iris360

Our Plan is Our Promise

www.iris360.org

Network and Information Security Policies

Revised: February 22, 2023

1. **OBJECTIVE**

The objective pursued by this document is to establish and communicate the Information Security Policies, foundation for establishing effective control over the activities of employees of **Iris360,** related to computer operations or to the use of the information and computer equipment.

2. **SCOPE**

The Information Security Policy applies to all employees, contractors, business associates, commercial promoters, and distributors of **Iris360**, who have access to information through the documents, computer equipment, technological infrastructure and communication channels of the organization.

3. **DEFINITIONS**

1. **Asset:** Everything that has value for the Organization. There are several types of assets including: Intellectual property, Software information, such as a computer programs and documents. Physical, like a computer. People, their qualifications, skills and experience. Intangibles, such as reputation and image.
2. **Files:** Set of data or instructions that are stored in the Hard Drive and / or any other means of storage with a name that identifies them. Example: EMPLOYEES.DOC, where EMPLOYEES is the name and DOC is the extension of the file.
3. **Authorization:** GROUP process or official procedure by which the authenticated user receives the permissions to carry out activities on elements of the information system.
4. **Password:** is a form of authentication that uses secret information to control access to a program or parts of a program, a terminal or personal computer, a point on the network, etc. The password must be kept secret at all times.
5. **Confidential:** Means that the information, labeled as such, is not available nor can be disclosed to individuals, institutions or unauthorized parties.
6. **User Account*:*** Identifier used by an Information System in the authentication of a user.
7. **Email Account:** It is the service based on the exchange of information through the network and which is provided by **Iris360** to authorized employees. The main purpose is to share information quickly, easily and safely. The electronic mail system can be used to exchange information, manage address books, manage contacts, manage schedules and to send and receive documents, all exclusively related to Iris360's business.
8. **Information Custodian:** Individual in charge of the information security administration. Among the assigned responsibilities is the coordination of efforts between IT personnel and information users, the latter being responsible for the information they use.
9. **Hard Drive:** Equipment used for information storage.
10. **Information Availability:** It is the condition of the information to be available to those who must access it at any time they require it, whether they are people, processes or authorized applications.
11. **Computer Equipment:** They are the electrical, electronic and mechanical devices that are used to process data. (Hardware)
12. **Hardware:** Set of components (CPU, monitor, keyboard and mouse) that make up the material part of a computer.
13. **Integrity:** Property to safeguard the accuracy of information and its processing methods which must be accurate.
14. **Information:** It is all that can be expressed through a language and is used by Iris360 during the development of its business that is the result of some effort, cost, or investment that providing a competitive advantage, and that must be protected from inappropriate disclosure to a third party.
15. **Internet:** Global decentralized computer network, formed by the direct connection between computers through a special communication protocol.
16. **Intranet:** An intranet is a computer network that uses Internet Protocol technology to share information, operating systems, or computer services within an organization.
17. **Instant Messaging:** Commonly known as "Chat", it is a communication channel provided by Iris360 to facilitate a form of real-time communication between associates, suppliers and authorized distributors, creating a virtual space for a specific meeting.
18. **Monitor** (screen): It allows to visualize the data output of a computer.
19. **Phishing:** It is a cybercrime which, by means of an email, deceives people by inviting them to visit dark or fake web pages where the

recipient is requested to verify or update personal data to steal user names, personal passwords and other confidential information.

