SIMPLIFIED CONTRACTING TERMS AND CONDITIONS

These Simplified Contracting Terms and Conditions ("SCTC") apply to the services and goods provided to Suzano S.A. (or any company within its economic group) ("Suzano") and shall govern all contracts referring to them. The applicability of these SCTC does not depend on the signature or initials of this document by the Supplier (as identified in the Purchase Order or Supply Agreement) or by Suzano and shall apply automatically to all engagements entered by Suzano with suppliers of services or goods. The application of SCTC shall expressly exclude the applicability and/or effectiveness of any other understandings, agreements or contractual terms proposed by the Supplier and shall prevail over all other instruments or arrangements, regardless of their nature, for all legal purposes.

SCOPE

1.1. These SCTC aim to regulate the conditions under which the provision of services and/or the supply of goods described in the Purchase Order or Supply Agreement issued by Suzano ("Purchase Order") shall take place.

1.2. The activities and/or deliverables must be carried out at the units or locations established in the Purchase Order ("Execution Site"), and shall comply with all applicable norms and technical standards.

1.3. The Parties agree that the Supplier shall observe and comply with all guidelines issued by Suzano regarding access to and permanence at the Execution Site.

1.4. The Supplier may subcontract portions of the contractual object only with prior written approval by Suzano, and the Supplier shall remain fully liable for the subcontractor and its employees and/or agents. All references to the Supplier herein shall include any subcontractors.

1.5. Where applicable to the contractual scope, the Supplier warrants and declares, under penalty of law, that the seedlings provided under these SCTC are of public domain. The supply of any variety protected under Federal Law No. 9.456 of April 25, 1997, is strictly prohibited. Breach of this provision shall result in immediate termination of this Agreement and the Supplier shall be liable for all consequences related to the use of protected varieties.

1.6. Where applicable to the contractual scope, any changes to the legal or regulatory parameters applicable to the inputs acquired under these SCTC and/or any modification to the composition of the products supplied—whether or not such change affects the technical specification—must be notified to Suzano at least fifteen (15) days in advance, under penalty of breach of contract.

1.7. The following documents form an integral and inseparable part of these SCTC, and in case of conflict, the provisions of this instrument shall prevail over the annexes, which shall follow the order of precedence below:

Annex I – Key Approach Program;
Annex II – List of Documents for Document Management;
Annex III – Sustainability/ESG Principles;

Annex IV – Information Security.

TERM

2.1. This agreement shall be valid from the date of acceptance of the Purchase Order until full performance of the obligations undertaken by the Parties.

PRICE AND PAYMENT TERMS

3.1. The total price to be paid by Suzano to the Supplier is set forth in the respective Purchase Order(s) ("Price").

3.1.1. The Price adjustment may occur, if applicable, as previously agreed between the Parties, provided that the minimum periodicity of 12 (twelve) months from the date of acceptance of the Purchase Order is respected.

3.2. The Parties declare, irrevocably and irreversibly, that the Price already includes (i) all taxes levied on the services and/or goods supplied, (ii) all costs related to labor and equipment used by the Supplier, as well as any exchange rate variations related to this agreement, and (iii) all expenses with travel, accommodation, meals, insurance, and any others required for the labor involved in the provision of services and/or supply of goods, unless previously and expressly approved in writing by Suzano.

3.3. The Price shall be invoiced and paid as described in the Purchase Order, subject, where applicable, to fulfillment of payment events and agreed measurements. Payment shall be made by bank deposit, with the receipt serving as proof of payment. Price due dates shall fall on the 1st, 10th, or 20th of each month (or the next business day if a holiday or weekend) ("Suzano Payment Date"), provided that billing documents issued by the Supplier have been received by Suzano at least seven (7) business days in advance. Delay in delivery of billing documents shall result in postponement of the payment to the next Suzano Payment Date, without any penalties or charges.

3.3.1 In the event of an unjustified delay in the payment of the Price, Suzano shall pay the Supplier the overdue and unpaid amount, updated by the minimum index applicable under the law, plus a late payment fine of 0.5% (zero point five percent) and default interest of 1% (one percent) per month, calculated on a pro rata die basis, all applied to the overdue amount.

3.4. Any invoices with discrepancies in price and/or taxes will be returned by Suzano, and any costs or charges arising from such return shall be borne by the Supplier.

3.5. Suzano shall make an advance payment to the Supplier, if and as provided for in the Purchase Order ("Advance Payment"), subject to the simultaneous fulfillment of the following conditions: (i) receipt of an advance payment guarantee for the same amount as the advance, which must be unconditional, irrevocable, independent, and payable on first demand, substantially in accordance with terms and conditions previously approved in writing by Suzano, and issued by the Supplier at least twenty (20) days before the advance payment date ("Advance Payment Guarantee"); (ii) the Supplier shall contract all required insurance policies and immediately provide Suzano with proof of coverage and copies of the relevant policies, as applicable; and (iii) receipt by Suzano of the respective invoices and/or corresponding documents issued by the Supplier to Suzano.

3.5.1. The Advance Payment Guarantee shall be issued by a first-tier financial institution previously approved in writing by Suzano (the "Guarantor") and shall comply with the following minimum requirements: (i) the Guarantor shall pay Suzano, upon Suzano's request, within a maximum of seven (7) days, without Suzano being required to prove the Supplier's default; (ii) the Advance Payment Guarantee shall be valid from the issuance date until full performance of the Supplier's obligations to Suzano, as confirmed by written discharge from Suzano; and (iii) the Advance Payment Guarantee shall be returned by Suzano to the Supplier no earlier than twenty-eight (28) days after Suzano confirms in writing that the advances have been fully offset, without prejudice of other requirements, terms and conditions to be requested by Suzano on a case by case basis.

3.5.2. The advance payment shall be offset by the delivery of goods and/or provision of services until the total value of the advances has been matched by corresponding deliveries or services.

3.5.3. The Advance Payment Guarantee shall remain valid and enforceable until the latest of the following events: (i) full offset of the corresponding advance payments through proper performance of the Purchase Order, duly approved and invoiced by Suzano; or (ii) delivery of all goods and/or provision of services duly accepted by Suzano.

