POLICY ON INFORMATION SECURITY AND THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES (ICT)

POLICY ON INFORMATION SECURITY AND THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES (ICT)

PREAMBLE

The evolution and rise of new information and communication technologies significantly change our society's relationships between individuals and the business world.

The significant changes and the evolution of computer communication tools and new information technologies allow businesses to reach previously unimaginable levels of business efficiency. At the same time, these tools entail a great shared responsibility between the companies and the users and beneficiaries of these media in the business environment.

It is, therefore, essential to develop, develop and promote within the business environment those appropriate protection and security mechanisms that guarantee adequate and permanently updated IT infrastructures from which companies and the professionals that make them up can benefit together while developing all the elements that ensure the integrity and security of their systems.

For this reason, the SANDO GROUP defines its Information Security and ICT Use Policy, developing the guidelines and principles that ensure adequate and effective use of technological mechanisms within a secure environment for information.

The policy and its guidelines are governed by the principles of social awareness, cooperation, integrity, transparency, legality and good faith of the Company and all the professionals who make it up (considered as such, directors, managers and employees of the Company) (the "Professionals"), based on its Code of Conduct.

SANDO expressly recognises the importance of Information Systems and their protection to avoid data loss and/or unauthorised or illicit use, which could cause significant damage to customers, professionals, and/or the Company itself and its image in the market.

To this end, this policy is defined to adopt all technical and organisational measures necessary to ensure integrity, availability, confidentiality, and the information systems that support them. The Company's commitment is embodied in the following points:

- Constant investment and responsibility for information security. The necessary and appropriate means will be established to protect and guarantee the security of the data, people, programs, equipment, facilities, documentation and other supports that make up SANDO's computer and technological systems to prevent the alteration, copying, loss, processing or unauthorised access of the information they contain. At the same time, it will be the responsibility of all the Company's Professionals to know and respect the security mechanisms adopted by the Company.

- Continuous development and adaptation to technical advances. This policy will be specified and developed through rules, guides, standards, circulars, manuals and procedures, which will be updated as necessary under the new requirements imposed by advances in technology.

- Dissemination of information and training. The dissemination of information and training to all professionals and consultants, agents or contracted third parties will be encouraged, preventing the commission of errors, omissions, fraud or crimes and trying to detect their possible existence as soon as possible.

- Risk control. Adequate and reasonable preventive, detection and corrective controls will be established against possible criminal conduct and those risks that may influence the information not being accurate, complete or not available within the established time. These controls shall be proportionate and appropriate to the criticality of the assets to be protected and their classification. Likewise, these controls will be auditable based on the applicable Rules and Procedures and always under current legislation.

SCOPE OF APPLICATION

This Information Security and ICT Use Policy is mandatory for all users of the information and communications systems of the companies belonging to the SANDO GROUP.

For these purposes, users will be considered the Company's Professionals, comprised of all managerial, technical, administrative, productive or service staff, regardless of their employment contract, whether permanent, temporary or any other.

Likewise, third-party customers, suppliers, subcontractors, and other similar entities working for SANDO and all those providing access to the Company's computer, technological mechanisms, and resources will be considered users.

There is a *Communication Channel* (through the e-mail address ***canaldenuncias@sando.com)*** available to all SANDO GROUP Professionals that will attend and resolve any questions, doubts or uncertainties regarding the application of this policy in each specific case.

GUIDELINES IN THE FIELD OF INFORMATION SECURITY AND THE USE OF ICTS

Along with SANDO's commitment to creating, developing, maintaining and controlling the most effective and robust information and communication technology systems, keeping guidelines on information security and technology uses is essential.

This policy sets out the essential guidelines related to information and ICT security so that all organisations' efforts converge on the following primary objectives: safeguarding the security of the Company's technological systems and the information they contain and guaranteeing the correct development of professional services.

KEY POINTS TO KEEP IN MIND

SANDO's commitment to compliance with the laws and principles on which they are inspired is absolute in every one of its areas of activity and is an essential part of the development of its activity under the principles of ethics and excellence.

Concerning information and communication technologies, Spanish law prohibits and punishes, among others, the following conduct:

- The use, possession or dissemination of computer programs and files protected by intellectual or industrial property rights, for which there is no authorisation or licence to use.

- The use, possession or dissemination of programs or means intended to neutralise or suppress the protection measures of computer programs and files protected by intellectual or industrial property rights.

- Delete, deteriorate, alter, suppress or render inaccessible computer programs or electronic documents, or by the same means impede the normal functioning of a computer system.

- Invading the privacy of another by intercepting their e-mails or stealing their documents or images, as well as their subsequent dissemination.

- The discovery, seizure or interception, by any means, of restricted, secret or confidential business data or information, as well as its subsequent dissemination.

- The modification, seizure or use of confidential data belonging to others and their subsequent dissemination.

- Downloading, possessing or disseminating racist, sexist, xenophobic, pedo-pornographic, degrading or illegal content.

- Harassment.

The above conducts can be punished severely for the natural person (up to 5 years in prison in some cases and a fine) and the Company on behalf of which that natural person eventually acts (fines, suspension of activities, closure of premises, etc.).

To analyse security incidents and ensure that information and communication technologies are used under this policy, the Company has mechanisms for monitoring and recording the computer systems made available to users. This includes but is not limited to, the use of the Internet and corporate e-mail, as well as fixed and portable computer equipment such as workstations, mobile devices, data storage devices, etc.

