

	INSTRUCTION	Number: IN-TEC-014
		Revision: 00
Subject INFORMATION SECURITY AND TECHNOLOGY		

1. GENERAL CONSIDERATIONS AND OBJECTIVES

Considering:

- The need to define the Information Security and Technology Policies, aiming to establish unified concepts and common practices within the ORTIZ Group;
- That the information and software, as well as the resources used for their development, processing, storage, and distribution of their content, must be protected regarding their consistency, security, and access permissions;

This Instruction aims to establish the Information Security and Technology Policies to be applied in all Business Areas and Corporate Administration.

2. SCOPE

The provisions of this Instruction apply to all companies of the ORTIZ Group.

ANNEXES:

Annex I – Responsibilities, Policies and Guidelines
 Annex II – Glossary

This Instruction comes into effect as of this date.

São Paulo, January 24, 2018

	INSTRUCTION	Number: IN-TEC-014
		Revision: 00
Subject INFORMATION SECURITY AND TECHNOLOGY		

ANNEX I

RESPONSIBILITIES, POLICIES AND GUIDELINES

1. RESPONSIBILITIES

1.1. LEADERS

- a) Guide their team members in accordance with the provisions of this document, especially to ensure they do not use Internet access and e-mail resources for personal purposes during working hours.

1.2. TEAM MEMBERS

- a) Be familiar with and follow the Policies and Guidelines established in this Instruction.
- b) Report to the Technology Director any fact or incident that may compromise or put at risk the security of the information and products (games) of the ORTIZ Group.

1.3. TECHNOLOGY DIRECTOR

- a) Manage Information Technology resources.
- b) Develop and implement electronic game software and their respective control systems, carrying out maintenance, changes, and/or cancellations as necessary.
- c) Ensure compliance with this Instruction, promoting or obtaining innovations and the continuous improvement of the quality and security of the information and products (games) developed and marketed by the ORTIZ Group.
- d) Analyze and assess cases of violation of this Instruction, proposing corrective and preventive measures and suggesting disciplinary actions to the violators' respective Leaders.
- e) Block communication channels and systems when members are terminated.

	INSTRUCTION	Number: IN-TEC-014
		Revision: 00
Subject INFORMATION SECURITY AND TECHNOLOGY		

- f) Draft and propose supplementary Information Security Standards, based on legal requirements, market best practices, and the business characteristics of the ORTIZ Group.

1.4. ADMINISTRATION AND FINANCE DIRECTOR AND REGIONAL DIRECTORS

- a) Disseminate this Instruction to all Members, including in their Employment Contracts confidentiality clauses acknowledging the contents of this Instruction, in accordance with Instruction IN-PES-007.
- b) Together with the Technology Director, carry out refresher and awareness programs for Members regarding information security aspects.
- c) Inform the Technology Director of any Member's termination so that their access to communication channels and systems can be blocked.

1.5. OTHER CORPORATE DIRECTORS

- a) Ensure compliance with this Instruction by all Members of their respective Teams.

1.6. AUDIT AND INTERNAL CONTROLS MANAGEMENT

- a) Conduct periodic audits of networks and systems to ensure this Instruction is being followed, and may request monitoring of equipment, systems, and networks when deemed necessary.

2. POLICIES AND GUIDELINES

2.1. OWNERSHIP OF INFORMATION AND SOFTWARE

- a) The data and information created using ORTIZ Group's computing resources are its property and must be used by its Members and Service Providers exclusively in the performance of their activities.
- b) Software acquired on the market or developed internally belongs exclusively to the ORTIZ Group, including all rights related to any inventions, technological innovations, and intellectual creations developed by its Members and Service Providers during the term of their employment/contractual relationship, or when ORTIZ Group resources, data, means, materials, facilities, equipment, technological

	INSTRUCTION	Number: IN-TEC-014
		Revision: 00
Subject INFORMATION SECURITY AND TECHNOLOGY		

information, and trade secrets are used.