3.5.4. If the Supplier fails to comply with any obligations set forth herein, or if the Purchase Order is terminated, with or without fault of the Supplier, Suzano shall have the right, at its sole discretion, to: (i) enforce the Advance Payment Guarantee(s); and/or (ii) withhold any Price payments or amounts otherwise due by Suzano to the Supplier until the full offset of the advances, without prejudice to the Supplier's obligation to fully reimburse Suzano for any outstanding balance of the advances if none of those alternatives fully compensate the advance payments.

3.5.5. Whenever necessary, and at least thirty (30) days prior to the expiration date of the Advance Payment Guarantee, the Supplier shall replace it with another guarantee under the same conditions.

WARRANTY

4.1. The Supplier shall be solely and exclusively responsible for the activities undertaken pursuant to this SCTC, assuming full and entire liability for their specifications and technical quality, and undertaking to perform its activities in accordance with the highest standards of technique available in the market.

4.2. The Supplier undertakes, immediately upon Suzano's request, to redo, rectify, and/or replace any and all services rendered and/or goods supplied that Suzano deems incorrect or inadequate. If the Supplier fails or refuses to carry out the required correction within the period established by Suzano, or displays any form of negligence or incompetence in the performance of such rectification or replacement, Suzano shall be entitled to: (i) deduct the corresponding amounts from the subsequent installment(s) of the Price; or (ii) carry out the necessary rectifications itself or through third parties, in which case the Supplier shall reimburse Suzano for all costs incurred.

OBLIGATIONS OF THE PARTIES

5.1. The Supplier undertakes to:

a) comply with all applicable legislation, including but not limited to civil, environmental, tax, labor, and social security laws, as well as all requirements and interpretations issued by public authorities, especially, if applicable, the provisions of Federal Law No. 9,456, of April 25, 1997, its regulations and/or any legislation that may replace it;

b) maintain all licenses and authorizations necessary for the performance of its activities and compliance with its obligations under the Purchase Order, especially environmental licenses, in force and effective, and to comply with all requirements and conditions set forth therein, including, if applicable, registration with the National Registry of Seeds and Seedlings (RENA SEM);

c) promote decent work, comply with applicable labor and occupational health and safety laws, and ensure compliance with all labor and social security obligations, including freedom of association, union freedom, and collective bargaining rights;

d) be aware of and comply with Suzano's Supplier Code of Conduct, Sustainable Procurement Policy, and Corporate Human Rights Policy, available at www.suzano.com.br, undertaking to observe and comply with them by itself and/or its affiliates, companies in its economic group, its representatives, employees, and suppliers, without restriction, insofar as applicable to its activities;

e) process and store any personal data to which it may have access in the course of performing the activities under the Purchase Order strictly in accordance with Federal Law No. 13,709/2018 ("LGPD"), always observing the principles of good faith, transparency, security, and other applicable legislation and principles;

f) Any and all information security incidents (or suspected incidents) that may impact the confidentiality, integrity, and availability of information and/or personal data, and/or the exercise of any rights related to the performance of the Purchase Order, must be immediately reported to the following email addresses: lgpd@suzano.com.br and csirt@suzano.com.br;

g) not infringe upon any intellectual property rights or other third-party rights in the performance of its activities or under this instrument;

h) ensure the origin of any minerals eventually used in its supply, taking into account the social and environmental aspects of the extraction and production process, and guarantee that they do not contain substances from conflict regions that directly or indirectly finance or benefit armed groups;

i) indemnify Suzano for any losses it may incur due to the breach of any obligation assumed by the Supplier;

j) strictly follow the rules of the Key Approach Program ("Key Approach Program");

k) allow Suzano, or any third party on its behalf, to inspect and supervise the

performance of the activities without this implying any liability on Suzano's part;

l) maintain, through itself, its representatives, and employees, full confidentiality and secrecy regarding all information exchanged, whether written or verbal;

m) comply with all instructions provided by Suzano for the entry and permanence of its employees, representatives, and/or subcontractors at the Execution Site, as well as the procedures for the monthly monitoring of the Supplier's compliance with labor and social security obligations, available at: http://www.ddestra.com.br/?q=procedure;

n) prioritize the hiring of local labor for the execution of the activities under this agreement;

o) observe tax incentives and/or tax regimes to which Suzano is entitled and comply with the obligations arising therefrom.

LIABILITIES

6.1. This agreement does not and shall not create any employment relationship between Suzano and the Supplier and/or its legal representatives, employees, agents, collaborators, subcontractors, authorized personnel, or third parties. The Supplier shall be responsible for all obligations related to its activities, including labor, social security, land, and insurance charges.

6.2. The Supplier undertakes to defend, hold harmless, and indemnify Suzano against any and all proceedings and/or legal actions, as well as any claims or debts, directly or indirectly arising from the Supplier's obligations under this agreement and/or the relationship maintained by the Supplier with its employees, representatives, agents, or subcontractors.

6.3. If Suzano is subject to any claim, whether judicial or extrajudicial, the Supplier shall, within 15 (fifteen) days from the date of receipt of Suzano's corresponding notice, as applicable: (i) request Suzano's removal from the defendant's side of the proceedings; or (ii) obtain from the claimant a full and final release in favor of Suzano.

6.3.1. If (i) Suzano is not excluded from the judicial proceeding for any reason, and/or (ii) the aforementioned release is not obtained within the time period set forth above, Suzano shall have the right (but not the obligation) to withhold from any amounts due under this agreement and/or any other contractual or legal relationship. between the Parties, the amount (a) that Suzano may be at risk of being ordered to pay in the judicial proceeding and/or (b) that Suzano has been extrajudicially demanded to pay.

6.4. Any disbursements, including attorneys' fees and court costs, or losses resulting from the scenarios set forth in this Clause may, at Suzano's discretion, be deducted from payments to be made by Suzano to the Supplier until Suzano is fully reimbursed and compensated. If this agreement is terminated, the Supplier shall reimburse Suzano within seventy-two (72) hours of receiving the corresponding notice.

6.5. Whenever any part of the services and/or supply is performed within Suzano's premises, the Supplier must present documents evidencing compliance with its labor and social security obligations as

provided in Annex II. Failure to do so shall entitle Suzano to withhold any installment of the Price.

6.5.1. Whenever the Supplier's personnel enter Suzano's premises, the Supplier must strictly comply with the Key Approach Program (Annex I), being subject to a non-compensatory fine of BRL 3,500.00 (three thousand five hundred reais) for each Minor Infraction and BRL 5,000.00 (five thousand reais) for each Serious Infraction, in accordance with the annex.