20. **Policy:** General statement of principles that presents the position of the administration for a defined control area. The policies are developed to have long-term application and to guide the development of more specific rules and criteria that address specific situations. Policies are deployed and supported by standards, best practices, procedures and guidelines, policies must be few (i.e. a small number), must be supported and approved by the organization's senior management and must offer directions to the entire organization or to an important set of departments. Policies are mandatory and the inability to fulfill a policy requires that an exception be approved.
21. **Programs (software):** Set of computer language instructions built to automate a process or a task through electronic data processing.
22. **Information Owner:** In information and communication technologies (ICT) is the individual responsible for preserving and disposing of information according to the guidelines provided by Iris360. The term information technologies are often used to refer to any form of automation.
23. **Screen Saver:** Image or mobile design that appears on a device screen when a certain period elapses during which there is no interaction with a user. The screen savers prevent the screen from being damaged because of the presentation of dark and luminous areas in the same position for a long time.
24. **Information Risk:** Possibility threat against an information asset caused by a vulnerability and / or a failure in a control, resulting adverse impact. Controlling the threat or vulnerability reduces the risk.
25. **Information Security:** Refers to information being kept confidential (meaning that information is not made available or disclosed to unauthorized individuals, institutions or other parties), having integrity (protection of the accuracy and completeness), and being available (accessibility and usability on demand by an authorized institution).
26. **File Storage Service "On line":** A file hosting service, online file storage service, or online media center is an Internet hosting service designed specifically to host static content, mostly large files that are not web pages. In general, these services allow web and FTP access. They can be optimized to serve many users (as indicated by the term "hosting") or be optimized for single user storage (as indicated by the term "storage"). Some related services are video hosting, image hosting, virtual storage and remote backup copying.
27. **System:** Set of components that are neatly interrelated to contribute to a certain objective.
28. **Information Systems:** An information system is a set of organized elements oriented to the processing and administration of data and information, generated to fulfill a need or an objective. Usually the term is used erroneously as a synonym for computer information system, partly because in most cases the material resources of an information system are constituted almost entirely by computer systems. It could be said then that computer information systems are a subclass or a subset of information systems in general.
29. **Software:** It is the set of instructions by which the Hardware can perform the tasks ordered by the user. It is integrated by programs, operating systems and utilities.
30. **Illegal Software:** It is the Software that is acquired and installed without the consent of the person or company that develops it. It is also called Pirate Software, where its manufacturer does not obtain any economic consideration for its use and its intellectual property rights are violated.
31. **Spam:** Also known as junk mail, spam is email that involves almost identical messages sent to numerous recipients to create chaos and damage computer resources. Malware is often used to spread spam messages by infecting a computer, searching for email addresses and then using that machine to send spam messages. Spam messages are generally used as a method of propagating phishing attacks.
32. **Third Parties:** People or companies other than **Iris360** but related to the company. Example: Customers, prospects, suppliers, distributors or any company that are candidate to provide services to **Iris360**.
33. **Types of Information:** Any information produced and/or received by, the company, its associates, and in general by any other related party, regardless of the means of registration and reception (analog or digital), and that are stored in:
    a. File documents (physical and electronic).
    b. Organizational files (physical and electronic).
    c. Corporate Information Systems.
    d. Cooperative Work Systems.
    e. Document Management Systems.
    f. Electronic Messaging Systems.

g. Portal, Intranet and Extranet.

h. Data base System.

i. Hard drives, servers, disks or portable media, tapes or video and audio media (analog or digital), etc.

j. Tapes and support media (back up or contingency).

k. Storage technologies in the cloud.

34. **USB:** USB memory (Universal Serial Bus) is a type of data storage device that uses flash memory to store data and information.

35. **Information User:** Individual who uses a device or a computer and performs multiple operations with different purposes. It is often a user who acquires a computer or electronic device and who uses it to communicate with other users, generate content and documents, use software of various types, and many other possible activities.

36. **Vulnerability:** Weakness of a system, which opens the possibility to perform actions that may negatively affect it.

1. INTRODUCTION

Information assets and computer equipment are important and vital resources for **Iris360**. Therefore, the Board of Directors and Senior Management have the duty to protect, preserve, use, and improve them.

This implies that appropriate actions be taken to ensure that information and computer systems are properly protected against any kind of threats and risks.

The information property of **Iris360** must be protected according to its value and importance. Security measures must be adopted and used regardless of how the information is created and stored (on paper or electronically), how it is processed (PCs, servers, voicemail, etc.), and how it is transmitted (email, file transfer, verbally).

5. APPLICATION OF SECURITY POLICIES

Iris360's Information Security Policies have been adopted as mandatory and contain the necessary information to allow all employees to adapt a "Culture of Security and Control of Information", so that they become aware of the imperative need to protect Information, Hardware and Software. These policies are applicable to the administration of:

- **Information:** Data sorted, classified and stored in any media (Magnetic, Paper, email, telephone conversation, etc.).
- **Software:** Set of Operational Systems, programs, products and applications used by the organization.
- **Hardware:** Set of computer equipment, telecommunications and networks used by the Organization.
- **People:** Users and Administrators of information and computer equipment.

6. BASIC CONCEPTS

6.1. INFORMATION CHARACTERISTICS

- **Confidentiality:** Refers to the protection of sensitive information from unauthorized disclosure.
- **Integrity:** Related to the completeness and accuracy of the information in accordance with the values and expectations of **Iris360.**
- **Availability:** Related to the ease and opportunity to access information when required by **Iris360** processes to conduct business now and in the future.

6.2 CLASSIFICATION OF INFORMATION

Sensitive or Confidential Information: Information that, due to its nature, must be maintained under strict reservation and security t guarantee access only by authorized personnel and for a previously defined purpose.

- **Internal Information:** Information used by **Iris360** employees to perform normal business operations. Example: policies, methods, procedures and standards.
- **Public Information:** Information that is available for public distribution through authorized channels. Example: newsletters, brochures, advertisements and advertising related to the products and services offered by **Iris360** among others.

