Digital Security Policy
Territoria.

Territoria, comprised of El Olivar SpA, Territoria SpA, Territoria Asset Management SpA, Territoria Apoquindo S.A., Territoria Santa Rosa SpA, SIR Desarrollo Inmobiliario II SpA and Fondo de Inversión Privado Apoquindo, is committed to promoting sustainable urban development, creating value for all its stakeholders. To achieve this objective, its social responsibility includes unrestricted respect for human rights, full compliance with its labor obligations, care for the environment and the building of virtuous relationships with the community.

Any person who considers that any of the principles or rules contained in this document have been violated may report the fact confidentially and anonymously to any of the following means:

- E-mail: mvalles@territoria.cl
- Whistleblower channel: http://denuncias.mut.cl/

Index

a) Objective

The Digital Security Policy (hereinafter referred to interchangeably as "the Policy") of Territoria (hereinafter also "the Company" or "the Company") aims to protect the people working in the company, protect the company's resources, and maintain order and security within the company. This policy contains a summary of the principles in use at Territoria, a list of relevant digital resources, writing conventions, and a brief glossary of terms and abbreviations used throughout the document.

b) Scope

The scope of the Policy covers all of the Company's activities, and compliance with it must be ensured in each of its assets. This policy is applicable to all employees, who have the obligation to report any fact that may constitute a violation of the principles or rules contained in it.

An institutional digital resource is any website, database, digital directory, e-mail lists, intranets, applications, or in general any software or digital object that belongs to the company, and that is used and shared between two or more users. The digital institutional resources that are currently available are the following:

- Institutional e-mail: E-mail is the main means of communication between employees. There are two applications for accessing institutional e-mail:
  - Microsoft Office 365: Microsoft 365 is our productivity platform with tools such as Microsoft Teams, Word, Excel, PowerPoint, Outlook, OneDrive and much more.
  - Microsoft Outlook: This is the primary and preferred means of accessing institutional email. It requires the use of a computer provided by the company, and the installation of MS Outlook software. To access e-mail through this medium, a user name and password are required.
- Outlook Web: This is an alternative means of accessing institutional mail. It does not require a computer provided by the company; it does require a browser and authentication through a user name and password each time the application is accessed. This resource can be accessed at the following URL: http://outlook.com
- Sharepoint Sites: Institutional web site with diverse information. A user name and password are required to access this resource.
- BUK: Institutional web site with information on salaries, salary settlements, vacation requests. To access this resource a user name and password are required.
- Softland: ERP system used for accounting, collection, financial and HR management of the company and its clients. Access to this resource requires a user name and password and the assignment of a user profile.
- Solutions Malls: System used for the management and administration of leasing contracts for shopping malls. Access to this resource requires a user name and password and the assignment of a user profile.
- Ticket System: System based on the Zendesk platform used for the management of internal requirements.

- Adobe Creative Cloud: Adobe Creative Cloud is an Adobe service that gives users access to graphic design, video editing, web design and cloud services.
- Autodesk: Suite of design programs.
  - AutoCAD LT. / AutoCAD.
    AutoCAD is a computer-aided design software used for 2D drafting and 3D modeling.Revit. / AutoCAD Revit LT Suite.
  - Revit is an intelligent design and documentation software, which allows the development of the BIM (Building Information Modeling) methodology; facilitating the design of projects and work processes in this environment.
  - BIM Collaborate Pro.
    Autodesk BIM 360 is Autodesk's collaborative platform in the cloud, which allows you to manage and share documents, plans and models of BIM projects and interact with the different actors involved in the life cycle of a project.

Likewise, the Company shall extend its obligations and require compliance with them to any person with whom it enters into an act or contract, regardless of its nature, whether they are suppliers, lessees or any other. To this end, clauses shall be established to sanction non-compliance, which may include the termination of the act or contract.

Finally, Territoria will promote its compliance among the other interested parties, through suitable dissemination mechanisms.

c) Principles

The Company has adopted the following 4 principles due to their importance in relation to the development of its activities and business, assuming the commitment to respect them and promote their compliance by all its stakeholders.

For the purposes of this Policy, stakeholders are understood as all those who have a direct or indirect interest in Territoria's business, such as customers, employees, tenants, suppliers and contractors, other related companies or companies that have commercial relations with the Company, the financial community, trade organizations, the media, authorities, local communities, among others.