6.6. The Supplier shall be liable for any losses and damages caused to Suzano or third parties, by its action or omission, as well as those of its legal representatives, employees, collaborators, agents, authorized personnel, subcontractors, and/or third parties involved in the performance of this agreement, including damages to property.

6.7. In the event of breach of any obligation established herein, the defaulting Party shall pay the non-defaulting Party a non-compensatory penalty in the amount of 10% (ten percent) of the Price.

6.8. The Supplier undertakes to complete the activities related to its engagement within the deadlines set forth in the Purchase Order. In the event of delay, the Supplier shall be subject to a late payment penalty of 0.5% (half percent) of the Price for each day of delay in the execution of the supply, capped at 20% (twenty percent) of the Price.

6.9. Suzano, at its sole discretion, may, during the term of the Purchase Order, temporarily make available to the Supplier one or more pieces of equipment, trucks and/or mechanical implements for the provision of services ("Loaned Assets"). Upon delivery and return of the Loaned Assets to Suzano, the Parties shall carry out a checklist to certify the condition of the Loaned Assets..

6.9.1. The Supplier shall use the Loaned Assets exclusively for the performance of the activities under this Purchase Order and shall be responsible for the custody, use, and maintenance of the Loaned Assets. In the event of any damage to such Loaned Assets, the Supplier shall be fully liable for the cost of necessary repairs, with Suzano being authorized to offset the corresponding amounts.

BRAZILIAN ANTI-CORRUPTION LAW

7.1. The Parties, on their own behalf and on behalf of their affiliates, companies belonging to the same economic group, representatives, employees, suppliers, and subcontractors, declare, warrant, and certify that: (i) they act in compliance with and undertake to observe, in the performance of their activities, all anti-corruption provisions set forth in applicable laws and regulations, including, but not limited to, the Brazilian Anti-Corruption Law (Law No. 12,846/2013), the United States Foreign Corrupt Practices Act ("FCPA"), and the United Kingdom Bribery Act ("UK Bribery Act") (collectively, the "Anti-Corruption Legislation"); and (ii) they adopt internal integrity mechanisms and procedures, including training, communication, auditing, and whistleblower channels to ensure full compliance with the Anti-Corruption Legislation.

TERMINATION

8.1. This agreement may be early terminated under the following circumstances:

a) by either Party, in the event of a breach of any obligations set forth in this SCTC that is not remedied within ten (10) days from written notification;

b) by either Party, in the event of the declaration or filing for bankruptcy, dissolution, liquidation, or judicial or extrajudicial reorganization of either Party;

c) by Suzano, immediately, in the event of any breach of the Brazilian Anti-Corruption Law, ESG/Sustainability Principles, Information Security provisions, or any rules established under Suzano's Supplier Code of Conduct, whether by the Supplier, its affiliates, companies in its economic group, suppliers, subcontractors, employees, or representatives;

d) by Suzano, at any time, without cause and without any liability, upon giving thirty (30) days' prior written notice to the Supplier of the intended termination date.

8.2. In the event of early termination of the relationship between the Parties, except for the cases provided in items (b) and (d), the Parties agree to a termination penalty in an amount equivalent to thirty percent (30%) of the Price, payable by the breaching Party to the non-breaching Party, without prejudice to the payment of any proven damages.

8.3. If it becomes impossible to perform obligations due to a duly evidenced force majeure or act of God event lasting more than sixty (60) days, this agreement may be automatically and legally terminated, without the need for any further formality, and without any penalty or indemnity being due by one Party to the other, on any grounds.

GENERAL PROVISIONS

9.1. It is hereby agreed that no exclusivity is established between the Parties by virtue of this SCTC.

9.2. Neither Party may assign or transfer, directly or indirectly, the rights and obligations herein to any third-party without the prior and express written consent of the other Party. Notwithstanding the foregoing, Supplier hereby authorizes Suzano to assign, in whole or in part, the rights and obligations arising from this agreement to any company within its economic group.

9.3. The Parties agree that the Supplier is expressly prohibited from using and/or referring to the name, brand, and/or logo of Suzano (or any company within its economic group) without Suzano's prior written authorization. The Supplier acknowledges that the trademarks Scott, Kleenex, Duramax, among others, are owned by Kimberly-Clark Worldwide, Inc. ("KCWW") (the "Licensed Trademarks") and have been licensed to Suzano for importation, manufacture, marketing, and distribution, through any channel, exclusively in Brazil, by Kimberly-Clark Commercial, LLC, an affiliate of KCWW.

9.3.1. The Supplier agrees to use the Licensed Trademarks in accordance with the written guidelines provided during the term of the commercial relationship between the Parties, in a manner consistent with the high

standards, reputation, and image established by Kimberly-Clark.

9.3.2. Upon Suzano's request, the Supplier shall provide information and samples of marketing materials, point-of-sale materials, or any other materials related to the use of Suzano's brands or the Licensed Trademarks to demonstrate proper usage.

9.3.3. If Suzano determines that its brands or the Licensed Trademarks are being used by the Supplier in a manner that does not comply with the applicable guidelines or is misaligned with the brand's reputation and image, the Supplier shall immediately cease commercialization or distribution of the non-compliant product and/or marketing materials, at its own expense, until such materials are corrected and approved in writing by Suzano.

9.4. All rights and obligations referred to in this agreement may be settled through the legal mechanism of set-off, pursuant to Articles 368 and following of the Brazilian Civil Code.

9.5. Neither Party shall be deemed to be in default or breach, nor shall be liable for any indemnification or penalty, if the delay or failure to perform results from an act of God or force majeure event, duly evidenced, as provided for in the sole paragraph of Article 393 of the Brazilian Civil Code.

9.6. Should any provision of this SCTC be held illegal, null, or unenforceable at any time after its entry into force, such provision shall not affect or impair in any way the validity and enforceability of the remaining provisions, which shall remain in full force and effect.

9.7. This instrument constitutes an extrajudicial enforceable title and may, therefore, be subject to enforcement proceedings for the collection of any amounts arising from the provisions of this SCTC and/or for compelling the performance or forbearance of any obligation by either Party.

