be tested regularly to ensure usability in case of recovery.

CXXXIII. The procedure must define appropriate technical and operational requirements for the creation, restoration, and validation testing of Backups.

CXXXIV. Backup tools must be maintained and updated in accordance with the vendor's recommendations and with valid licenses, aligned with the contract established for this purpose.

5.14. Intellectual Property

CXXXV. All Users have the duty to perform their functions ethically, committed to the integrity and confidentiality required for the matters handled at Brazilian Nickel S/A, as well as to protect the organization's intellectual property assets, including trademarks, source codes, models, methods, documents, research, know-how, and other strategic information.

CXXXVI. It is prohibited to use, reproduce, adapt, or distribute materials protected by copyright, patents, trade secrets, or licenses without proper formal authorization or without complying with the conditions established by the rights holders.

CXXXVII. All content, documentation, software, analysis, reports, or solutions developed in the course of professional activities, using corporate resources or company information, are considered the intellectual property of the organization, unless otherwise provided by contract.

CXXXVIII. The installation or use of software, libraries, cloud services, or third-party tools must occur exclusively under valid licenses and in compliance with applicable contractual terms, and any form of misuse or unlicensed use is prohibited.

CXXXIX. Users must always act in defense of BRN's interests and maintain confidentiality regarding business matters, operations, personal data, and other confidential information.

CXL. It is prohibited to use, disclose, photograph, scan, and/or record information owned by BRN for personal or third-party benefit,

even after the termination of the relationship with BRN.

CXLI. It is prohibited to create copies or backups, by any means, of documents and information provided to Users or that became known to them due to their relationship with BRN, regardless of the information classification.

CXLII. It is prohibited to use BRN systems to upload, reproduce, or distribute music, videos, data, or other content not licensed by BRN.

CXLIII. All documents and information contained in BRN systems and network are confidential and may not be disclosed to third parties or used for any purpose other than that determined by BRN, including after the end of the relationship with the organization.

Upon termination of the relationship with SCMP, the User must return all Information Assets or prove that they have securely destroyed the information to which they had access, with proper authorization.

5.15. Risk and Incident Management

CXLIV. Risks and incidents involving information security matters must be continuously monitored, in accordance with the Incident Management Policy and the best technical standards available on the market. All incidents involving Information Assets must serve as a basis for the implementation of new methodologies and/or controls.

CXLV. Within the Company, in order to mitigate information security risks, antivirus software is used on all machines, and firewall solutions are implemented.

CXLVI. Users are also an important part of information security risk management. If an employee notices anything unusual happening with their computer, this may be a sign of a hacker intrusion; in such cases, the IT department must be notified as soon as possible to prevent a potential cyberattack from succeeding. In addition, the following prohibited actions must be observed:

a) Installing software that has not been properly reviewed or authorized by the IT department;

b) Disabling and/or delaying updates of the antivirus program installed on equipment; Users must regularly check files downloaded from the Internet as well as those contained in any type of backup using antivirus software;

c) Performing computer maintenance without the supervision of the IT department;

d) Changing computer settings without prior authorization and proper supervision by the IT department.

CXLVII. If it is necessary to perform any type of maintenance on your computer, contact the IT team via email at suporte.ti@brnickel.com and/or itsupport@brnickel.com, as applicable.

5.16. Devices and Technical Criteria

CXLVIII. All devices **(desktops, laptops, and mobile devices)** must comply with the technical standards approved by the IT Department, meeting minimum performance and security requirements.

5.16.1. General Guidelines for Desktops and Laptops:

CXLIX. Only equipment with TPM 2.0, compatibility with Windows 11 Pro/Enterprise, a minimum of 16 GB of memory (32 GB recommended), a minimum 512 GB NVMe SSD, i7/i9 CPU or Ryzen Pro, and active corporate antivirus software will be accepted.

a) Only dedicated Nvidia GPUs may be used.

b) Single-channel memory configurations are not permitted.

c) Where applicable, all wireless hardware must be manufactured by Intel.

d) All display devices must have a minimum resolution of 1920 × 1080, a 16:9 aspect ratio, and full high definition.

e) All touchscreen displays may optionally include the Dell Premium Active Pen (PN579X).

f) All laptops must have an infrared camera certified by Windows Hello for Business.

CL. The following Dell hardware models are strictly prohibited for use at Brazilian Nickel S/A:

- Dell Inspiron.
- Dell G-Series.
- Dell Alienware.

CLI. The following Android hardware brands are strictly prohibited for use at Brazilian Nickel S/A:

- Huawei ®
- Positivo ®

CLII. Only 24" / 32" 4K monitors, Thunderbolt 4 docks, and Teams-certified headsets are permitted.

CLIII. Personal devices used for home office must be managed under MDM (Mobile Device Management) / Intune.

CLIV. The specifications established in this regulation are minimum required specifications. They do not prevent the selection or acquisition of machines with higher specifications (e.g., memory, storage, etc.), when required by the role, based on technical and/or commercial justification at the time of acquisition.

