Dear Partner,

Information is an asset of great value to Gerdau and we must all take care over it, protecting it in a way that guarantees its confidentiality and integrity, according to Gerdau's Code of Ethics for Third Parties.

Technology enables us to obtain, store, process and retrieve vast amounts of data, essential to the Company's administrative and productive flows. Care with this data, its protection and proper use, is not only an integral part of the business, but also part of the construction of Gerdau's history.

The involvement and conscious adherence of each of our third parties is fundamental to consolidate the collective behavior, more attentive and secure, regarding the treatment of Gerdau's information.

We count on your participation and commitment regarding the guidelines below.

1. DEFINITIONS

1.1. INFORMATION: It is the result of the organization of the data, regardless of its presentation or storage. All information is considered an asset for Gerdau, that is, it is part of its equity.

1.2. USER: anyone who has permission to access Gerdau information, regardless of the way of access.

2. GUIDELINES

2.1. Information Protection

2.1.1 All information produced, individually or jointly, by third parties in the service of Gerdau, originated or derived from its work activities are considered property of Gerdau, also applying to any information provided or licensed to Gerdau.

2.1.2 Every third party should have access only to the information and resources that are necessary for the execution of their work.

2.1.3 Every third party shall ensure and protect non-public Gerdau information which it has access to. Such information may not be disclosed without the prior consent of Gerdau. Copies of this information may not be made for personal or third-party use.

2.2. Physical Access

2.2.1 The Gerdau's Corporate Security area have responsibility to establish the physical barriers necessary to control access and protect Company information. The third party must respect the physical accesses allowed within Gerdau.

2.2.2 It is prohibited to film or photograph Gerdau's internal areas without prior formal authorization.

2.3 Logical Access

2.3.1 Logical access to the Gerdau internal network environment will be evaluated and approved according to the need, following the Corporate Information Security Guidelines(CG-15).

2.3.2 Third-party computers should not be connected without prior approval from Gerdau IT and computers that will be connected to the network must be protected by anti-virus / anti-malware software and other properly licensed software.

2.3.3 The access, downloading or distribution of any content that infringes copyrights and property within the Gerdau network is prohibited. Likewise, it is not allowed access or distribution of pornographic content of any nature or content that violates the Statute of the Child and Adolescent.

2.3.4 Remote access to the internal Gerdau environment when necessary shall occur via VPN (Virtual Private Network) using encrypted tunnels to keep information in transit secure.

2.3.5 Gerdau provides to the third parties a VPN Lan-to-Lan, or Site-to-Site VPN access to facilitate remote work. It is the third party's responsibility to have the necessary infrastructure to connect to Gerdau using this available platform.

2.3.6 Where applicable, the user and password made available to the third party are for exclusive use and may not be disclosed or shared.

2.3.7 The third party must keep his access credentials secure and any misuse of these credentials is his responsibility

2.3.8 It is the responsibility of the third company to communicate to Gerdau any termination of third parties in order to have their accesses properly canceled in the Gerdau environment.

2.4 Computer and Device Security

2.4.1 Each user is responsible for the protection of the physical devices containing Gerdau information that is in his or her custody.

2.4.2 Each user must be aware that the use of any IT resource in the Gerdau environment, even if personally owned, is subject to inspection, whenever permitted by local law.

2.5 Information Security Incident Management

2.5.1 Incidents and non-conformities of Information Security that are known to the third party must be immediately reported to a Gerdau manager, and the Ethics Channel may be used (https://www.gerdau.com/br/pt/quem-somos/codigo-de-etica).

2.6 Compliance

2.6.1 The administration, exploitation, transmission or any other use of Gerdau's proprietary information shall comply with the legal, regulatory and statutory provisions applicable to each of Gerdau's Business Operations

Sincerely,