Ingeteam ELECTRIFYING A SUSTAINABLE FUTURE

RN8. A.11-5-01

IS Clauses for Suppliers

DOCUMENT CONTROL	
DATE:	07/03/2024

CONTENT

1 PROPOSED PROTECTION AND INFORMATION SECURITY CLAUSE

Ingeteam has Information Systems Security Regulations that regulate the measures to be adopted in the processing of information and the information systems that support them. The supplier will accept these Safety Regulations for all the services that are the subject of this contract.

1.1 DEFINITIONS

a. **Information Systems Infrastructure**: This refers to electronic information and communications systems and services, as well as the information contained therein. This includes both systems hosted on physical premises and those based on cloud services, owned or third-party, in all their forms. The Information Systems Infrastructure comprises the hardware and software used to process (create, access, modify, and delete), store (on various magnetic, electronic, or other media), and transmit (share and distribute) information, as well as any combination of these elements. It encompasses a wide range of electronic devices, such as standard (desktop/laptop) computers with a network connection, digital storage media, mobile phones, smartphones, personal digital assistants (PDAs), digital and video cameras (including CCTV video surveillance systems), mobile navigation systems, among others.

b. **Restricted Information**: Refers to all information created, received, transmitted or stored that, due to its nature or value to Ingeteam, requires additional protection measures. This includes, but is not limited to, confidential or reserved information, personal data, credit card data, commercially sensitive information, information related to critical infrastructure, strategic business data, access credentials, encryption data, access logs to systems and applications, as well as any other information subject to regulation or that may be considered sensitive.

c. **Data Security Breach:** For purposes of the Contract or Order, "Data Security Breach" shall include: (A) the loss or misuse of Restricted Information; (B) unauthorized or unlawful processing, corruption, modification, transfer, sale, or assignment of Restricted Information; or (C) any act or omission that compromises the security, confidentiality, or integrity of the Restricted Information.

1.2 SUBCONTRACTING

If the Supplier, duly authorized by Ingeteam, decides to subcontract part of the services related to this clause, it undertakes to ensure that the subcontractor assumes the same obligations established in this document. At all times, the Supplier shall be liable for any failure by the subcontractor or its personnel to comply with the cybersecurity and information security obligations described in the Contract or Order.

1.3 DATA AND INFORMATION OWNERSHIP

In cases where the data or information related to the Contract or Order is the property of Ingeteam, or where the elements of the Information Systems Infrastructure are supplied to the Supplier by Ingeteam, the Supplier undertakes to process and use such data and information exclusively to fulfil its obligations under the Contract or Order and for no other purpose.

Throughout the process of processing the data or information related to the Contract or Order, the Provider undertakes to comply with all applicable laws and regulations regarding security and data protection. In addition, the Supplier undertakes not to put Ingeteam in a situation of non-compliance, either by action or omission.

In cases where personal data is processed, the personal data processing contract must be signed.

1.4 INFORMATION PROTECTION

The Provider undertakes to maintain continuous knowledge of the level of protection of the Restricted Information related to the Contract or Order, as well as the applicable relevant regulations and legislation. It will adopt appropriate technical and organizational security measures to ensure the protection of such information.

These security measures will be proportionate to the type of Restricted Information processed and the services that are the subject of the Contract or Order, ensuring at least a level of security consistent with industry best practices. Such measures shall include physical, electronic, and procedural safeguards to protect the Restricted Information against potential data security breaches or other security incidents, as well as to comply with any security requirements, obligations, specifications, or reportable events set forth in the Agreement or Order.

The Supplier shall ensure a secure environment for all Restricted Information and for any hardware or software containing such information and which is to be provided or used by the Supplier in the performance of the Contract or Order, provided that such items are on its premises.

When processing Ingeteam information, the Provider must comply with Ingeteam's information classification scheme. If the Provider has its own classification scheme, an association must be developed between both information classification schemes.

The Provider will guarantee the security of information transfers by implementing the necessary security controls depending on the level of classification of the information to be transferred.

The Provider is not authorized to disclose, provide direct or indirect access to, or allow access to Ingeteam's Restricted Information to third parties, including for its storage. It is also not authorized to provide the ability to decrypt encryption keys. In the event that it is necessary to involve a third party, an express written authorization from Ingeteam will be required, indicating the purpose, and the third party will be required to comply with the same obligations as the Provider.

External personnel who have access to Ingeteam information must consider that such information, by default, is confidential. Only Ingeteam information to which it has had access through the means of public dissemination of information provided for this purpose by Ingeteam may be considered as non-confidential information.