- c) The ORTIZ Group develops and implements electronic games and their respective management and control systems, which are essential for revenue generation and for meeting regulatory and contractual obligations. To ensure the Group's Business Security, these systems (games) require clear definitions of the essential controls regarding: (i) access; (ii) maintenance; (iii) changes; (iv) cancellations; (v) validations; (vi) parameter settings; and (vii) other necessary controls. These definitions must be part of the development and implementation stages of these software (games) and their respective management and control systems

2.2. USE OF INFORMATION TECHNOLOGY RESOURCES

- a) Information technology resources must be used exclusively for the performance of professional activities of Members and/or Service Providers of the ORTIZ Group.
- b) The ORTIZ Group may inspect any and all information—such as files, emails, directories, etc.—that transits or is stored in its environment or in any devices belonging to the ORTIZ Group, in accordance with the Responsibility, Commitment and Confidentiality Agreement signed by the Members who fully agree and adhere to the content of this Instruction.
- c) The antivirus system used to protect workstations must remain active, without configuration changes, and must always be updated by the Technology Directorate team.
- d) Backups of all information produced on desktops, notebooks, tablets, and smartphones must be stored in the storage infrastructure provided by the Technology Directorate and/or the respective Technical Teams of the Regional Directorates.
- e) Access to essential and infrastructure systems must be requested via email, specifying the required access profile, and must be approved by the hierarchical superior and/or the respective information owner.

	INSTRUCTION	Number: IN-TEC-014
		Revision: 00
Subject INFORMATION SECURITY AND TECHNOLOGY		

- f) During vacation periods and/or any type of leave, access to essential systems, network, email, and remote access must be deactivated. This rule does not apply to Managers and Directors. Other exceptions must be analyzed and approved by the Technology Director upon prior request by the respective Leader.
- g) Access to restricted environments may only be granted with approval from the person responsible for the environment or the Technology Director.
- h) The Member receiving a visitor is responsible for accompanying and granting the visitor access to ORTIZ Group facilities.
- i) Users must use encryption resources when made available by the Technology Directorate.
- j) For the transmission of confidential and sensitive content, it is the responsibility of the Technology Directorate to provide encryption resources and guide Members in their use.
- k) Remote access by Members and Service Providers to ORTIZ Group information and technological resources must be arranged by request from the respective Leadership, via email to the Technology Directorate, and in accordance with the specific conditions for each type of access.

2.3. INFORMATION SECURITY

- a) All data and information generated and handled during the development and execution of ORTIZ Group systems and processes are considered its Intangible Asset. Therefore, they must be protected in accordance with the provisions of this Instruction.
- b) All Members must ensure that the information contained in the systems is kept within their work environment and must not be disclosed or shared with individuals outside the ORTIZ Group's staff.
- c) Information contained in systems, documents stored on the network, local computers (desktops, notebooks, etc.), or email accounts whether under the responsibility of the Member or third parties must be considered strictly confidential and must not be disclosed or removed from ORTIZ Group premises by any physical or electronic means, to avoid loss, theft, copying, misuse, or unauthorized disclosure.

	INSTRUCTION	Number: IN-TEC-014
		Revision: 00
Subject INFORMATION SECURITY AND TECHNOLOGY		

- d) All computers connected to internal networks must have standardized antivirus software, permanently activated and updated, as well as password-protected screen savers.
- e) Service providers and consultants must not have access to the internal network except when using computers supplied by the ORTIZ Group, properly configured according to adopted standards.
- f) Service providers and consultants may only access the Internet via wireless connection using the guest network, properly segregated from the corporate network, and with prior approval of the person responsible for the area managing the services provided.
- g) Users of devices with Internet access must be extremely cautious and must not open emails with attached files from unknown or suspicious addresses, in order to avoid receiving viruses, spam, etc.
- h) The Audit and Internal Controls Management must conduct periodic audits of networks, systems, and equipment to ensure that this Instruction is being followed, and may request monitoring of these resources when deemed necessary.

2.4. INFORMATION SECURITY IN THE WORKPLACE

- a) Members must not leave documents containing strategic, sensitive, or confidential information exposed on desks, meeting rooms, whiteboards, flipcharts, printers, fax machines, or mail dispatch/receipt points.
- b) Each Member must adopt a “clean desk” practice whenever absent for a significant period from their workstation, such as during long training sessions, vacations, trips, etc. “Clean desk” means the organized storage of documents and media in drawers and/or appropriate cabinets provided for their use.
- c) Special attention must be given to cleaning meeting rooms at the end of activities so that no information, confidential or otherwise, is left behind.
- d) Members who use mobile or removable devices such as notebooks, tablets, smartphones, USB drives, removable hard disks, etc., that store ORTIZ Group information must take special care in storing and transporting these devices to avoid theft or loss.