6.3 INFORMATION MANAGERS

- **Administrators or Custodian:** Individuals or departments that provide information services of different kinds. The custodians do not need to know the information to carry out their work, they only process it, manage its storage, and make it accessible
- **Owner:** Individual responsible for an application that uses information systems to provide services that support one or several operational areas or businesses. Also responsible for ensuring that controls are implemented to reduce the associated risks. Has the delegation to authorize access to information.
- **User: Iris360** associate who creates, reads, introduces, changes, or deletes the information stored in a Computer Systems. To acquire a user profile, authorization is required from the Owner of the information.

7. RESPONSIBILITIES REGARDING INFORMATION SECURITY

The Information Security Policies, as established by **Iris360's** Board of Directors and the Senior Management**,** always become the responsibilities of the Users,

Any security violation or breach can cause the Company enormous economic damages. Therefore, Users must be aware that information security is everyone's responsibility; and it is vital they know and respect the policies that the organization adopts on this matter.

The responsibilities regarding **Iris360's** information security are defined, shared, and published. Acceptance by all employees of the organization is mandatory and required to start and remain as an employee.

7.1 RESPONSIBILITIES OF THE INFRASTRUCTURE DEPARTMENT

- Apply and enforce the Information Security Policy and its components.
- Provide physical, logical, and procedural security measures for the protection of all digital information.
- Manage the access rules and attributes to computer equipment, information systems, applications, and other sources of information.
- Analyze, apply, and maintain the security controls to ensure data and information managed by the Company are duly protected.
- Resolve, in agreement with the areas and the owners of the information, any conflicts that arise from the information within the organization. This includes the possible information access methods, data produced by information processed through any application or system, data input to applications, and data that is an integral part of the application support.
- Establish, maintain, and disclose the technology services policies and procedures throughout the company in accordance with the best practices and Iris360 guidelines.
- Determine the strategies for the continuous improvement of the technology services and the optimization of resources.
- Direct all investigations into incidents and problems related to Information Security, as well as recommend pertinent measures.

7.2 TECHNICAL SUPPORT RESPONSIBILITIES

- Guarantee service availability and schedule or inform all the users about any problem or maintenance activity that may affect the normal utilization. Managing user access according to the requests received and following the established procedure.
- Provide the necessary support to users through the help desk channel currently implemented in the company.

7.3. INFORMATION OWNERS RESPONSIBILITIES

- Information Owners include all area directors, managers, and coordinators where information is generated, processed, and maintained in any appropriate media.
- Classify the information that is under their administration and/or generation.
- Authorize, restrict, and limit the users access to information according to their roles and responsibilities.
- Determine the information retention time jointly with the areas that are responsible for its protection and storage according to the

Iris360 ‘s determinations and policies as well as the external entities, regulations, and applicable laws.

- Determine and permanently evaluate the risks associated with the information as well as the controls implemented to access and manage the communication of any anomaly, or improvement to users and the custodians.
- Inform all Iris360 employees about the requirements of this policy and obtain acceptance.

7.4. INFORMATION USERS RESPONSIBILITIES

- Know and apply the appropriate policies and procedures regarding information management, Hardware, and Software.
- Keeping **Iris360** confidential information as such by preventing access by unauthorized persons or the improper.
- Be able to explain and assume responsibility for all activities performed through access using the assigned username and password.
- Meticulously protect passwords and prevent them from being inadvertently seen and used by others.
- Select a secure password that has no obvious relationship with the user, their relatives, the work group, or other similar relationships.
- Inform superiors about any policy violation user becomes aware of, any security incident, or suspicious event that could compromise the security of **Iris360** and its computer resources such as virus, intruders, modification or loss of data, and other unusual activities.
- Propose information security measures that make **Iris360’s** operations more secure.
- Use only the information necessary to carry out the assigned function, according to its Position Profile.
- Manage the information and be accountable for the use and protection of it.
- Protect the information to which accessed and processed, to avoid loss, alteration, improper destruction or improper use.
- Comply with all the controls established by the owners of the information and the custodians thereof.
- Protect the data stored in the computer equipment and information systems from inadequate destruction or intentional or unjustified alteration or disclosure.
- Protect the computer equipment, communications, and other technological devices assigned. Establishing connectivity and exchanging information with external networks, individuals, or companies require CEO authorization.
- Use only authorized software that has been legally acquired by **Iris360.** Installation or use of software not directly supplied by Iris360 is prohibited.
- Accept and acknowledge that, at any time and without prior notice, the General Management of **Iris360** may request an inspection of the information under its charge regardless of its location or storage. This includes all data and files in corporate emails, corporate website, and
- social networks owned by the organization as well as the network, computers, servers or other storage facilities of the organization. This review may be required to ensure policies compliance.