Principle 1: Acceptable use of electronic equipment.
Describes what constitutes acceptable use of institutional electronic resources: desktop computers, laptops, fixed telephones and cell phones.

General rules

- The equipment provided by the company to each user may be owned by the company or may be leased under an operating lease. In both cases the company is the owner of all the information stored in the equipment provided by the company. The company will keep a record of each person to whom one or more electronic equipment is assigned.

- Each user is responsible for physically protecting both the equipment assigned to him/her and the information stored therein, to the extent that this protection does not endanger his/her physical integrity (for example, in case of robbery with intimidation or violence).
- Each user is responsible for protecting access to each computer assigned to him/her through a password, in accordance with the provisions of the policy.
- Each user may access, use or share company information only to the extent necessary to perform his or her job.
- Each user is responsible for exercising common sense regarding the use of institutional equipment for personal activities. In case of doubt, a user should ask his or her direct supervisor, or in his or her absence, the IT manager.
- For security reasons, IT personnel may remotely monitor the activities performed by each user through the institutional equipment assigned to them. This monitoring in no case is intended to monitor the actions of a user, but to detect malicious software that could jeopardize the company's information or the identity of the company's users.

<u>In case of theft, robbery or loss of equipment:</u>
In the event of theft, theft or loss of institutional equipment, the user to whom the equipment was issued must report the event within 6 hours of it occurring, or of first noticing its absence, even if the event occurs during non-business hours.
All theft, robbery or loss must be reported through one of the following options:
(a) Via email soporte@territoria.zendesk.com
In case of reporting a theft, robbery or loss via email or phone call, the following must be reported:
(a) Name of the user making the report or his/her user name.
b) In case of theft, the date, time and place of the event must be reported.
c) In case of theft or loss, date and time when the equipment was first noticed missing, and the estimated date and time of the last use of the equipment.
d) Circumstances under which the theft or loss occurred.

Important: In case of theft or robbery of equipment, it is the user's responsibility and obligation to report the theft to the nearest police station by means of a report, which must be submitted to the IT area.

<u>Specific rules on the use of cell phones</u>
The rules contained in this section are applicable to those users who have been assigned cell phones (smartphones), and must be complied with in addition to the rules and prohibitions in the rest of this policy.

1. Smartphones provided by the Company to certain users are for the exclusive purpose of maintaining a dedicated line of voice and data communication with such users.

2. Upon receipt of a cell phone, each user will be made aware of both the Acceptable Use Policy for Electronic Equipment (p. 5) and the Acceptable Use Policy for Email and Networks (p. 8).

3. The following communications applications may be installed on each cell phone assigned to company users:
- WhatsApp, developed by WhatsApp Inc. for non-confidential messages.

4. If a user needs to use an application other than those indicated in the previous point, he/she may request in writing to the IT manager that such application be installed on his/her phone, justifying the need. The IT manager may or may not authorize the installation of the application, based solely on IT security criteria. Such authorization must be in writing.

5. Users who have access to email through their assigned cell phone must strictly follow the Acceptable Use of Email and Networks policy (p.8) for the use of such email.

6. Users who receive a company-provided phone must not:

- Install applications on the phone.
- Uninstall or modify applications already installed on the phone.
- Modify the phone's settings in any way.
- Add personal contacts to the phone, either in the applications identified above or in the phone's native contacts application.
- Allow anyone else to use the phone, including family and friends.
- Reinstalling the phone's operating system with elevated privileges (rooting or jailbreaking), or asking someone else to do so, regardless of whether or not this activity is paid for.

Prohibitions

The activities listed below are generally prohibited to all users of the company. This list is not intended to be exhaustive, but rather to provide guidelines on those activities that are considered inappropriate. Any exceptions must be expressly authorized by the IT manager.
The following activities are prohibited for all company users:

1. Downloading or installing software, plug-ins, add-ons or any other proprietary application on institutional electronic equipment, if the user or the company does not have the corresponding license.
2. Downloading, installing, storing or forwarding malicious software, such as viruses, worms, Trojans, e-mail bombs, etc.
3. Connecting any personal electronic equipment to the institutional network; specifically, it is strictly prohibited to connect a wireless router or personal switch to any company network point. In justified cases, a user may connect his or her personal computer to the institutional network, if he or she has prior authorization from the Security Officer. To request authorization to connect a personal electronic equipment to the institutional network, you must request authorization via e-mail: soporte@territoria.zendesk.com.
4. Installing or executing scripts or programs whose intention is to interfere with, disable or impede the normal operation of institutional networks, or other users' institutional equipment.

