Security of Information (CIA)

February 1, 2021

130 Cypress Club Drive #316
Pompano Beach 33060 FL USA

Secure.Cloud@WiseGroup.info
www.WisePlant.com

Table of Content

Summary

From WiseGroup we are aware of the importance it has for our clients, by the nature of our services dedicated to functional safety, Security of people, security of assets, Industrial cybersecurity and critical infrastructure, to have an information management system that meets the requirements of the projects and services we provide.

Our information security document management system is aligned and integrated with the ISA/IEC-62443 series of industrial cyber security standards as a supplier and incorporates all related services and projects.

Our management system has scope over all the information managed by WiseGroup, which must be and is treated according to its classification without exception. It includes all the information that is received as well as all the information that is generated by the sales, engineering, services, productive and administrative units of WiseGroup.

Security of Information

It is a fact that information security has become a key aspect to be considered by security companies and one of the biggest concerns today. Clear proof of this is that, currently, there are organizations – both public and private – focused exclusively on security issues and have published guidelines to help companies cope with security problems.

An example is the ISO 27002 standard. It is a standard implemented by the International Standards Organization, which deals specifically with information security. ISO 27002, originally published as a renaming of the ISO 17799 standard, describes an infinity of possible controls and control mechanisms for greater security of documents and business data.

And finally, a good document security system, usually implemented through a document management system, not only protects the company, but also improves the perception and confidence of customers and users in terms of service quality or the product that that we offer, sell, provide, support and maintain.

------ Continue next page ------

Management of Confidential Documents

The management of confidential documents is essential in the development of our activities to ensure adequate treatment of sensitive data regarding security, availability, privacy and compliance with legal provisions. To this end, we implemented an internal policy aimed specifically at regulating the treatment of confidential documents.

The absence of control implies exposure to serious risks. All confidential or personal data, regardless of the support in which they are located, must be handled in such a way that it is guaranteed always, the security of the information they contain either during use, file, custody, transfer or destruction, so that only authorized personnel can be accessed in compliance, in addition to the guarantees required by law and/or the requirement of our customers.

Confidential documents contain sensitive information that requires protecting your security, privacy, integrity, or availability. Instead, non-sensitive information is not subject to special protection and can be shared with anyone. Known as "classified information" is a special type of sensitive information whose access is subject to restrictions imposed by governments or other agencies because their disclosure may impair the interests of our clients and the security of their Assets.

Confidential document management includes aspects of identification of confidential documents, classification, storage, utilization, distribution, access control or follow-up procedures, among others.

For the confidential documents to be treated properly, we have a classification methodology in order to protect the information that, to become public, it could harm its owner or affect their safety and or security. The grading process may require an impact assessment. Depending on the possible damage that the information could cause in the event of falling into the wrong hands, the classified information is typically marked with one of several hierarchical levels of sensitivity, such as Critical, Strictly Confidential, Confidential, Private/Restricted or Public.

Confidential document management policies must be applied to all documents generated in the enterprise with confidential information and data sensitive whatever the support, both for digital format and paper and others, since the rules applicable to data security refers to all types of media.

To ensure the security of the information contained in the confidential documents, we make sure that computer systems and corporate networks, that in principle are systems that can be insecure for the problems generated by viruses or hackers, are managed in a proper way determining in other respects, who has the privilege of accessing a document as well as to its location, conservation, security or recovery in case of loss or destruction of the file. These precautions and safety measures must also be applied to the paper holder.

We establish internal standards in terms of confidentiality and information security so that all documents containing confidential data and/or sensitive, regardless of the support in which they are located, are managed during their use, filing, custody, transfer and destruction in such a way that only authorized personnel can access them with the guarantees required by law if they exist or by our clients on demand of contracts.

Privacy and data confidentiality is an increasingly important issue for many organizations, especially for security services such as those we developed at WiseGroup, so companies that handle sensitive data in a regular way they must be very careful in the treatment of such information so that their clients are sure that their privacy will be respected always. And

this depends on the prestige, the image of the company and the safety of the critical infrastructure, essential for business and operations to work.