8. INFORMATION SECURITY POLICY GUIDELINES

8.1. USE OF WORKSTATIONS

The User is responsible for keeping the assigned Hardware properly identified for inventory control purposes. The responsible Area must maintain the inventory records updated.

- It is forbidden to use the Information, Hardware and Software, to perform activities other than those strictly related to Iris360’s business activities.
- It is forbidden to move Hardware, relocate it, or take it outside of **Iris360** premises without written authorization signed by the responsible party.
- It is forbidden to install and use unauthorized Software or illegal software on **Iris360** equipment. Only legal and official software can be installed and used. Likewise, it is forbidden to modify the Hardware and Software configuration established by the Infrastructure and Support Department. It is also not allowed to make copies of the software for personal purposes.
- It is forbidden to install on **Iris360’s** Hardware and software owned by the user, unless it has been rigorously checked and approved by the Infrastructure and Support Management.
- The User is responsible for periodically saving the information when using the Hardware to prevent a power outage or other failure from losing the information. For this purpose, **Iris360** has defined the use One Drive as a backup site; this tool is available on the Microsoft

Office 365 platform acquired by the Company.

- The User is responsible for having a screen saver with password to prevent other people from accessing resident files. Likewise, whenever possible, the Hardware must be installed in such a way that it does not allow visitors or strangers to the Company to have access to any type of information whether on screen, printer or any other device.
- The User is responsible for turning off or blocking the Hardware assigned to him when he must leave his workstation for periods of time exceeding one (1) hour.
- It is the responsibility of the Human Resources Department, as soon as an employee leaves Iris360to notify Technical Support to take all appropriate actions.
- The User is responsible for keeping the hard drive organized and saving in it only the files needed to carry out the assigned duties.
- The Technical Support area is responsible for deleting Confidential Information contained in equipment assigned to a user before shipping it outside the Company for repair.
- It is forbidden to have laptops, CPUs, or any other equipment property of the user at the work place, unless prior authorization has been granted.
- Access to **Iris360** information assets is prohibited to third parties unless previously authorized by Senior Management.
- It is the responsibility of the Users to identify and report to their supervisor the use of any
- unauthorized Hardware and Software, = as well as the loss of any equipment.
- The Hardware should not be left unattended at any time.
- It is the responsibility of the User to avoid the deterioration of the Hardware and to comply with the following basic rules:
- No eating or drinking near the Hardware.
- Do not place heavy objects on the Hardware.
- Do not place the Hardware on unstable surfaces and/or exposed to being unintentionally hit.
- Do not open the Hardware. If necessary, this work will be carried out by the Technical Support Area.
- It is the responsibility of the Users to keep their work place always clean, as well as their Hardware.
- Keep the cables in good condition, organized, and correctly connected. There should not be any type of cable tension or tangling.

8.2. USE OF PASSWORDS AND USERIDs

Assignment of userids, and passwords is a privilege granted by **Iris360** to its employees to access technological resources such as platforms and information systems that allow the operation, inquiry, and safeguarding of organizational information.

All the access accounts to the technological platforms, as well as to information systems and applications, are owned by the organization. For purposes of this guideline, two account types are defined:

1. **Information System User Account:** These are all accounts that are used by users to access the information systems. These accounts allow access for inquiry, modification, updating, or deletion of information, and are regulated by the user roles in each Information System.
2. **Information System Administration Account:** Type pf account that allows the System administrator, technology platform, or database to perform specific user tasks at the administrative level, such as: adding / modifying / deleting user accounts.

Below are the guidelines that must be met by any **Iris360** employee**:**

i. All passwords, regardless the type of account, must be changed at least every 3 months.

ii. All passwords must be treated confidentially.

iii. Passwords may in no way be transmitted by email or by instant electronic messaging services.

iv. Avoid mentioning and typing passwords in front of others.

v. Avoid revealing passwords in questionnaires, reports or forms that are visible on the screen in any of the processes in which they are used (connection, usage, etc.).

vi. Avoid using the same password to access operating systems and/or databases or other applications.

vii. Activation or use of password autofill features is prohibited.

viii. It is the responsibility of the technical area to assign a unique userid and it is the responsibility of the user to create a complex password of at least eight characters that complies with the minimum rules of:

1. Do not use personal information.
2. Do not use the same password for all equipment.
3. Combine uppercase and lowercase letters.
4. Combine letters and numbers.
5. It is prohibited to assign generic or universal user identification codes. Its use is restricted to automatic processes that are carried out by systems and that cannot be changed by personalized users.

ix. It is never authorized to assign userids to people outside of **Iris360.**

x. Administrator passwords must never be shared.