5. Executing any kind of monitoring of the institutional network that has not been expressly and previously authorized by the Security Officer, unless this monitoring is part of the user's regular work.
6. Installing any kind of software or application that allows circumventing or overriding the entry of passwords to access institutional equipment.
7. Storage devices:
   - Users must not use personal storage devices, all information must be stored in the shared folder area provided for this purpose.
   - It is not permitted to store company information on storage devices, they should only be used to facilitate the carrying of functional information (e.g. Power Point presentations).
   - In general, the company will not provide pendrives or external hard disks or any external storage media, due to the risk they represent to the security of the information.
   - All removable storage media used outside the company's technological platform must be checked for the possible presence of viruses by scanning it with the antivirus installed on your computer.

Principle 2: Acceptable use of institutional e-mail and networks.
This principle describes what constitutes acceptable use of institutional e-mail and social networking through institutional networks; it also describes what constitutes acceptable use of institutional networks and bandwidth.

Standards:

I. Use of Institutional E-mail

Institutional e-mail is provided to a user exclusively to communicate with the rest of the users, and with people outside the company when their work requires it.

Institutional e-mail should not be used to create accounts in social networks, e-commerce sites, retail stores, or in general any kind of service provided online, except if this service is directly related to the user's work.

For security reasons, institutional e-mail is checked by automatic programs to filter out viruses, malware, spam, and other types of threats that spread through e-mail. Although institutional e-mail will not be read or reviewed by human beings, users' messages may be reviewed by automatic filters and flagged for further review by IT staff if the content of the message meets predefined risk criteria.

In no case, the user is authorized to modify the text of your email signature, nor its font, nor its size. Nor add any type of image or sticker. Any change of position in the e-mail signature will be made by TI once notified by the department of people and DO or their direct management.

II. Use of the Internet and social networks

A user can normally surf the Internet through institutional networks, exercising good judgment in deciding which sites to visit, and being frugal in terms of the bandwidth used. In this regard, the following is recommended:
a) Listening to music over the Internet is permitted, as long as it is done with a personal headphone system.
b) Avoid playing movies over the Internet; for example, through services such as Netflix or YouTube.

For security reasons, all sites a user visits may be monitored by automatic filters, and some sites may be flagged by automatic filters for review by IT staff.
by IT staff.

The IT area may partially or completely block websites or Internet addresses when:
(a) These addresses are on blacklists of any kind. The IT department may publish a list of those blacklists it uses to block websites.
b) These addresses contain pornography, or content that is defamatory or denigrating to any person; or racist or discriminatory content of any kind.
c) One or more of the general managers so request(s) for good reason(s).
A user may make use of his personal social network accounts or personal email through institutional networks, provided that:
(a) This use does not distract him/her from his/her usual work.
b) Does not disclose information related to their work or the work performed by other users of the company.
c) Your messages are not defamatory, denigrating, racist, or discriminatory to any other user of the company, or to people outside the company.
d) Do not make excessive use of the bandwidth made available to the company's users. What constitutes excessive use will be analyzed on a case-by-case basis by the IT area; in case of doubt, a user should ask the IT manager.

III. Company Representation

Any message from a user of the company through social networks is the sole responsibility of the user, and does not in any way compromise the position or opinion of the company or its representatives.

No user is authorized to send messages through social networks on behalf of the company, except for the highest authorities (Managers) and those expressly authorized by them.

IV. Prohibitions

The following activities are prohibited for all users of the company. Any exceptions must be expressly authorized by the Security Officer. It is strictly prohibited:

1. Using institutional e-mail to create accounts on online gambling services, pornographic sites, dating or matchmaking sites, or any other site whose use is against company regulations.

2. Using institutional networks to download, store, distribute, forward or transmit any material that infringes Law 17.336 on Intellectual Property and Copyright; for example, music, movies, television series, applications, books, images, photographs, etc.
3. Using institutional networks to download, store, distribute or forward any type of pornographic material, whether through images, audio, or video.
4. Using institutional e-mail or institutional networks to sell products or offer services of any nature.
5. Using institutional e-mail to send unsolicited e-mail (spam).
6. Using institutional e-mail or institutional networks to send messages to harass or sexually harass other people, whether or not they belong to the institution.
7. Modify e-mail signatures, as these must be authorized by your management and HR.