9.8. Any waiver or tolerance by either Party regarding the exercise of any right, prerogative, or faculty granted herein shall not constitute a waiver of such right on future occasions, nor shall it constitute a novation or amendment of this agreement.

9.9. This agreement shall be binding upon the Parties and their successors.

9.10. This SCTC shall be governed by and construed in accordance with the laws of the Federative Republic of Brazil.

JURISDICTION

10.1. The central court of the Judicial District of the Capital of the State of São Paulo is hereby elected as the exclusive forum to settle any doubts or legal actions arising from this agreement.

ANNEX I
KEY APPROACH PROGRAM

Purpose: The Key Approach Program establishes a set of priority Safety rules that must be strictly followed at Suzano S.A., with the purpose of developing an Operational Discipline and Safe Behavior in the daily activities, related to a consequence matrix, seeking to eliminate the exposure of employees (own and suppliers) to potential (serious) risks of accident and incident, strengthening the Safety Culture of the company at all levels.

Key Approach Rules: The priority rules of the Key Approach Program were established through the evaluation of the main critical risks in the processes, history of occurrences, and potential severity of associated injuries.

Consequence Management Matrix: The consequence management matrix establishes the criteria adopted to apply accountability measures, in the occurrence of acts or omissions that put at risk the health or safety of the person, the people who work or pass through the site, generating accidents or not, being included in Wrongful Action or Serious Fault.

CONSEQUENCE MATRIX			
Consequence Matrix	Wrongful Action		Second Recidivism or Serious Fault (Non-compliance with Key Approach)
	First Time	Recidivism	
Own Professionals	Warning	Suspension	Dismissal
Service Provider	Warning notice + Contractual Fine	Suspension Notice + Contractual Fine	Dismissal Notice + Contractual Fine

Serious Fault

The classification of a situation as a Serious Fault will occur whenever one of the priority rules of the Key Approach Program, established for the Industrial, Forestry, Distribution Centers and Ports areas, is not complied with.

Exposing or exposing people to Serious and Imminent Risk situations will also be deemed a Serious Fault situation.

Serious and Imminent Risk

According to Regulatory Standard (NR) 3, “serious and imminent risk is deemed to be all work conditions or situations that can cause an accident or illness with serious injury to the worker”.

Serious is an adjective that characterizes something dangerous, serious, severe. Imminent, on the other hand, qualifies something that is about to take place. In other words, the first classifies the gravity of the situation and the second, the chances of it happening. Both, then, serve to characterize the risks in occupational health and safety.

Wrongful Action

Wrongful action is the non-compliance with standards, instructions or procedures issued related to occupational health and safety, that are not included in the Key Approach rules deemed as serious fault.

Registration of Wrongful Action and Serious Fault

Suzano encourages all communications of occurrences in order to allow an analysis system to be prepared to avoid the recurrence of the fact, by establishing action plans.

Any person that is in the business units of Suzano S.A. has the duty to report a situation of exposure to accident risk, mainly when it is characterized in the rules of the Key Approach Program and should take the initiative to request the support of the Labor Safety area to fill out the Incident Analysis Report.

As evidence for the registration of an incident can be used photographic record, CCTV record and/or witness present at the scene of the incident.

In the absence of other witnesses, the report of the employee referring to the identified situation will be considered, for later analysis of the facts.

If it is impossible to register it with a photo, the scenario must be simulated to better represent the incident.

BEHAVIOR RISKS AND RULES – INDUSTRIAL AND DISTRIBUTION CENTERS

Blocking Power Sources: To perform the blocking of all power sources (electric, waterpower, mechanic power, pneumatic power and pressurization), guaranteeing failure before the beginning of activities with the proper tests performed.

Working at height: Use all appropriate, certified fall protection devices.

Handling of Suspended Loads: Possess qualification, certification and authorization to operate machinery and Material for load movement, watching over the due isolation, signaling and access restriction under suspended loads.

Hazardous Substances: Use the appropriate protection Material against chemical and hazardous agents.

Safety Devices: Keep all machinery and Material safety devices in permanent operation, being prohibited to change the operating logic of buttons, emergency stop cables and safety doors.

Access to Restricted Spaces: Access to places characterized as restricted (electrical rooms, substations and confined spaces) only after qualification, training and/or authorization.

Work Release: Perform activities only after the formal issuance and release of the work permit, considering activities that involve risk of fire, corrosive/toxic substance, falling people/materials, burial, electric shock, explosion, burn, radiation, pressing, high/low temperature, oxygen deficiency and/or drowning.

Moving Material: Keep any part of the body out of reach of moving machinery and Material.

Alcohol and Drugs: Drive to work sober, free from the influence, use or possession of illegal drugs or alcohol.

BEHAVIOR RISKS AND RULES – FORESTRY

Safety limits and lists: Work respecting the safety rules between employees and the distance limit between the Material in the forest harvesting.

Speed Limits and Seatbelt: Drive respecting the maximum speed allowed and use the seat belt, without performing dangerous maneuvers.

Working at height: Use all appropriate, certified fall protection devices.

Handling of Suspended Loads: Possess qualification, certification and authorization to operate load moving machines and Material, watching over the due isolation, signaling and access restriction under suspended loads.

Movement of People: Transporting employees adequately in vehicles appropriate for transporting people.

Qualification, Certification and Authorization: Operate machines, vehicles and Material only if you are trained and authorized for the operation.

Hazardous Substances: Work with the handling and application of pesticides protection to avoid contact and exposure to the product and use the proper protection Material protection against hazardous chemical agents.

Safety Devices: Keep all machinery and Material safety devices in permanent operation, being prohibited to change the operating logic of buttons, emergency stop cables and safety doors.

Alcohol and Drugs: Drive to work sober, free from the influence, use or possession of illegal drugs or alcohol.

BEHAVIOR RISKS AND RULES – PORT

Qualification and Training: Operate machinery and Material (crane, forklift, elevating platform and tractor) only if you are qualified, trained and authorized.

Suspended Load Movement: Transit and position only in places where there is no suspended load movement.

Working at height: Work at height (above 02 meters) only if you are trained and authorized, with all the appropriate safety devices.

Blocking Power Sources: Perform and test blocking of all power sources (Electric Power, Mechanic Power, Waterpower, Pneumatic Power, Thermal Power, Chemical Power, ETC, including residual ones), before performing intervention.