xi. It is responsibility of the User not to save password in a legible form in files on disk; neither should it be written on paper, left at places where can be easily found, or share or reveal it to any other person.

xii. It is the User's responsibility to immediately change their password when they have sufficient indication or reason to believe that it has been compromised.

xiii. It is the responsibility of the User not to use passwords that are identical or substantially like previously used passwords.

xiv. The initial password issued to a new user should only be valid for the first session. It is the User's responsibility to change their initial password in this first session.

xv. The consecutive number of unsuccessful attempts to enter the User's password is limited to three (3); after the third and last attempt the involved account is blocked.

xvi. It is the responsibility of Human Resources that as soon as an employee leaves **Iris360** to notify Technical Support to proceed with the cancellation of his user identification codes and Password.

xvii. If it is detected or suspected that the activities of a user account may compromise the integrity and security of the information, access to said account will be suspended and will be reactivated only after taking the necessary actions.

xviii. **The Infrastructure Team Leader** should have a file that lists sensitive passwords for the administration of information systems, technology platforms and databases. This file must rest in the Management System defined by the Company with visualization permits for the Internal Administration and Management.

8.3 ANTIVIRUS

Antiviruses are programs which objective is to detect or eliminate computer viruses, helping to protect computers against most viruses, worms, trojans and other unwanted invaders that can infect it. As time goes by, the emergence of more advanced operating systems and the Internet, antivirus programs have evolved towards more advanced systems that, in addition to searching for and detecting computer viruses, block them.

Iris360, to protect all its equipment, provides the necessary antivirus licenses. However, this will not be enough unless precautions are taken by the users.

Below are the guidelines that must be met by all **Iris360** employees:

1. It is responsibility of the User to use only the Antivirus software authorized by **Iris360**.
2. It is responsibility of the User to keep the Antivirus permanently active so that it constantly monitors all the operations carried out in the System. It is strictly forbidden to the User to deactivate the Antivirus.
3. It is strictly forbidden to the User to open or run files attached t emails unless they come from a recognized and secure source.
4. It is responsibility of the User to ensure the safety of the equipment assigned by the Company, so it is recommended to avoid using CDs, USBs or other storage devices that have previously been used in public PCs or doubtful activities, such as: educational centers, internet cafe, or even the user’s personal computer.
5. It is responsibility of the User to give immediate notice to Technical Support and to immediately turn off the assigned equipment now the presence electronic virus that is not eliminated by the Antivirus is detected.
6. For security reasons, messages that contain viruses will be immediately deleted without possibility of recovery.
7. It is the responsibility of the User to scan removable disk drives or flash memory before use.

8.4. **USE OF THE EMAIL SERVICE**

Electronic mail is a service based on the exchange of information through the network provided by **Iris360** to authorized.

Iris360, at its own discretion, can grant or deny access to electronic mail services to employees. Access includes the ability to write, send, receive, and store email messages and attachments. The CEO, Directors, Managers or Coordinators have the authority to request and grant access to this service for their teams.

The consecutive failure, after five (3) attempts, to access an email account causes the blockage of the account which can only be unblocked by request to Technical Support.

Type of Accounts:

1. **Personal Accounts:**
   a. Any **Iris360** employee may be authorized to obtain and operate a business email account. The userid of the email account will be created following the name.lastname@iris360.org format**.** If two or more people have the same user ID, the newest userid will contain the middle name as a differentiator (e.g. **firstname.lastname@iris360.org**).
2. **Work Group Accounts:**
   a. These accounts are created to address the needs of specific departments, regions, or Work Groups. They must be requested by the departmental manager and an administrator needs to be appointed. The email account id will be defined in the form name@iris360.org The administrator of the account will be responsible for the proper use and maintenance of the account.