Principle 3: Use of passwords.
The selection and use of good passwords is an important part of an institution's security.
institution. A "good password" is one that is easy for the owner to remember, difficult for others to guess, and difficult to find out by automated means.
by other people, and difficult to find out through automatic means. A bad password can be guessed by others, and can allow those people to gain access to resources to which they should not have access. All users are responsible for choosing good passwords for the institutional digital resources to which we are provided access.

Standards:

I. Creation of access and profiles

When a new employee joins the company, he/she will be assigned a user name and role according to what is indicated in the "Check list of Software and Applications for Workstations", which establishes the technical requirements that the chosen candidate will require to develop his/her functions, such as computer, software, mail, intranet, access, among others, and must be delivered directly to the IT area for its management, with the authorized signature of the interested management. The interested management will be responsible for monitoring compliance with this process directly with the IT area, without HR intermediation for this purpose, the idea is that when the new employee enters to work, he/she will have all the necessary implementation to be able to develop his/her work.

II. Changes or extension of profile

A profile change or extension must be requested to IT by HR, when it corresponds to a change in the employee's area.
When a temporary extension of a user's profile is required, this request must be made by the direct boss of the area and notified via e-mail to IT, clearly indicating the new attributions and for how long they will be applied.

III. Creation of passwords

1. All institutional digital resources must be protected through a password. All passwords must be created following the recommendations for the digital world (page 18).

2. Sometimes, for reasons of good service, a user is assigned a temporary password that is communicated verbally or given in writing on a piece of paper. Any user who is assigned a temporary password must change this password the first time he/she accesses the corresponding digital resource.

IV. Password Protection

A password is always for personal use. A user should not disclose or share any of his or her passwords with other users, including assistants, secretaries, administrators, and family members of the user. This is especially applicable when institutional electronic equipment is used at the user's home, or when the user is on vacation, on leave, or away from his/her work station.

1. A password must not be shared or disclosed under any circumstances to persons outside the company, including the user's family members or persons living under the same roof as the user.
2. A password must be unique; that is, it must not be reused in any other digital institutional resource.
3. A password should not be stored on physical or digital media, such as unencrypted text files, USB flash drives, external hard drives, CDs or DVDs. In particular, a user must not use the password storage functionality offered by browsers.
4. A password must not be sent or communicated orally, via telephone, physical mail, memorandums, memos, offices, circulars, e-mail, text messages (SMS), photos, images, or any other physical or digital means.
5. A password must not be written down or kept anywhere in an official's office.
6. For a person to find out a user's password through any method constitutes unauthorized access to institutional digital resources. Any user who suspects that one of his or her passwords may have been found out or spied on by others should:
   - immediately change their password.
   - report the incident immediately to the IT manager. To report the incident, the user must follow the procedure established in the Digital Security Incident Response policy (page 20).

V. Delegation of identity

In the event that a staff member, due to the nature of his/her position, must delegate part of his/her identity administration to other staff members, he/she must request support from the IT area in order to carry out these actions without having to reveal his/her password to other people.

Principle 4: Response to digital security incidents.

Anyone within an institution today can suffer a digital security incident. Most of the company's policies and best practice guidelines are dedicated to preventing the occurrence of digital security incidents. However, it is essential that in the event of an incident occurring, the person or persons who know about the incident are able to recognize and report it, so that together we are able to remedy the consequences of the incident

Standards:

I. Preventing Incidents

All users must know and practice the recommendations for the digital world (page 13), in order to prevent digital attacks on the electronic equipment assigned to them and on the institutional digital resources to which they have access.

II. Identify incidents

All users should be familiar with the contents of the Security Incident Identification Guide, in order to know how to identify the security incidents described therein.

III. Remedying Incidents

Any user who has identified a security incident in an electronic equipment under his charge must follow the following procedure:

If it is a desktop or laptop computer:

1. If the computer is connected to the network, unplug the network cable immediately. Do not turn off the computer.
2. If you have immediate access to the Internet through another computer, open the following URL, and follow the instructions there to report the incident on the corporate intranet in the IT section.
3. If you do not have immediate access to the Internet, immediately contact the IT Manager at +569 9144 1400 to report the incident.
4. If you do not have immediate Internet access or access to a telephone, get a computer with Internet connection or a telephone as soon as possible to report the incident.