GUIDELINES IN THE FIELD OF INFORMATION SECURITY

The following guidelines address the ethical and security principles in developing SANDO's activity. They aim to safeguard the integrity and security of the information made available to users for the optimal performance of their functions. Specific guidelines for the use of ICTs complement them.

First.- Personnel Safety

Any technological resource user accessing the Company's Information Assets must observe the confidentiality principle, which prohibits disclosing sensitive information to third parties inside or outside the Organization without express authorisation.

Second.- Privacy

Compliance with the regulations related to personal data protection will be observed.

Third.- Access Control to Information Assets

Passwords are strictly confidential and personal; therefore, they must be used responsibly and diligently.

Fourth.- Responsibility of the User

All users of technological resources who have access to SANDO's Information Assets must adhere to the Rules and Procedures derived from this policy to protect Information Assets.

Fifth.- Telematic commercial relations

Establishing a relationship with a customer, partner and/or supplier through e-commerce must be preceded by a risk estimate that determines the value of

the information being exchanged, the shared access system and the acceptable level of risk.

Sixth.- Access Security of External Collaborators

The access of external collaborators (consultants, agents or contracted third parties) to SANDO's communications or IT resources will be restricted and duly authorised.

Seventh.- Business Alliances

The interactions and relationships that the Company maintains with its partners, collaborators, etc., must be duly protected to ensure the confidentiality, integrity, availability and traceability of the information of both parties. Therefore, the information provided and received, and the security procedures of our own and others in this regard, must be analysed.

Eighth.- Evaluation of Information Assets and their Protection

All SANDO business information will be classified and its value set to ensure the information is adequately protected throughout its life cycle.

Ninth.- Entry Access Control Security

Access to all facilities containing Information Assets that need to be protected will be protected.

GUIDELINES FOR THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES (ICTS)

The following guidelines respond to the ethical and security principles in developing SANDO's activity, particularly in the use of information and communication technologies available to users for the optimal performance of their functions.

First.- SANDO owns the information, resources and professional ICT tools

All computer and communications resources and tools made available by SANDO to its Professionals are owned by SANDO. They are provided to increase productivity and improve the work environment. The user of these computer resources must use them responsibly and diligently.

All the information contained in physical media (files, paper, etc.) or electronic format (intranet, computer equipment and electronic devices of the Company) is part of the knowledge and value of the Company and, therefore, owned by SANDO.

Second. - Professional use of devices and systems

The devices and systems made available to its Professionals by SANDO will be used exclusively for the functions and purposes arising from the position held.

Each user will respect the privileges attributed to them and act according to the ethical principles and conduct set out in the Sando Group's Code of Conduct.

Third.- Unauthorised uses of devices and systems

Any use of devices and systems contrary to the law, this policy and the principles of conduct established in the Code of Conduct are not permitted. In particular, those that may affect the principles of data integrity, availability and confidentiality, the protection of intellectual property, respect for individuals and their privacy, and the prevention of the discovery or disclosure of trade secrets.

CONTROL AND SUPERVISION

SANDO ensures information security and the use of ICTs under the principles established in this policy through appropriate supervisory mechanisms.

When any of the following cases occur, the Company may implement the control and supervision mechanisms it deems appropriate, consisting of the monitoring of its computer systems, including, among others, corporate Internet and e-mail services, regardless of the location and device used:

1. There are indications that a user is engaging in any of the conduct prohibited by this policy;

2. existence of reasonable indications that criminal offences or offences of any nature (administrative, labour, etc.) may be committed through SANDO's ICT means;

3. the existence of reasonable indications of harassment or any other conduct in using the Company's ICT resources that may cause harm.

In these cases, SANDO may investigate the corresponding breach within the limits and guarantees legally applicable.

RESPONSIBILITY

Failure to comply with the provisions of this policy, the guidelines for action contained therein, or the implementing Rules and Procedures will lead to disciplinary sanctions that, where appropriate, may lead to the termination of the employment or commercial relationship that the offender maintains with SANDO, under the applicable legislation and conventional regulations, as well as the initiation of appropriate legal actions by the Company.

In the event of termination of the employment contract, the procedures described in the current Rules and Procedures will be followed.

Those consultants, agents or contracted third parties temporarily provided with access to SANDO's computer and technological resources must previously adhere to this Information Security and ICT Use Policy so that its action guidelines bind them.

REPORTING OF NON-COMPLIANCE

Any SANDO employee who becomes aware of an action that violates this policy or constitutes a breach of any of its rules of conduct must report it to the *Compliance Body* by any of the following means:

- Through the Whistleblowing Channel enabled on the SANDO intranet
- By letter addressed to:

  Criminal Enforcement Body
  Avenida José Ortega y Gasset, 112 – SANDO Building
  29006 - Malaga

All reports of violations of this policy and its rules of conduct will be considered and appropriately investigated.

Such notification will be protected by confidentiality as long as it is given in good faith.

COMMUNICATION OF THIS POLICY

This INFORMATION SECURITY POLICY AND THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES ("ICT") will be communicated to all administrators, managers and employees of SANDO, as well as periodic awareness-raising and reminding actions of the Company.

its existence.

* * *

NOTE: This policy is annexed to the Protocol on the Prevention and Detection of Crimes, approved **by the SANDO Board of Directors at its meeting on April 30, 2021.**