2.5. USE AND PROTECTION OF PASSWORDS

	INSTRUCTION	Number: IN-TEC-014
		Revision: 00
Subject INFORMATION SECURITY AND TECHNOLOGY		

- a) Passwords are personal and non-transferable and must be kept under the custody and responsibility of each Member. Passwords must not be shared. They are an important information security tool, as they are used to validate users when accessing internal systems, the Internet, email, and active network elements (routers and switches).
- b) Passwords must be created by the Members who use the systems. The following precautions must be taken in creating and protecting passwords:
 - Whenever the system allows, passwords must contain at least eight (8) characters, including one (1) special character, one (1) number, and six (6) interspersed alphabetic characters. The last six (6) passwords used must not be repeated.
 - Passwords must have a maximum validity of sixty (60) days and may be changed by the user at any time within this period if there is any indication or suspicion that they have been compromised, or for any other justifiable reason at the user's discretion.
 - Do not use common words such as the names of family members, colleagues, companies, pets, IT terminology, website names, etc.
 - Do not use birthdays, addresses, phone numbers, sequential words, numbers, or letters.
 - Do not use "remember password" features in applications such as Internet Explorer, Outlook, Dial-up, and others.
 - System, application, and equipment administrator passwords (ROOT, NT, ADMIN, and others) must be changed at least every forty-five (45) days and previous passwords must not be reused.

	INSTRUCTION	Number: IN-TEC-014
		Revision: 00
Subject INFORMATION SECURITY AND TECHNOLOGY		

c) Remote access to internal data and information:

- Allows users of IT resources, who must be duly authorized by the Directorate, to access their databases and information outside their usual workplace to meet professional needs.
- Suppliers and service providers authorized by the Directorate to remotely access data and information must have specific “confidentiality” clauses in their Service Provision Contracts.
- Such access must be carried out with additional care by Members and include special protection mechanisms to prevent undue exposure of information and damage caused by unauthorized access.
- Remote access must be via the Internet, through an Internet Service Provider (ISP) contracted by the user, provided that a Virtual Private Network (VPN) for external access to the internal network of an ORTIZ Group company is installed on their computer and supplied by the IT Support Manager, along with standardized antivirus software.

2.6. INTERNET AND EMAIL

- a) Internet access must be for the purpose of obtaining information essential to the ORTIZ Group’s business or for performing online services that may increase the productivity of each Member’s functions.
- b) The Internet access services available and allowed are as follows:
- www (World Wide Web), to access various websites of professional interest to the Member.
 - FTP and downloads: specific tools for transferring large-volume electronic files.
 - Videoconferences: specific tools for participating in forums, debates, and seminars remotely.
 - Email, for communication between people.

	INSTRUCTION	Number: IN-TEC-014
		Revision: 00
Subject INFORMATION SECURITY AND TECHNOLOGY		

- c) Internet access may be used by Members for personal matters (bank transactions, email, etc.) before clocking in at the start of work, during lunch breaks, or after clocking out at the end of work, within reasonable limits.
- d) Access to videoconferences, large file transfers (over 10 MB), and other services that require extensive Internet bandwidth must be scheduled in advance by mutual agreement with the person responsible for IT resources.
- e) Internet access and browsing must be protected by access monitoring controls, antivirus software on workstations and servers, and a firewall to protect against attempts to damage the infrastructure and the information existing in ORTIZ Group networks.
- f) All Internet access is monitored and analyzed, and any violations of this Instruction are subject to administrative sanctions.
- g) Access to websites with prohibited content must be automatically blocked by the access servers.