Access to Restricted Locations: Access to places characterized as restricted (Electrical rooms, substations and confined spaces) only after qualification, training and/or authorization

Access Permit to Work: Perform activities of high-risk potential (Electricity, restricted spaces, height, hot works, diving and flammable chemicals) only upon the Work Release (LT) duly signed and approved by the person responsible for the service/area.

Machines, Vehicles and Material: Check that during the route you will not be exposed to the action radius of self-propelled machinery in operation and in the risk zones of rotating Material.

Alcohol and Drugs: Work without the influence of the effects or possession of illegal drugs or alcohol.

No Smoking: Smoking is allowed on the terminal premises only in the places designated for this purpose.

ANNEX II
LIST OF DOCUMENTS FOR DOCUMENT MANAGEMENT

DOCUMENTS FOR DOCUMENT MANAGEMENT
(concerning the employees who are made available for the performance of this Agreement)

A. CONCERNING LABOR OBLIGATIONS

1. PAYROLL
2. R.E. FGTS – SEFIP/GFIP
3. WAGE PAYMENT RECEIPTS
4. VACATION RECEIPT
5. INSS SOCIAL SECURITY FORM
6. FGTS PROOF OF PAYMENT
7. TERMINATION OF EMPLOYMENT CONTRACT
8. GRRF + STATEMENT (40% OF FINE OF FGTS ON TERMINATION)

B. CONCERNING OCCUPATIONAL SAFETY AND HEALTH

1. PPRA OR PCMAT
2. PCMSO
3. CIPA
4. PRE-EMPLOYMENT HEALTH PERIODIC, RETURN TO WORK CHANGE OF FUNCTION AND DISMISSAL EXAMS

C. CONCERNING MTB RULING INSTRUCTION 03/97

1. REGISTRATION OF THE EMPLOYEE
2. CONTROL OF WORKING HOURS IN ACCORDANCE WITH THE LAW
3. EMPLOYMENT CONTRACT
4. ANNUAL LIST OF SOCIAL INFORMATION
5. WORK INSPECTION BOOK
6. SUZANO'S SAFETY AREA INSPECTION BOOK
7. CIPA MINUTE BOOK, IF SO REQUIRED, BY VIRTUE OF THE PROVISIONS OF NR. 05
8. *Anotação de Responsabilidade Técnica*., IF APPLICABLE

D. OTHERS

1. LIST OF HIRED AND DISMISSED EMPLOYEES
2. CATEGORY UNION AGREEMENT

Note1: All documents in a single copy.

Note2: The delivery of labor documentation is not restricted to the documents mentioned herein. If necessary, other documents may be requested.

ANNEX III
PRINCIPLES OF SUSTAINABILITY/ESG

Preamble

Sustainability is a relevant part of Suzano's business and is fully integrated into its long- term strategy and vision.

The principles of sustainability established in this document represent social, environmental, and governance guidelines for Suzano's activities in its value chain to build a fairer and more sustainable society.

Suzano also believes that the different connections in its value chain are an essential part of this construction. Therefore, Suzano encourages its suppliers to adopt sustainability commitments, initiatives, and strategies in business performance, with a greater focus on the environmental, social, and governance context (ESG Criteria - Environmental, Social, and Governance), encouraging the adoption of the principles described in this document ("ESG Principles").

1. ENVIRONMENTAL PRINCIPLES

1.1. The Contractor will use its best efforts to monitor its relevant emissions indicators and ensure compliance with the parameters established by the competent environmental agencies, if applicable.

1.2. The Contractor will use its best efforts to reduce greenhouse gas emissions involved in its production cycle and to support the transition to a low-carbon economy.

1.3. The Contractor will use its best efforts to maintain all the necessary structures for the storage of hazardous and non-hazardous chemicals, as well as all necessary authorizations and documents, under the terms required by law, if and when applicable.

1.4. The Contractor will seek to foster the efficient use of natural resources and environmental protection through the appropriate management of the life cycle impacts of its products and services.

1.5. The Contractor claims to be aware of and comply with Suzano''s Wood Supply Policy and undertakes to adopt the necessary actions to not deforest or carry out any vegetation suppression without authorization from the competent authority and not to subcontract services or inputs from suppliers who act in violation of these guidelines.

1.6. The Contractor will seek to foster respect, conservation, and restoration of ecosystems and their biodiversity in the locations where it carries out its activities.

2. SOCIAL PRINCIPLES

2.1. The Contractor will respect human rights, will use its best efforts regarding the UN Guiding Principles on Business and Human Rights and the OECD Guidelines for Multinational Enterprises, and will seek to prevent potential adverse impacts on human rights caused by its activities and throughout its value chain and, if they eventually happen, undertakes to mitigate and repair any resulting damage.

2.2. The Contractor will not condone sexual exploitation or human trafficking.

2.3. The Contractor will promote an equal, inclusive, and non-discriminatory work environment based on gender, sexual orientation, origin, race, color, physical condition, religion, marital status, disability, nationality, or age and will not tolerate any form of discrimination, complying mainly with the provisions of the Contracting Party's Diversity and Inclusion Policy.

2.4. The Contractor will promote a healthy work environment, based on respect and dignity and will not tolerate any physical, moral, or sexual harassment.

2.5. The Contractor will act respecting the way of life of the communities with which it relates in the execution of its activities and will prevent potential adverse impacts caused by its activities on local communities, indigenous peoples, traditional communities, ethnic minorities, and inhabitants surrounding the units where it develops its operations and activities, when applicable, in particular, complying with the guidelines established by the Contracting Party's Policy for Relationships with Indigenous Peoples and Traditional Communities.

2.6. The Contractor undertakes to maintain, if applicable, lodging and/or temporary accommodation ("Lodgings") under the conditions established in the rules applicable to the matter so that the allocation of its employees and/or subcontractors in Lodgings will be mandatorily conditioned to the prior inspection of the Lodgings by the Contracting Party.

3. GOVERNANCE PRINCIPLES

3.1. The Contractor will ensure that there are no conflicts of interest when interacting on behalf of or for the benefit of the Contracting Party, with government agents or any individual, undertaking to inform situations of conflict of interest whenever identified.