CLV. Brazilian Nickel S/A requires the original equipment manufacturer (OEM) to be Tier 1 and approved by the Information Technology Department.

CLVI. The OEM must supply all hardware. This not only ensures continuity across countries, but also a consistent hardware flow with associated support available in all areas where the Group operates. This standard may be used to determine the acquisition of desktops, laptops, and complementary devices in the operational technology (OT) environment.

CLVII. Currently, the following global suppliers are contracted and approved as Tier 1 OEMs:

- Dell para monitores, desktop e laptop;
- Lenovo para laptops.

CLVIII. Currently, the following suppliers are not contracted but are permitted:

- Apple para hardware complementar.
- Microsoft para hardware alternativo de laptop;

CLIX. Hardware that is available for use subject to justification and approval by line management is not mandatory nor a substitute for a desktop/laptop. Desktops/laptops will continue to be the primary devices for all employees.

CLX. All new Dell Precision series devices will come factory-equipped with a GPU.

5.16.2. Equipment Configuration Criteria by Job Profile

CLXI. Define minimum technical criteria and configuration recommendations for the acquisition, replacement, and maintenance of corporate desktops/laptops, according to the usage profile and level of responsibility of employees, ensuring performance, security, and technological standardization.

5.16.3.Standardized Brands

CLXII. Equipment should preferably be from brands that offer corporate support, on-site warranty, and compatibility with the Company's security and MDM policies: Dell (Latitude, Precision, XPS lines), Lenovo (X1, X9, ThinkPad lines), Microsoft (Surface Pro, Surface Laptop lines), and Apple (MacBook Air or MacBook Pro lines, as required).

5.16.4. Base Minimum Configuration (All Profiles)

Item	Minimum Specification
Processor (CPU)	Intel Core i5 (12th generation or higher) or equivalent AMD Ryzen 7
RAM	16 GB DDR4 or DDR5
Storage	512 GB NVMe SSD
Display	14" Full HD (minimum) – anti-glare
Connectivity	Wi-Fi 6 or higher, Bluetooth 5.x
Ports	USB-A, USB-C, HDMI
Operating System	Windows 11 Pro
Security	TPM 2.0, BitLocker, Intune MDM support

5.16.5.Criteria by Job Profile

Position / Profile	Equipment Type	Recommended Configuration *	Notes
Group 01 (Apprentice, Clerks, and Assistants)	Intermediate corporate desktop/notebook	i5 CPU | Ryzen 7 | 16 GB RAM | 512 GB SSD	Standard equipment for administrative and operational tasks.
Group 02 (Analysts and Technicians)	Intermediate corporate notebook	i7 CPU | Ryzen 7 Pro | 16/32 GB RAM | 512 GB SSD	Standard equipment for administrative and operational tasks.
Group 03 Specialist	High-performance notebook	i7 CPU | Ryzen 7 Pro | 32/64 GB RAM | 1 TB SSD	Recommended for intensive technical activities (Data, BI, Development, Engineering).
Group 04 Supervisor	Premium corporate notebook	i7 CPU | Ryzen 7 Pro | 16 GB RAM | 512 GB SSD	Balanced performance and good portability.
Group 05 Coordinator	Premium ultra-thin notebook	i7 CPU | Ryzen 7 Pro | 16 GB RAM | 512 GB SSD	Preference for lightweight models with long battery life.
Group 06 Manager	Executive notebook	i7 CPU | Ryzen 7 Pro | 32 GB RAM | 1 TB SSD	Prioritize performance and connectivity. Possible Surface option.
Group 07 General Manager / Director	Executive ultrabook	i7 CPU | Ryzen 9 Pro | 32 GB RAM | 1 TB SSD	Premium equipment with performance and corporate design.
Group 08 C-Levels (CEO, CFO, COO, CPO, etc.)	Executive ultrabook	i7 CPU | Ryzen 9 Pro | 32 GB RAM | 1 TB SSD or higher	Equipment with the highest reliability, performance, and aesthetics.

*** Requests that require the use of a dedicated graphics card must be submitted for prior evaluation by the Information Technology Department and will be analyzed on a case-by-case basis, based on technical, operational, and cost criteria. The provision of this resource will be subject to formal approval by IT, after validation of the actual necessity for the user's job performance.**

5.16.6. Renewal Cycle and Asset Management

Equipment Type	Renewal Cycle	Notes
Desktops	5 years	Early replacement in case of obsolescence or critical failure.
Corporate notebooks	4 years	Early replacement in case of obsolescence or critical failure.
Executive / premium ultrabooks	3 years	Subject to updates according to technological evolution.
Mobile devices	3 years	Technical capacity reassessment at each cycle.
High-performance equipment (data, engineering, IT)	3 years	Technical capacity reassessment at each cycle.