2.7. PROHIBITED USES

- a) IT resources (computers, software, networks, Internet, emails, etc.) must not be used by Members for illegal or unethical activities, such as:
 - Obtaining or distributing software or files that imply “copyright” or “intellectual property” infringement; the legislation in force on licensing and copyright in each country must be strictly followed.
 - Disseminating or distributing software or products that function as viruses and/or that may harm the ORTIZ Group or cause damage to recipients/third parties.
 - Installing, distributing, reproducing, and using any software not licensed by the ORTIZ Group.
 - Obtaining or attempting to obtain unauthorized access to other ORTIZ Group systems or computer networks.

	INSTRUÇÃO	Número: IN-TEC-014
		Revisão: 00
Assunto: SEGURANÇA E TECNOLOGIA DA INFORMAÇÃO		

- Interfering with or interrupting services, servers, or networks connected to ORTIZ Group systems.
 - Disclosing information or lists of Members to third parties without prior authorization from the Corporate Directorate.
 - Sending unsolicited emails (spam) or chain letters/pyramid schemes.
 - Transmitting or disclosing material with illegal or defamatory content, that may violate third-party privacy, or that is abusive, discriminatory, prejudiced, threatening, obscene, harmful, offensive, or otherwise objectionable.
 - Transmitting political, religious, or similar material.
 - Accessing websites that promote violence, corruption, pornography, social, racial, religious, or political discrimination, or any that promote offense and violate good morals.
 - Sending messages without identifying the source or using other people's email accounts without their authorization.
- b) Storing and/or copying email messages on desktops, notebooks, and/or mobile devices (smartphones, tablets, removable media, etc.) in .pst files or similar formats.
- c) Changing workstation settings, especially security settings, without prior formal authorization from the appropriate authority. These settings are made and maintained by the Technology Directorate.
- d) Using ORTIZ Group Information Technology resources to provide services to third parties.
- e) Any other uses for illegal purposes or that violate any applicable law or regulation of each country, or that are not in accordance with the Policies and Guidelines of the ORTIZ Group.

	INSTRUÇÃO	Número: IN-TEC-014
		Revisão: 00
Assunto: SEGURANÇA E TECNOLOGIA DA INFORMAÇÃO		

ANNEX II GLOSSARY

1. **Access:** Authorization to use a technology resource, with permission to read or modify information stored on it (normally controlled by a security device such as a password). Also, the ability to enter a secure building (physical security definition).
2. **Remote Access:** Authorization to use the corporate network's IT resources, with permission to read or modify information stored on it from physically distant locations, and the ability to integrate computers located outside the network so that they operate as if they were locally connected to it.
3. **Information Classification:** Process by which a level of confidentiality is assigned to information. The higher the level of confidentiality of a piece of information, the more it will affect the data set in which it is contained—whether a document, a file, or even a database.
4. **Email:** Systems for managing electronic messages whose purpose is to manage and streamline communication between people and companies, adding business benefits and facilitating the flow of information.
5. **Service Providers:** Consultants, technicians, or outsourced labor who use the information assets and/or IT resources provided by the ORTIZ Group.
6. **Access Control:** Prevention and control of unauthorized use of a resource. Tasks performed by hardware, software, and administrative controls to monitor the operation of a system, ensure data integrity, identify the user, record access and changes in the system, and allow user access.
7. **Flipchart:** Sheets suspended on a wooden stand used in lectures, conferences, and training sessions, enabling the instructor to write, draw, and create charts.
8. **Security Incident:** Any event or occurrence that triggers one or more actions that compromise or threaten the confidentiality, integrity, and availability of information resources, resulting in damage.
9. **Information Resource:** Everything that is part of the information technology components of the ORTIZ Group (e.g., hardware, software, documentation, data).
10. **Physical Security:** Set of measures aimed at protecting and ensuring the integrity of the physical assets of the ORTIZ Group.
11. **Essential Systems:** Systems considered mission-critical, which, due to regulatory needs, contractual obligations, operational support, and revenue, are of high importance to the business.
12. **Infrastructure Systems:** Fundamental infrastructure systems intended to define, maintain, and establish domains of computer environments and networks.

	INSTRUÇÃO	Número: IN-TEC-014
		Revisão: 00
Assunto: SEGURANÇA E TECNOLOGIA DA INFORMAÇÃO		

13. **Software:** Games, control systems, and operating systems.
14. **User:** Person responsible for handling information (viewing, editing, adding).