3.2. The Contractor will develop its business under the law and principles applicable to antitrust.

3.3. The Contractor will use its best efforts to guarantee the regularity of its organization and registration with the competent authorities, keeping all licenses, documentation, certificates, registrations, and other authorizations necessary for the development of its activities valid, informing the Contracting Party immediately, in case of any event that interferes in its regularity.

3.4. The Contractor will promote ESG good practices in its value chain and promote the qualification and training of employees, managers, and third parties that may act on behalf of the Contractor regarding ESG issues, observing their area of activity, size, and operational complexity.

3.5. The Contractor will use its best efforts to provide a legitimate, accessible, equitable, independent, and confidential communication channel to register reports, complaints, or information of any nature, ensuring their processing and investigation, considering its area of activity, size, location, and operational complexity.

4. MONITORING

4.1. The Contractor's compliance with the guidelines consolidated in these ESG Principles may be monitored by the Contracting Party through the adoption of specific processes and tools, as determined by its internal policies and procedures.

4.2. The Contracting Party may request clarification from the Contractor at any time and, if deemed necessary, require the Contractor to prepare formal action plans to mitigate any controversial activities, risks related to the breach of Human Rights, or activities in disagreement with the contract or the contractual relationship between the Contracting Party and the Contractor.

4.3. In addition to the consequences provided in this Agreement, the Contracting Party may apply the following penalties to the Contractor in case of non-compliance with the ESG Principles:

a) Determination of the Contractor's engagement in a social and environmental impact initiative supported by the Contracting Party and related to the issue of the ESG Principle not complied with; and

b) Participation in training on the subject of the ESG Principle not complied with or on value chain management, as applicable.

ANEXX IV
INFORMATION SECURITY ANNEX

1. OBJECTIVE

This document aims to formalize the minimum information security requirements, both logical and physical, aiming at the protection of Suzano's information, especially restricted and confidential data, allocated within or outside Suzano's environment, in contracts with the Service Provider Companies (SPC). This document applies to any Service Provider that treats or will process (access, modify, store, transmit, etc.) information from Suzano, whether in the Corporate or Industrial environment.

All normative documents published and under Suzano's responsibility, including the Public Information Security Policy, made available on Suzano's website, whose content is available in Documents and Policies, must be followed by the Service Providers that have a contract, which in the context of this relationship, process or can process information.

Suzano reserves the right to perform tests, request corrections and evidence whenever it deems necessary, according to criticality and need.

Important:

• The Service Provider must meet, but not be limited to, the following minimum information security requirements described below, considering both the minimum information security requirements that apply to both the Corporate and Industrial environments;

• It is essential that the Service Provider Company assess the applicability of each of the minimum information security requirements, taking into account the context of the contract. Therefore, topics listed in this Information Security Annex that are not applicable may be disregarded;

•All recommendations from national and international best practices, especially the NIST Cybersecurity Framework, NIST 800-82 guide “Cybersecurity for Industrial Control Systems”, ISA/IEC 62443, and ISO/IEC 27001 must be complied with.

2. GLOSSARY

• Confidential Information: It can be attributed to any information considered highly strategic and critical, for example: trade secrets, intellectual property, marketing and sales strategy, financial data, credentials and passwords, etc., including personal data of users, customers, external parties, among others.

• Information Processing: Set of actions related to the production, reception, classification, use, access, reproduction, transportation, transmission, distribution, archiving, storage, elimination, evaluation, disposal, or control of information;

• ICT Asset (Information and Communication Technology): All technology that allows access, storage, transmission, archiving and manipulation of information, such as, but not limited to: applications, systems, development tools, utilities, industrial automation assets, virtual assets, network assets, among other tools that will be used in the future, due to technological innovation;

• Service Provider Company (SPC): Service provider company or company providing goods with linked services;

• Suzano or Company: Suzano S.A., its subsidiaries and its controlled companies.

3. PROCESS GUIDELINES

3.1. Vulnerability Analysis and Pentest

It is essential that the Service Provider Company conduct cybersecurity tests periodically, to previously address existing Vulnerabilities, to keep its environment up to date and secure, following international best practices, notifying about critical vulnerabilities and action plans for correction. It must also, when requested by Suzano, provide the results of the tests performed.

Suzano reserves the right to perform vulnerability tests and Pentest (Penetrating Test), when applicable and agreed with the Service Provider Company as critical and necessary. For Suzano's validation purposes, a vulnerability test can be performed to prove the corrections were made. The tests are repeated until the identified vulnerabilities are corrected and approved by Suzano's Cybersecurity area.

However, if weaknesses are identified during the vulnerability analysis by Suzano, or even identified by any means, whether by media, security forums, bug bounty, etc., on the platform developed or made available by the Service Provider Company, the SPC, after notification formalized by Suzano, must immediately and timely rescan them, as determined by Suzano.

If the Service Provider Company technically proves the non-applicability of the correction, it will be responsible for any damages generated to Suzano and its related parties due to the Vulnerabilities detected and notified.

If any action is identified as necessary to correct information security vulnerabilities in the environment, that is the responsibility of Suzano, the Cybersecurity area must be informed explicitly and specifically within 48 (forty-eight) hours, via email at CSIRT@suzano.com.br.

Important: Impossibility of performing the vulnerability analysis in ICT Assets or the non-proof of the corrections suggested by Suzano can be considered as a breach of contract or omission by the Service Provider Company.

3.2. Audit

Suzano reserves the right to conduct audits, previously aligned with the Service Provider Company (SPC), to verify the effectiveness of the implemented information security controls. In the case of an information security maturity assessment of the Service Provider Company, it must respond to the assessment questionnaire and send the supporting evidence, ensuring the confidentiality of its information, regarding the implemented information security controls and policies, when requested by Suzano.

3.3. Awareness and Training

The Service Provider Company must periodically provide its employees with appropriate information security training, education, and awareness, as well as regular updates on the organization's information security policy, specific policies, and procedures by topic, relevant to their roles.

3.4. Business Continuity

The Service Provider Company must keep up to date and tested periodically a Business Continuity Plan, in addition to presenting recovery plans thus ensuring the continuity of the services provided to Suzano, in the case, but not limited to, of the occurrence of an information security incident, including cyberattack, such as Ransomware, which can cause the interruption of a service. The SPC must predict at least cases of unavailability of ICT Assets, unavailability of dependencies or unavailability of users.