Considerations for Sending and Transferring the Email Service

- The mailbox capacity of each collaborator's mail server is ***50 (fifty) GB***, including the recycle bin and sent messages. In certain occasions it is necessary that the users free space in their mailbox by eliminating the emails that are no longer needed, copying the messages to the local mailbox, and downloading the attachments to their assigned computer.
- Once the storage assigned by the user has been exceeded, the messages cannot be downloaded to their local mailboxes until the necessary space is released from the mail server. Each user is notified with a message when they are close to reaching maximum capacity.
- The maximum size of each email message must not exceed ***20 MB*** for sending and ***50 MB*** for receiving including attachments due to the limitations of the mailboxes. It is a good practice to compress the files to be sent through this service, to reduce the bandwidth demand in its transmission.
- If a message cannot be delivered to the recipient (connection problems, service not available, etc.), it will remain as pending delivery until the problem is solved.
- Messages destined to invalid domains (accounts) are rejected immediately to avoid erroneous addresses (for example, badly written) being accepted by the server as valid.
- Below are the guidelines that must be met by all **Iris360** employees:
  a. Users may never send massive messages through email; this type of messages can only be sent by authorized users. The authorized users are: CEO, Directors, Area Managers, and Marketing and Communications Coordinator. It must also be requested that these emails are not replied by the recipients because it can cause slowness in the communication channel or misrepresent the purpose of the information with additional comments.
  b. Use corporate email is exclusively for and limited to job related purposes.
  c. Ensure all the messages sent via email comply within the standards of respect and electronic communication protocol by drafting email messages in such a way that they are serious, clear, concise, and courteous.
  d. Prevent your email account from being used by third parties (customers, distributors or suppliers).
  e. Avoid the use of an email account that belongs to another user, if there is a need to do so in the case of absences or vacations, alternate mechanisms should be used, such as redirecting messages.
  f. Do not send messages from a user's email account with another's signature.
  g. Do not attempt to access and / or access without authorization to another email account.
  h. Do not engage in activities or massive broadcast of messages that may cause congestion or interruption in the communication services of **Iris360** or the normal operation of the electronic mail services.
  i. Maintain or file the messages sent and / or received for documenting to third parties (internal or external) the execution of operations

or actions.

j. Periodically delete messages that you no longer need from your storage devices. This reduces the risks that other users may access that information; and in addition, disk space is released.

k. No **Iris360** employee is authorized to monitor e-mail messages, except for the Internal Auditing area or an area previously authorized by the CEO. Authorized monitoring is carried out to ensure compliance with internal policies in cases of suspicious or unauthorized activity, investigations, and other reasons defined by the CEO; in these cases, **Iris360** is not obligated to request any authorization from the User involved.

l. All messages sent via email belong to **Iris360** and the company reserves the right to access and disclose messages sent for any purpose.

m. Do not engage in the broadcast of "thread messages", in pyramid schemes or propaganda inside and outside the organization.

n. Do not make unauthorized attempts to access another corporate email account.

o. Do not disclose, publish, or send sensitive information of Iris360 to external people or organizations without authorization through unsafe channels (encoded) such as Internet and / or public use email accounts (Gmail, Hotmail, Yahoo, etc.). Electronic mail is subject to the same laws, policies and practices that apply to the use of other means of communication, such as telephone services and print media.

p. Do not download, send, print or copy documents or content against copyright laws.

q. Do not download any software or file without taking precautionary measures to prevent virus access in networks and computer equipment.

r. Do not use defamatory or rude expressions against individuals. Messages sent through this service may not contain insidious, offensive, obscene, vulgar, racist, pornographic, subversive, or other material that may be offensive.

s. Avoid sending SPAM emails of any kind.

t. Avoid forwarding emails with PHISING content.

u. Do not use pseudonyms and send anonymous messages, as well as those that give titles, positions or unofficial functions.

v. Do not use email for commercial purposes outside the organization.

w. Do not use public mail for the reception, sending or distribution of sensitive or confidential information belonging to **Iris360**.

x. Do not configure and connect email clients with social networking sites or RSS feeds that are not authorized by the organization.

y. Except for the Infrastructure staff, no employee should send files with extension .exe, .pif, .scr,

z. .vbs, .cmd, .com, .bat, .hta, .dll because these types of extensions are prone to be used for virus propagation.

aa. Do not send multimedia contents (video or audio) with extension .wav, .mp3, .mp4, .mpeg,

ab. .wma, .wmv, .mov, .asf, .flv since these documents are very heavy and slow down the network of communications.

- Inappropriate use or abuse in the email service causes temporary or permanent deactivation of accounts. The deactivation of the account entails the impossibility of accessing the mail messages that are at that moment in the server and the impossibility of receiving new ones until it is not activated again.

8.5. USE OF THE INTERNET / INTRANET SERVICE

- The Internet / Intranet service is of great importance. Access to the Internet/Intranet service is a privilege granted by **Iris360** to its employees and carries responsibilities and commitments for its use. It is expected that the users of this service practice appropriate utilization, confidentiality, and ethical criteria.
- Each Director, or Area Coordinator has the authority to grant and request the access to this service for their teams, according to the current procedure. Access to this service is done through the platform that the organization uses, which in this case is, the Internet browser installed on each machine.
- Below are the guidelines that must be met by any employee of **Iris360:**
- Use this service exclusively for work purposes.
- Keep standards of respect, confidentiality, and ethical criteria.
- Download documents or files taking precautionary measures to prevent virus access to networks and computer equipment.
- Protect the copyright of the information obtained through this service. It is recommended to quote the source (web page) in the documents or reports generated with information obtained by this means.