The confidentiality agreement between the Supplier and Ingeteam must be signed before the start of the contractual relationship.

1.5 INFORMATION EXCHANGE

No person should conceal or manipulate their identity under any circumstances.

The distribution of information, whether in digital or paper format, will be carried out using the resources determined in the contract for the provision of services for this purpose and for the exclusive purpose of facilitating the functions associated with said contract. Ingeteam reserves the right to implement control, registration and audit measures on these dissemination resources, depending on the risk identified.

In relation to the exchange of information within the framework of the contract for the provision of services, the following activities shall be considered unauthorized:

a) Transmission or receipt of material protected by Copyright in violation of the Intellectual Property Law.
b) Transmission or receipt of any kind of pornographic material, messages or of an explicit sexual nature, racially discriminatory statements and any other kind of statement or message classifiable as offensive or illegal.
c) Transfer of files to unauthorized third parties of Ingeteam material or confidential material.
d) Transmission or receipt of files that infringe the GDPR or Ingeteam's guidelines.
e) Transmission or reception of games and/or applications not related to the business.
f) Participation in Internet activities such as newsgroups, games, or others that are not directly related to the service provided.
g) All activities that may damage the good reputation of Ingeteam are prohibited on the Internet and elsewhere.
h) Any information that contains personal data (whether on computer or paper media or by e-mail) may only be carried out by authorized personnel and with due permission, in compliance with the defined procedure and the laws in force.

1.6 USE OF INGETEAM'S COMPUTER RESOURCES

In the event that Ingeteam makes electronic devices or other computer resources available to the Supplier's or its subcontractor's personnel, or grants them an Ingeteam email account or credentials to access applications, connections or other elements of Ingeteam's Information Systems Infrastructure in order to fulfill the object of the Contract or Order, the Supplier shall be responsible for ensuring that such personnel are fully informed and expressly undertake to comply with the security conditions and the Acceptable Use Regulations established by Ingeteam. Such conditions will be provided to the Supplier in a specific addendum. The Supplier will be responsible for safeguarding the documents that prove compliance with these obligations by its staff and will make them available to Ingeteam when required.

1.7 SECURITY MEASURES TO BE ADOPTED BY THE SUPPLIER

a) Connection between Networks: The connection between Ingeteam's network and that of the Supplier is not permitted, unless expressly agreed in the Contract or Order. In such a case, it shall be based on encrypted and authenticated virtual private networks, with the minimum number of interconnection points required. This connection will be removed once your need is over. Direct connections of Supplier users to the Ingeteam network will not be permitted, unless expressly authorized and for the agreed time. In the event of a connection to the Ingeteam network, it is not possible to make a connection to another network at the same time.

b) Physical Access Control: If the Contract or Order is carried out at the Supplier's premises, the Supplier shall establish physical access control mechanisms to prevent unauthorized access to the infrastructure or Restricted Information.

c) Logical Access Control: The Provider will implement identification, authentication and logical access control measures to prevent unauthorized access to its Information Systems Infrastructure and Ingeteam's Restricted Information. Procedures based on the principle of least privilege will be established and an updated inventory of accesses and permissions will be maintained. The Supplier will pay special attention to the custody of access credentials to the Systems owned by Ingeteam. In cases where Ingeteam so requires, the Provider shall implement the two-factor authentication system for access to any system of the organization.

d) Operational Continuity: The Supplier shall establish technical and organizational measures to ensure the continuity of operations, including contingency plans, backup and recovery procedures.

e) Computer Equipment: In the event of access to Ingeteam's Information Systems Infrastructure with the Provider's computer equipment, adequate security measures will be guaranteed, such as automatic blocking, protection against malicious software and updating of the operating system. Provider agrees that these devices may be audited and monitored.

f) Paper Data Protection: Procedures will be established to adequately protect and destroy paper documents containing information related to the Contract or Order when they are no longer necessary.

g) Equipment Development: Appropriate security measures will be included in the development, maintenance and testing of equipment used for the fulfillment of the Contract or Order, including secure code development standards and the use of fictitious data in test environments.

The Provider will apply these security measures in accordance with the sensitivity of the information involved and following Ingeteam's information classification scheme. In addition, it will provide the information requested by Ingeteam on any processing of Restricted Information.

1.8 CHANGES AND DEPARTURES OF PERSONNEL ASSOCIATED WITH THE SERVICE PROVIDED

The supplier undertakes to immediately notify any change or termination of personnel who have access to Ingeteam's systems, data or facilities. This notification must be made no later than 24 hours after the termination of the employee's employment or contractual relationship with the supplier.