Information Classification

For the purposes of the classification we have adopted the following criterion according to the following degrees of sensitivity of the information:

- **C4 - Critical** (Top Secret or Ultra Secret): It is the highest level of classified information. Such material would cause "Extreme Damage" to National security if it is made available to the public.
- **C3 - Strictly Confidential** (secret): Material that would cause "serious harm" to national security or private if publicly available.
- **C2 - Confidential** (confidential): Material that may cause "damage or harm" to safety or security.
- **C1 - Private** (Restricted, broadcast limited or only for official use): Material that would cause "undesirable effects" in case of disclosure.
- **C0 - Public** (of free access): Although technically it is not a classification level, it is a common feature in the classification schemes, for documents that do not deserve a classification or that have been declassified.

Protection of information

When destroying data carriers containing confidential information (either paper, microfilm, perforated chips, optical media such as CD or DVD, magnetic media such as hard drive, ID cards or floppy disks, electronic media such as USB flash drives or Chip cards) DIN 66399, which regulates the destruction of data carriers, establishes 3 levels of security with respect to data carriers:

- **Protection Class 0 "Not Controlled Documentation"**: General or global access public information. The documentation and its contents are obtained by means generally public and does not require control by WiseGroup. Examples: brochures, third-party technical information, data sheets, etc.
    - Intellectual property rights must be ensured.
    - Free Access or easy access.
- **Protection Class 1 "Controlled Documentation"**: Normal protection requirement for internal data, whose unauthorized disclosure would have few negative effects on the company. Examples: source files for Class 1, administrative documents, purchase orders, licenses, etc.
    - Restricted access only to its recipients or holders.
    - Traceability is required.
    - Possible authentication and authorization processes.
    - Controlled by Quality Management Systems.
    - Identification, revision control, validity, etc.
- **Protection Class 2 "Confidential Documents"**: High protection requirement for confidential data, whose unauthorized disclosure could have significant consequences for the company and could violate contractual laws or commitments. Examples: Sensitive customer information for specific projects.
    - Digital signatures required.

  - Document's Control processes in place.
  - Possible protection through Secure systems and methods.
- **Protection Class 3 "Strictly Confidential Information"**: Requirement of very high protection for secret data, whose unauthorized disclosure would have serious consequences for the company and would violate professional secrecy, contracts and laws. Examples. Patents, copyrights, information classified by our clients, secret, etc.
  - Encryption of documents required.
  - Encrypted Access and Access through secured means.
  - Circulation of information is strictly limited in access, read, copy, print, etc.
- **Protection Class 4 "Critical Documents"**: Requirement of the highest data protection Ultra Secrets, whose unauthorized disclosure would have serious consequences for the Nation.
  - (We don't manage or handle these type of documents)

Class Definition

To the effects of giving adequate treatment to all the information that is received, generated and managed by WiseGroup we introduce the following class definitions. Classes can be applied to documents, manuals, programs, designs, engineering, configurations, systems, information and/or hardware.

C0: "Public information" generally of public access without restrictions, except those restrictions related to the rights of the intellectual property or the author of the information included in it. This documentation can be obtained, received or generated internally or by a third party. Public documentation can be controlled, that is, subject to review, approval process, etc.

C1: "Information Private or restricted" With requirements for normal protection of private data of restricted access to be used only by the recipients for a specific purpose. The Public disclosure is not authorized. Traceability is required with possible authentication and validation mechanisms. Must be identified uniquely and is susceptible to control of revisions and validity period. We must provide protection against accidental, unintended or unintentional violations.

C2: "Confidential Information" which contains data or Material that can cause "harm or be harmful" for safety. We must provide protection against intentional violations by means of simple mechanisms, low resources, generic knowledge and low motivation. Usually confidential information is associated with information that has a certain level of secrecy.

C3: "Strictly confidential Information" Material that would cause "serious damage" to national security if publicly available. We must provide protection against violations using sophisticated methods with moderate resources, specific knowledge and moderate motivation.

C4: "Critical information" usually intended or referred to the National security or national critical infrastructure security, governmental, military, secret of summary and/or state secrecy. Specific management requirements and/or compliance with specific standards can be incorporated into this kind of information. We must provide protection against intentional violations using sophisticated mechanisms, broad resources, specific knowledge and high motivation.

Traceability

Our document management system must keep the audit trails of the operations carried out. It is in this way that we can carry out a thorough monitoring of the documents with the possible modifications made and the people who have accessed them. Thus, any auditor will be able to trace the data to be able to reach the source document.

Signatures

Date, Feb 1st, 2021

WisePlant Group LLC

Sign

Maximillian G. Kon, CEO

Name and Position

Date, _____

Sign

Name and Position

Sign and return to
Secure.Cloud@WiseGroup.info