3.5. Secure Software Development

For contracts involving software development, applications, etc., the Service Provider Company must:

• Ensure and highlight the absence of Vulnerabilities in the source code, for all software modules that make up the ICT Asset, even those not directly developed and, in any case, must follow international standards OWASP, SANS Institute, etc.;

• Ensure a secure software development process to mitigate risks and vulnerabilities cataloged or not, at development time. In case of development or customization for Suzano, the processes and standards already practiced by Suzano must be followed, in addition to subjecting the code to vulnerability checks;
• Ensure the creation of profiles and corporate users with proper access control, ensuring the Need to Know and Least Privilege;
• Ensure the sanitization of all information that is in homologation or test environment;
• Ensure that real data is not used in the testing or homologation environments. A base with no real information or appropriately masked data must be generated for use during testing;
• If there is traffic of credit card data, the Software must be developed in accordance with the PCI-DSS standard.

3.6. Corporate E-mail Suzano S.A.

If the outsourced employee, linked to the Service Provider Company, receives Suzano's corporate e-mail, there must be concerns to use exclusively for the performance of the labor activities signed in the contract, observing the legal and regulatory obligations in force. It must be noted:
• The email account must not be shared with other users;
• The information must be classified, before sending the e-mail and highlighted according to its sensitivity, mainly confidential information, according to the Public Information Security Policy;
• Attachments of unknown origin must not be opened, and suspicious links must not be clicked;
• The e-mail must not be used for registrations on external websites;
• In case of any suspected information security incident, notify immediately via email CSIRT@suzano.com.br.

3.7. Workstations, Servers, and Other Devices

Considering the workstations, servers and other devices used and belonging to the Service Provider Company, including any removable media, used for the work activities provided, it must be guaranteed:
• Perform through individual access credentials, ensuring a unique ID and authentication through strong password and, using the double authentication factor, for the accesses performed;
• Maintain a process of updating software of ICT Assets necessary to correct flaws or defects, avoiding possible Vulnerabilities;
• Have an antivirus update routine and with the "monitoring" function always active. Also, it must be disabled the "disable antivirus" option for the end user. In the event of an information security incident with the identification of viruses, Suzano's Cyberecurity area, through the e-mail CSIRT@suzano.com.br, must be notified, within 24 (twenty-four) hours;
• The data must not be stored, except in cases where it is established in the contract, to fulfill the purposes of the service or contracted activity, and the Service Provider Company must be responsible for applying the necessary security measures for the protection of the information, as well as performing the appropriate disposals, in order to avoid any unauthorized access and/or misuse in the event of Job Rotation or Turn Over;
• Ensure screen lock through password, and downtime on workstations;
• The workstations of the Service Provider Company, when connected to Suzano's network, must:
• Block peripheral ports (USB, USB-C, and SD) to prevent the use of removable devices;
• Be equipped with firewalls, being desirable also Host IPS or EDR/XDR;
• Be free of software that contains tools capable of enabling certified systems on the Internet to interact, access, or manage ICT Assets through communication flows encapsulated in traffic transmitted by Proxy;
• Not be used as bridge devices for the interconnection of logically or physically segregated networks, in particular workstations equipped with more than one connection interface;

• Have restricted, proxy-controlled Internet access with malicious website protection policies for the purpose of protecting any type of unauthorized access;
• Keep patches up to date.

3.8. Information Security Events and Incidents

• It is necessary to ensure the information security of the service provided, identifying and providing information about the person responsible, area and structure, regarding the aspects of information security, to ensure the relations between the Service Provider Company and Suzano, in advance communicating any changes;
• The Cybersecurity area must be notified, when identifying or suspecting any information security event or incident, without discrimination, including accidental ones, via email: CSIRT@suzano.com.br. Communication must be carried out within 24 (twenty-four) hours from the knowledge of the event or information security incident, sharing detailed information, vulnerabilities found, and mitigation actions taken. It must also, when requested by Suzano, provide information inherent to the information security event or incident;
• All activities inherent in the information security incident response management must be documented and stored, providing the entire timeline of the treatment process;
• The Service Provider Company must ensure the necessary security for cases of loss or theft of equipment that may contain information owned by Suzano, through encryption technology and must ensure the deletion of the information. Suzano must be notified, as noted above;
• The Service Provider Company must provide a communication channel for Suzano's Cybersecurity area to communicate, when necessary, in the event of information security incidents;
• The Service Provider Company must commit to collaborating on all necessary actions for addressing an information security incident that occurs in one of Suzano's units involving ICT Assets under the management of the Service Provider Company, in a timely manner.

3.9. Information Protection

The information can be considered the structured and unstructured data set, which may be related to any news or verbal or written communication, manual or automatic. Regarding Suzano, the information expresses the ordering and organization of the data that can generate value and have a meaning for Suzano, regardless of the form or technology employed, whether for its processing, manipulation, transmission, storage, etc. From this concept, the Service Provider Company must:
• Provide all the documented information necessary for the development of the business, in Portuguese (native language of Brazil);
• Ensure that the information under Suzano's property is processed, in accordance with the Need to Know and Least Privilege principles, in addition to applying the segregation of duties, exclusively within the contractual service, avoiding disclosure to unauthorized users;
• Safeguard the confidentiality, integrity, availability, authenticity and legality, including maintaining compliance with current laws and regulations, of all information processed in Suzano, regardless of its format;
• Have full traceability of access to Suzano's information, in order to identify the origin, author, date and time, in addition to the information accessed, with a minimum retention time of 12 (twelve) months;
• Encrypt confidential data under Suzano's responsibility at rest and in transit, using strong encryption methods, when handling, storing or transmitting;
• The Service Provider Company must ensure that the Subcontractor follows all the minimum information security requirements expressed in this document. The Service Provider Company is responsible for any contracts or partnerships involved in providing the service to Suzano.

3.10. Cloud Service Provider

For the Service Provider Company that is a cloud service provider or that uses its services for information storage, a secure cloud computing environment must be ensured for Suzano, following the requirements of the Cloud Security Alliance (CSA).