At the time of notification of the change or termination, the supplier must ensure that all access by outgoing personnel to Ingeteam's systems, data and any property is immediately revoked. This includes, but is not limited to, user accounts, physical accesses, authentication credentials, and any other type of access that allows interaction with Ingeteam's resources.

1.9 SECURITY OF SUPPLY OF EQUIPMENT AND MATERIALS

In the event that the object of the Contract or Order includes the supply of equipment and materials, the Supplier must guarantee the application of standards and good security practices in the design, manufacture, maintenance and, where appropriate, installation of the material supplied, as well as its components.

For equipment and/or materials with information processing capability or network connectivity options:

a) Supplier shall provide evidence or certificates ensuring the secure design of the equipment, periodic firmware/software updates and effective protection against malware.

b) A periodic vulnerability analysis will be carried out by the Provider, who will inform Ingeteam about the necessary updates, especially those related to security.

c) Devices with connectivity capacity must be protected by passwords with due complexity, allowing their modification by Ingeteam.

d) The configuration of the devices, equipment and materials must be adjusted exclusively to the needs of Ingeteam, deactivating any functionality not required. In the event that the Provider performs the configuration, it must provide documentation evidencing such adjustments.

1.10 SECURITY INCIDENT NOTIFICATION AND MANAGEMENT PROCEDURE

The Provider will implement a security incident notification and management procedure, which will be disseminated among its personnel. It will act with special diligence in cases involving critical elements of Ingeteam's Information Systems Infrastructure, Restricted Information, or when the reputation, legal liability, or interests of the persons whose information is processed are at risk.

The Provider will immediately notify Ingeteam of any security incident that may affect Ingeteam, within a maximum period of 24 hours from its detection or within the applicable legal period and will collaborate with Ingeteam in the communication to third parties and in the required remediation measures.

Security incidents will be reported by email to the address: csirt.global@Ingeteam.com.

In the event of incidents involving personal data, the Supplier must also inform Ingeteam's personal data controller.

Incidents to be reported include, but are not limited to:

to. Unauthorized access or attempts to systems, computers, applications, files, devices, etc.

b. Disclosure or compromise of credentials, authentication data, or encryption. Email account spoofing.

c. Total or partial loss of data or information for any reason.

d. Unauthorized Distribution of Information.

and. Loss or theft of computer equipment or media.

f. Virus or malware attacks.

g. Other irregularities related to the established security criteria.

Actions, resolution times and follow-up mechanisms will be agreed between the Supplier and Ingeteam according to the severity of the incident.

In the case of relevant incidents in the Supplier, even if it has not been possible to define the degree of affection to Ingeteam, it will also be notified within a period of less than 24 hours of becoming aware, A relevant incident is defined as one that:

- Has caused or may cause serious operational disruptions to services or financial loss to the affected entity.
- Has affected or may affect other persons or legal entities by causing substantial material or non-material damage.

1.11 RETURN AND DESTRUCTION OF INFORMATION AND EQUIPMENT

Once the contractual performance has ended or in the event of termination of the Contract or Order, the Supplier must return to Ingeteam or securely destroy, at the latter's option, all information belonging to Ingeteam that is in its possession, as well as any medium or document containing Restricted Information. In the event of opting for the destruction of the information, the Provider will provide a corresponding certificate, following recognized standards for this purpose.

In addition, all equipment, devices and media owned by Ingeteam will be returned, and all possible connections to Ingeteam's Information Systems Infrastructure will be cancelled. This process will be carried out when the infrastructure elements or information are no longer necessary to fulfill the obligations of the Contract or Order.

If the Provider is obliged by applicable regulations to keep Ingeteam Restricted Information, it must keep it duly protected and only for the time required by law. Once this period has elapsed, the information will be destroyed or returned to Ingeteam, at the latter's choice, as well as any medium or document containing such information, without keeping additional copies.

1.12 SECURITY ASSESSMENTS AND AUDITS

The Provider shall provide, at the request of Ingeteam, proof of security assessments or audits, and even allow, at the request of Ingeteam, independent audits and inspections to be carried out at its data processing facilities or in cloud services, with respect to the security measures set out in these clauses.

These audits or inspections may be carried out by Ingeteam or by an auditing entity commissioned by Ingeteam. Supplier agrees to comply with any action plan resulting from such audits.

1.13 SUPPORT IN RESPONDING TO DATA-RELATED COMMUNICATIONS

The Provider undertakes to provide Ingeteam with efficient and timely support in responding to any requests, complaints, or other communications received from government entities, regulatory authorities, or the like in the use, disclosure, or misuse of any data or information

1.14 TRAINING AND AWARENESS

The Provider shall ensure that its personnel are trained for the task at hand, in particular in specific information security procedures (e.g., resolution of security incidents).