CLXIII. In the event of a change in position, the equipment may be replaced according to the new group to which the user will belong and in compliance with the criteria set forth in item 5.17.5.

5.16.7. Minimum Specifications Defined for Complementary Mobile Hardware Devices

CLXIV. To increase end-user productivity and enable work on the move, the use of complementary mobile devices such as tablets and smartphones is recommended.

CLXV. All complementary devices are subject to mobile device management. Therefore, mobile equipment must be evaluated and approved by the Information Technology and Facilities departments.

CLXVI. Complementary devices are optional and depend on the employee's role and job function justification.

CLXVII. Complementary devices do not replace desktops or laptops and are not mandatory. Likewise, complementary devices do not necessarily determine the robust devices used in operational environments.

CLXVIII. The table below presents the MINIMUM SPECIFICATIONS DEFINED FOR COMPLEMENTARY MOBILE HARDWARE DEVICES. These definitions aim to protect the environment from devices that do not meet the requirements for running Brazilian Nickel S/A software. This specification indicates the minimum requirements for a new complementary mobile device in the production environment.

Profile	Device	Generation	Storage Capacity	Memory Storage	Screen Size
Light	Apple iPad Air	5th Generation	256 GB	8 GB* / 256 GB	10.9" / 1.0"
Standard	Apple iPad Pro 11"	5th Generation	256 GB	8 GB* / 256 GB	11.0"
Advanced	Apple iPad Pro 12.9"	5th Generation	256 GB	8 GB* / 256 GB	12.9" / 12.4"

CLXIX. Both Apple iPad and Surface Pro hardware are available in two configurations:

- Wi-Fi;
- Wi-Fi + cell phone.

CLXX. For Wi-Fi–only models, users may connect the tablet to their mobile phones to obtain Internet connectivity.

CLXXI. All Apple devices must be purchased with an Apple Pencil (2nd Generation).

CLXXII. All Microsoft devices must be purchased with a Surface Pro Pen.

CLXXIII. All Android devices, even if Samsung is the preferred manufacturer among users, must meet the minimum requirement of being produced by a Tier 1 OEM. The device must also be capable of running the Google Play Store.

CLXXIV. Devices manufactured by HUAWEI and POSITIVO are strictly prohibited, even if they meet the other guidelines established in this regulation.

CLXXV. The specifications established in this regulation for complementary devices are minimum required specifications. These specifications do not prevent the selection or acquisition of devices with higher specifications, when required by the role, based on technical and/or commercial justification at the time of acquisition.

5.16.8. Guidelines for the Selection of Desktops, Laptops, and Peripherals

CLXXVI. The table below presents optional devices and accessories recommended by the Information Technology Department. The table lists these devices according to the Tier 1 OEM manufacturer.

Tier 1 OEM Manufacturer	Device	Model	Specifications
DELL	Docking Station	Dell WD19DCS	Dual USB-C dock
DELL	Monitors	Dell P2422H	1080p resolution (1920 × 1080)
DELL	Monitors	Dell P2723QE	2160p / 4K resolution (3840 × 2160)
MICROSOFT	Tablet Dock	Microsoft Surface Dock 2	–
MICROSOFT	Tablet Pen	Surface Slim Pen 2	–
MICROSOFT	Tablet Keyboard	Surface Pro Keyboard	–
APPLE	Smart Pen	Apple Pencil	2nd generation
APPLE	Keyboard	Apple Magic Keyboard®	–
APPLE	Keyboard	Apple Smart Keyboard Folio®	–

CLXXVII. For DELL docking stations, it must be observed that USB and USB Type-C docking stations are compatible with DisplayPort over USB and Thunderbolt 3. This allows computers to be docked to keyboards, mice, displays, and other external functions. Any computer with the required hardware will work with a USB or USB Type-C docking station. There are requirements for docking stations to be compatible with or recommended for use with specific computers.

CLXXVIII. The specifications for desktops and laptops consider an individual user or user profile. Usage profiles are created based on how users typically use a machine. Typical usage can be classified into the following three categories:

a) **Basic Profile:** Single-task worker;

b) **Intermediate Profile:** Multitasking worker;

c) **Advanced Profile:** Critical-task worker.

CLXXIX. Based on the worker category, specifications and CPU classes (OptiPlex, OptiPlex Workstation, Latitude, and Precision laptops) are designed to meet the criteria of these categories. Specifications within these categories were selected to minimize overlap whenever possible, with an acceptable level of overlap being unavoidable to allow for a variety of models selected based on user profiles.