- Do not access online gaming or betting sites.
- Do not access sites to disclose, download or distribute movies, videos, music, real audio, webcams, online stations, etc.
- Do not access and/or download pornographic or offensive material.
- Do not use software or instant messaging services (chat) and or access social networks not installed or authorized by the Organization.
- Do not share information on **Iris360** websites classified as sensitive or confidential.
- Do not use this service for the reception, sending or distribution of sensitive or confidential information of **Iris360** through services and public mail accounts.
- Do not make unauthorized attempts to access another user account of this service.
- Do not upload, download, send, print or copy files, software or content against copyright laws.
- Do not use the Internet/Intranet service for commercial purposes unrelated to the organization.
- Do not attempt or modify the configuration options and/or security parameters of the browsers installed by **Iris360**.
- Do not intentionally interfere with the normal operation of any website or Internet portal.
- Do not buy or sell personal items through websites or online auctions.
- Do not access multimedia content sites (videos, music, online stations, etc.) due to the high consumption of communications channels.
- Do not publish or send personal opinions, political statements, and issues not specific to the organization, aimed at employees or the public in general, from the official sector, from other companies and organizations, through this service.
- Do not download, install and configure browsers other than those allowed by the Infrastructure and Support Department.

8.6. USE OF INSTANT MESSAGING SERVICE

This service is provided by **Iris360** to its employees, with the purpose of facilitating communication throughout the organization, regardless of physical or geographical location.

As a tool for virtual conferences it allows sharing computer desktops and the resident applications, therefore its use is mandatory for real-time presentations, remote training, web conferences and online meetings. Access is done through the platform that the organization has allocated for this case the email platform.

Service users should consider that instant messages can be saved. One of the parties participating in the conversation can copy and paste the entire conversation into a text document. This instant messaging service even allows you to archive complete messages and record conversations.

Below are the guidelines that must be met by any employee of **Iris360:**

- Use the organizational instant messaging service exclusively for work purposes.
- Transfer files that do not have **Iris360** sensitive or confidential information. It must be previously confirmed that any file to be sent is virus free.
- Refrain from sharing information or personal data through this service. It is not recommended to include personal information such as passwords or credit card numbers, bank accounts and even a confidential telephone numbers.
- Share concise, brief and truthful messages through this channel.
- Keep your status updated in the system so that other users know whether they are available and whether they can contact you.
- Refrain from using the organizational instant messaging service for extensive personal conversations.
- Do not express defamatory, offensive, obscene, vulgar, racist, slanderous and sexual opinions at all. This can compromise the reputation and credibility of both the personal and the organizational
- Do not use instant communications for political, religious or commercial purposes.
- Do not perform any type of harassment, defamation, slander, with intent to intimidate, insult or any other form of hostile activity.
- Do not share confidential information about the company or its associates through this channel.
- Do not share documents or files that are unrelated to the operation of the organization.
- Do not download, install and use instant messaging systems other than those defined by **Iris360**, except for those previously authorized by the CEO for specific cases.

- Inappropriate use or abuse in the instant messaging service will cause temporary or permanent deactivation of the accounts.
- It is illegal to record conversations without permission from all the participants in a conversation.

8.7. USE OF EXTERNAL STORAGE DEVICES

The use of storage media external to those available in the different computing equipment, shared network units and servers of **Iris360**, is a tool that is used for the rapid and direct transfer of information among the employees of the organization, which at the same time can expose confidential and sensitive information of **Iris360**.

Iris360 is aware that this type of tools are very useful for the protection and transportation of information but they also allow the extraction of information without leaving a physical trace or record; for this reason **Iris360** defines the limitations regarding the use of External Storage Devices to ensure that proprietary information, acquired or placed in custody of **Iris360** is not subject to leaks, unauthorized use, modification, disclosure, or loss and that all information remains adequately protected according to its value, confidentiality and importance.

The use of external storage devices is allowed in **Iris360** for employees of the organization, to facilitate the sharing and transportation of information that is not classified or reserved by the organization within the rules and responsibilities of the institutional information management policies.

The storage devices for external use include the units that can be connected as a USB memory, by means of a data cable, through a direct wireless connection to any **Iris360** computer equipment. Among these, you can find but are not limited to:

- USB Flash Memory
- MP3 / MP4 portable players
- Cameras with USB connection
- iPhones / Smartphones
- SD Cards / Mini SD Cards / Micro SD Cards
- PDAS / Tablets
- Devices with Bluetooth technology
- Compact Flash cards
- Hard drives for external use

From virtual personal storage units via the Internet, such as: SkyDrive, Dropbox, Rapidshare, GigaSize, MediaFire, 4shared, etc. Only OneDrive is authorized, being one of the benefits available in the current electronic mail platform acquired by the organization at corporate level.