The Provider must also ensure that personnel have an adequate level of awareness about information security and are up to date with the most common techniques of social engineering and other types of cybersecurity attacks.

1.15 RELEVANT CONTACTS

The Supplier must make available to Ingeteam at the beginning of the employment relationship, a list of the relevant contact persons in terms of information security, as well as the communication channels to be used.

1.16 ACQUISITION, DEVELOPMENT AND MAINTENANCE OF INFORMATION SYSTEMS. SAFE DEVELOPMENT POLICY.

The following requirements apply to all software development or maintenance services for Ingeteam.

Suppliers must apply secure systems engineering processes for developments that affect Ingeteam. These processes seek to provide objective guarantees regarding the security of the software produced. To do this, mechanisms must be applied and evidence must be produced during the process (measurable, verifiable, and repeatable) that guarantees that the software consistently exhibits the security properties that are required.

Ingeteam will supervise and control the software developed by third parties, specifically:

- Licensing and ownership of source code,
- Types of tests to be carried out on the outsourced software.
- Compliance with software security and functionality requirements.

System development should only be performed by qualified system developers with the necessary demonstrated knowledge of secure programming.

The provider shall follow and use secure development methodologies and support tools for the correct development of the applications.

When addressing the development of the application, it will be necessary to comply with all the requirements in terms of personal data protection contemplated in the General Data Protection Regulation, especially with regard to security by design and by default.

The use of components, libraries, etc. without a valid license or limited to private and non-professional use in the developments provided by the Provider is not permitted.

The vendor must establish a baseline of security requirements, throughout the life cycle of the software development, with the aim of preventing and solving possible threats/errors in early stages of development. If in doubt, it should be validated with the cybersecurity team.

The system architecture should be reviewed to determine if it meets the requirements of a secure infrastructure.

All system development must be controlled by change control procedures.

The validity dates of access permissions must be defined for all members of the project, restricting access for the time strictly necessary.

Prior to the application going into production, it must undergo security tests, defined by Ingeteam, in order to detect vulnerabilities.

The development environment must be continuously maintained, being separated from the production and test environments.

Development, pre-production, and production environments should be logically isolated from each other.

1.17 INTELLECTUAL PROPERTY

Compliance with legal restrictions on the use of material protected by intellectual property regulations will be ensured.

Employees may only use material authorized by Ingeteam for the performance of their functions.

The use of computer programs without the corresponding license in Ingeteam's Information Systems is strictly prohibited.

Likewise, the use, reproduction, transfer, transformation or public communication of any type of work or invention protected by intellectual property without due authorization is prohibited.

Ingeteam will only authorize the use of material produced by itself, or material authorized or supplied to it by its owner, in accordance with the terms and conditions agreed and the provisions of current regulations.

1.18 CLOUD ENVIRONMENTS

The following requirements apply to any contracted service located in the cloud:

In order to protect the information that is located and transmitted in the cloud, the provider must establish security measures related to the development of a security infrastructure that includes:

- Encryption measures for the storage and transmission of information using secure algorithms.
- Ensure the availability of the information stored in the cloud and the possibility of access by Ingeteam.

- A communications system between Ingeteam's applications or systems and those of the supplier that are carried out in encrypted form, are authenticated at each end and are hidden from the outside.
- In the event that Ingeteam's information shares the cloud with the information of other customers, a logical separation must be established to prevent unauthorized access.
- Access to Ingeteam's data by suppliers' technicians must always be approved and registered
- In the event that Ingeteam so requires, the supplier shall:
- To send the activity carried out by the users of the systems and applications, online and continuously, so that Ingeteam can monitor the service through its corporate tools.
- To provide physical and logical isolation for the Ingeteam service, assigning the devices (servers, databases, storage units, etc.) exclusively for the Ingeteam service, and may not be used to provide service to other customers of the supplier unless expressly agreed with Ingeteam.
- Completely isolate the internal network, based on communications, from the supplier in which the systems and applications intended for Ingeteam's service are located, from the rest of its network, and from the other networks used by the supplier for other customers.

1.19 SECURITY POLICY UPDATE

Due to the evolution of technology, security threats and new legal contributions in the matter, Ingeteam reserves the right to modify these policies when necessary. The changes made to these policies will be disclosed to all service provider companies to which they apply using the means deemed appropriate. It is the responsibility of each supplier company to ensure that its staff reads and is aware of Ingeteam's most recent security policies.