CLXXX. Single-task workers do not necessarily imply low-level task workers. Some individual tasks are critical to the business and must be addressed accordingly, increasing the specification, for example, from Ultra-Low or Low to Standard.

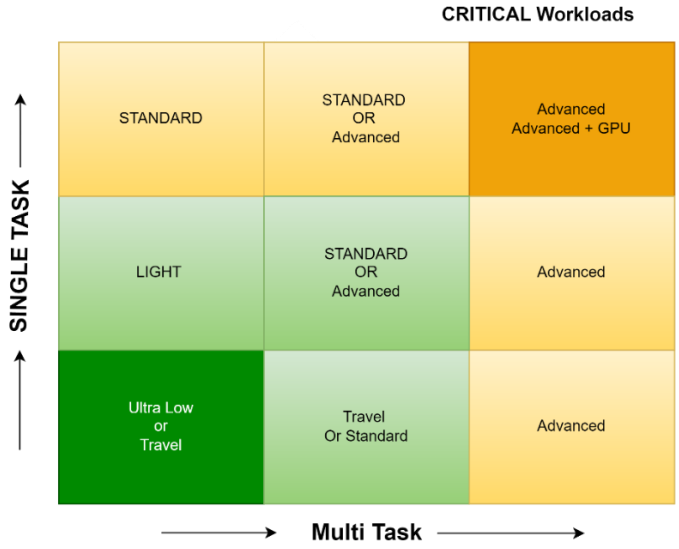

Figure 1 – Desktop / Laptop Selection

5.16.9. Guidelines for the Selection of Mobile Devices

CLXXXI. The specifications of complementary devices are considered based on a user or user profile. Usage profiles are created based on how users typically combine a complementary device in their daily professional lives. Typical use can be classified into the following three categories:

a) Promotion of mobility;

b) Promotion of productivity;

c) Highly mobile and productive.

CLXXXII. Based on the task category, using a laptop together with a complementary device provides the best experience. Productivity will always favor next-generation laptop or desktop hardware, as performance—rather than convenience—is believed to enhance productivity; however, combining productivity and mobility with a complementary device can enhance the experience of individuals who move in and out of the office. Mobility does not necessarily imply travel.

CLXXXIII. The specifications in these categories were chosen to ensure minimal overlap whenever possible, with an acceptable level of overlap being unavoidable to allow for a variety of configurations selected based on user profiles.

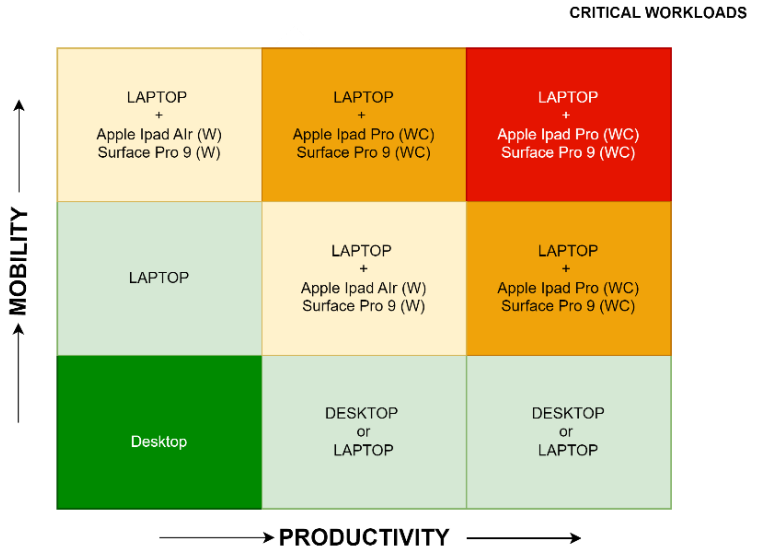

Figure 2 – Complementary Device Selection

WC: Wi-Fi + cell phone

W: Wi-Fi only (connected to a mobile phone when necessary)

5.16.10. Hardware Lifecycle

CLXXXIV. Existing hardware models must be gradually phased out in accordance with the hardware lifecycle standard.

CLXXXV. Guidelines for the replacement and disposal of hardware in general must follow a specific procedure developed for this purpose. When replacement or disposal is required, the end user must observe these guidelines and carry out the specific procedure under the direct guidance of the Information Technology Department.

5.16.11. Sustainability and Disposal

CLXXXVI. Replaced equipment must follow a certified reverse logistics policy (ESG).

CLXXXVII. There may be the possibility of corporate donation or buyback, subject to technical evaluation and in accordance with Brazilian Nickel S/A's internal policies.

6. REVISION CONTROL

Revision	Date	Reason for the revision
Rev. 01	31/03/2026	- Initial Edition

7. EMPLOYEES

Name	Area
Eduardo Almeida	Information Technology

****