Below are the guidelines that must be met by any employee of **Iris360:**

Use in a responsible manner the information you are responsible for and the external storage devices that you use to transport said information.

Ensure that external storage media are free of malicious software, spyware or viruses for which you must perform a verification of these devices every time you are connected to an organization's computer by means of the protection software provided for that purpose.

Do not store or transport sensitive or confidential information of **Iris360**.

Do not execute any type of program not authorized by the organization from any of the storage units mentioned.

Do not download any file without taking precautionary measures to prevent virus access in networks and computer equipment.

Do not use mechanisms and systems that try to hide or impersonate the user ID of any of these storage media.

Do not use external storage devices in order to store or expose sensitive or confidential information of users or employees of the organization.

The Infrastructure Team and Technical Support may at any time and in any area of the organization operate, store, acquire or withdraw external storage devices that allow them to guarantee the security of **Iris360** information.

8.8. USE OF CLEAN DESKTOPS AND SCREENS

Iris360 defines the necessary mechanisms that must be applied in the organization in order to protect the physical information at desks and

work stations, as well as the digital information stored in the computers and technical infrastructure available to all employees for the normal development of the activities.

The policy of clean desktops and screens is extensive to all employees, of **Iris360** and supports the security of sensitive and critical information.

This guideline is defined in the proper and orderly use of the work areas from the physical and technological point of view. For its definition and application, it is defined as follows:

Desktops:

- Desks and work areas should be organized, meaning that the documents with sensitive or confidential information should be protected, keeping them out of sight or within the reach of outsiders.
- As far as possible, documents with sensitive or confidential information must be kept under lock and key during non-working hours.
- The removal of documents with sensitive or confidential information from the organization should be avoided and, if necessary, it should be provided for their protection outside of Iris360 and their prompt return to it.
- The reception, flow of physical documents in the organization must be controlled by registering their recipients from the point of correspondence.
- The photocopying of documents outside normal working hours and outside the organization's facilities must be restricted.
- When printing or photocopying documents with sensitive or confidential information, they must be immediately removed from the printers and should not be left unattended on the desks.
- You should not send or receive documents classified or reserved by Fax.
- It is the responsibility of the user to not reuse paper that contains sensitive or confidential information. If you find information of this nature in the printing area, you must notify it.

1. **Screens:**
    - Computers or work stations must be blocked by users when they leave, and they must be unlocked through userid and password assigned to access them. It is the user's responsibility to ensure that the equipment has adequate protection.
    - The virtual work areas "screens" of the computer must have the minimum visible icons, limited to the necessary accesses for the execution of work related activities.
    - Digital documents should be organized in folders and avoid keeping them visible on computer screens.
    - When leaving the office, employees must turn off the computers. Active sessions must be terminated when the user finishes the scheduled activities.
    - **Infrastructure Team and Technical Support** determine an automatic configuration in all computing equipment, so that the screen saver of the computer is activated, blocking access to the computer when an inactivity of 15 minutes occurs. These can be used again by users when re-authenticating through assigned users and passwords.
    - The wallpaper of each computer is unique for all work stations and for all users and corresponds to the design sent by the Marketing Department. It can only be changed by **Technical Support** and at the request of the Marketing Department.

8.8. **REMOTE CONNECTIONS**

Iris360 defines the requirements and cases in which remote access is granted to the technological platforms, and the security measures that are established for the protection of the information that is accessed remotely.

The remote connections policy is extensive for all employees of **Iris360** that require and are authorized to access organizational servers through VPN tools for the performance of their activities at non-business hours or from locations other than the company offices.

Below are the guidelines that must be met by any employee of **Iris360:**

- Remote access to all information assets and equipment is restricted; accesses must only be allowed to authorized personnel and for established periods of time, according to the tasks performed.
- To establish remote connection to **Iris360** technological platform approvals are required. User must comply with the conditions of use established for such connections.
- Addresses must be kept confidential (IP addresses or Web addresses) as well as the credentials that have been granted for their protection.

- Maintain the confidentiality and protection of the information to which they have access outside the company's facilities.
- Apply antivirus tools on your personal computers, as much as possible, to provide greater protection to the files and information they are managing.
- **Notify Technical Support** of any possible abuse or attempted violation of both access and credentials delivered.

Who we are

Iris 360 is a next-level technology company.

We specialize in technology solutions that solve business problems and make life easier for our clients. Our team is highly experienced in understanding the needs and goals of businesses, across all aspects of day-to-day business operations.

Looking for more information?

Get In Touch

helpdesk@iris360.org

Our team will respond to you within 24-48 hours.

iris360
Our Plan is Our Promise