For a Service Provider Company that is a supplier of SaaS solutions, it must ensure, in addition to the minimum requirements mentioned in this document, but not limited to:

- There must be segregation of duties in administrative activities in the cloud management console;
- All user authentication activities in the cloud management console must be logged;
- All accesses to the cloud management console must use strong authentication methods, involving at least two authentication factors;
- Cryptographic keys used in the cloud infrastructure must not be stored or transmitted in clear;
- The cloud solution contracted by Suzano must have centralized Log management enabled, containing audit logs of cloud resources;
- Audit logs of cloud resources contracted by Suzano must always be available for access in case of suspected information security incidents identified by Suzano;
- Cloud monitoring must be enabled for event detection of possible cyber attacks and alert generation;
- When information security incidents or events are identified, the cloud solution must ensure the notification of alerts;
- Web services exposed on the Internet must be hosted in networks protected by Firewall and by infrastructure for monitoring/blocking anomalous traffic, such as IPS (Intrusion Prevention System) and IDS (Intrusion Detection System);
- The ICT Asset must use protection mechanisms against DoS/DDoS cyberattacks (Denial of Service attacks or Distributed Denial of Service attacks); The solution involving the ICT Asset must have controls for network perimeter and traffic interconnection points, including internal ones, such as VPC (Private Network), Firewall, IPS, IDS, etc.;

3.11. Network Segmentation

- Industrial Automation Assets that share common functionalities and security requirements must be organized into logical and/or physical security zones;
- Configurations with routing implemented in Next-Generation Firewalls must be established, allowing only necessary application communication for plant activities between segments. In other words, the flow must be restricted within the Industrial environment, which the ISA/IEC 62443 standard refers to as a conduit;
- Physical and logical segregation between the Corporate and Industrial environments is mandatory. Therefore, equipment sharing between environments, including subnets (VLANs), is not allowed. The concept of flow restriction, as outlined in the ISA 62443 standard, must be followed for communication in the Industrial Network;
- Suzano adopts a specific structure with well-defined communication rules between different network levels, based on the Purdue Enterprise Reference Architecture (PERA) model. All components of the Industrial environment for the Service Provider Company must be hosted in their respective subnets (VLANs) within this structure.

3.12. Physical Security

- A physical access control must be given to the Service Provider Company dependencies, for any user, being: collaborator, visitor, etc.;

• A CCTV system must be used, with recording and storage of images for a minimum period of thirty (30) calendar days, and online;
• There must be implemented preventive controls for physical security in all its premises, segregating, when possible, the facilities used exclusively for the provision of the contracted service, especially when the service uses confidential data of Suzano.

3.13. Information Systems

The ICT Assets of the Service Provider Companies are systems, platforms, physical or logical technological tools, through which Suzano's information is treated. From this concept, the Service Provider Company must:
• Make available to Suzano all major versions and packages of the Software that makes up the contracted Solution;
• Keep the facilities where the information systems are hosted protected and with controlled access;
• Ensure that the user has an individual access credential, with a unique ID, and must keep the history of all activities performed by that credential;
• Use M2M (Machine to Machine) access credentials only for troubleshooting, when applicable, in a controlled manner and performing the password exchange after use;
• Assign the defined authorization profiles to access the ICT Asset data, with the concepts of Need to Know and Least Privilege, in addition to applying role segregation. Profiles must be configured before the start of data treatment, so that it is documented and associated for each user or for a set of users who will perform the same function;
• Perform periodic review of credentials and access profiles to information systems;
• Access from users who are no longer assigned to Suzano or who no longer need to access Suzano's data must be removed immediately for the purpose of preventing unauthorized access. It must be guaranteed:
• Removal by downtime;
• Removal on the expected expiration date, unless extended at Suzano's request;
• Access block after incorrect attempts;
• Access block when identifying illegal use or when the security of information is put at risk;
• Access block at Suzano's request.
• Implement a strong password pattern using the double authentication factor, for the accesses performed;
• Ensure that all installed Software must be legally licensed;
• Have updated antivirus, whenever new versions are available;
• Keep Operational Systems and applications up to date according to OWASP standard security recommendations, when applicable;
• Modify and delete default information system settings, such as passwords, ports, service accounts, etc., applying Hardening according to the manufacturer recommendations;
• Implement appropriate security controls and practices to protect all communication interfaces used in the contracted services. Such measures should include strong authentication, authorization, and encryption mechanisms, recognized by industry best practices; Apply vulnerability mitigation already known, according to best practices;
• Protect the entire environment by Firewall and IDS (Intrusion Detection System), as well as having the proper segregation of networks, to protect the infrastructure, leaving exposed only the front end and the exposure layer. Information systems exposed on the Internet must have WAF (Web Application Firewall) and denial of service protection solutions (DoS/DDoS);

• Adopt appropriate backup and restore processes when there is Suzano information being processed, in accordance with the contract manager. The process must be documented and must contain at least an indication of the frequency, execution methods, archiving and retention of backups, including restore test;
• Suzano’s information must be kept only during the term of the contract. When applicable, backups must be delivered to Suzano and must be ensured the correct disposal of all information owned or controlled by Suzano;
• All solutions that contain Suzano's data must be segregated between production and testing environments, so that they are allocated in distinct physical and virtual infrastructures;
• Implement specific operational procedures for the execution of restoration activities, when applicable, including the implementation time agreed with the contract manager and the guarantee of the continuity of the service contracted by Suzano, on the occurrence of an information security incident in the information systems;
• Encrypt confidential information that is processed, stored and transmitted by the information systems that maintains Suzano information, to ensure the protection of the information;
• Implement tracking of users and administrators in information systems, aiming at the collection and storage of access records (Login / Logout) and any other actions performed, maintaining integrity, non-repeatability and non-repudiation. Traceability of access and actions must be maintained for a minimum period of 12 (twelve) months;
• Information systems, when applicable, must undergo vulnerability analysis and intrusion testing before entering in production environment and must be evaluated periodically even when already in a production environment.

3.14. Wi-Fi Suzano S.A.

Access to Suzano Wi-Fi is made available to users, from its premises, being dedicated to work activities. However, certain actions are not allowed, such as:
• Personal access point must not be installed over the Suzano network to set up a parallel Wi-Fi network. The connection to Wi-Fi services is only allowed through wireless, using Suzano's infrastructure;
• No activity that could cause damage to the Suzano network service or infrastructure must be performed. Here are some illegal activities, but are not limited only to these: port scanning, vulnerability scanning, password identification, sniffing, spoofing, network discovery, fingerprinting, footprinting, Pentest, redirect or traffic modification, etc.