Recommendations for the digital world

This chapter presents 7 recommendations for the institutional and personal digital world. These recommendations are aimed at company employees who must take special care to protect their information and the information of the company where they work; however, this chapter should be useful for everyone who wants to take basic digital security measures.

1. Take care of your passwords.

Passwords are nowadays the most used mechanism to access restricted access services. Although there have been many alternative proposals, it is very unlikely that passwords will be replaced in the near future.

A good password is one that is easy for the person who created it to remember, and difficult for anyone else to guess or figure out. Unfortunately, this is difficult to do because the most secure passwords are strings of randomly chosen characters, and these are very hard to remember. Even when we write them down, these passwords are so difficult to enter on a keyboard or smartphone screen, that we usually end up forgoing secure passwords and use passwords that are instead easy to remember and enter anywhere (such as "123456").

Some recommendations to take care of your passwords:

- **Recommendation 1**: Use different passwords for each digital identity (e.g. Work or Personal). According to a 2007 study, people have on average 25 accounts or sites that require a password, and we have on average 6.5 different passwords [7]. This means that, on average, we reuse the same password on about 4 sites.
- **Recommendation 2**: Use long passwords that are difficult for others to guess. In general, longer passwords are more secure for most everyday purposes.

2. Lock your computer/phone.

Faced with the above problems, a simple way to avoid the problem with both smartphones and computers is to lock them to prevent others from accessing it. All modern computers, laptops, tablets, and smartphones offer options to lock them and prevent others from accessing our devices. On Microsoft Windows computers, you can lock the computer by pressing the "Windows" and "L" (for "lock") keys; to unlock you use the combination CONTROL + ALT + DELETE, and then enter the same password as the user who locked the computer. On iOS (Mac) computers there are similar mechanisms to lock the computer.

- **Recommendation 3**: Lock your phone with at least a four-digit number.
- **Recommendation 4**: Lock your computer whenever you are away for more than a few seconds.

This is especially recommended for the workplace, where other people can sit and have access to my computer (not only work colleagues but also people who do not belong to the institution).

3. Data Network Security

a) Do not connect to unfamiliar wireless networks.

When you connect to a wireless network (Wifi), all your traffic passes through a small specialized computer known as a router. This computer, in addition to connecting you to the Internet (technically, to an Internet Service Provider or ISP, such as Claro, Entel, WOM, etc.), is primarily responsible for showing you the right sites. This computer is always under someone's control; and that person, company or public institution can decide (if they wish) to restrict your browsing in almost any way imaginable:

* It can show you other sites instead of the ones you want to visit,

* It can silently censor certain sites so that you do not visit them, or make it easier for you to visit specific sites,
* It can spy on your traffic and show you things based on that traffic,
* Etc.

In practice, the trust one can have in a wireless network is the same trust one places in the person, company or institution that controls the router. Therefore, the main recommendations on this are as follows:

- **Recommendation 5**: Before connecting to a wireless network, confirm the name of the network with someone at the institution.

For example, if you usually have a coffee at the corner store, ask the people who serve you at the coffee shop what the network name is before connecting. Stores such as Starbucks change the name of the network at each location from time to time.

b) Do not open e-mails or files from people you do not know.

E-mail is (and will continue to be for a long time) an important communication tool within institutions. One of the most complex problems of this tool, however, is that it requires little knowledge to impersonate another person, and to send mass emails with the purpose of deceiving others, or infecting their computers with malware (through attachments).
This is why one of the main recommendations is the following:

- **Recommendation 6**: Do not open e-mail from people or institutions you do not know.

Although this is not enough, in general it is a very good habit not to answer (and simply delete) emails from people or institutions that we do not know. How do we receive emails from people we know, but from whom we have not received mail before? For that, we should always first physically check with the person's e-mail address.

- **Recommendation 7**: Always check extraordinary requests with the person(s) involved.

What are the chances that our best friend, whom we haven't seen for a couple of months, had everything stolen while walking around Ukraine, lost his passport and money, and needs you to lend him $2,100 euros to pay the hotel bill?
The answer is: it depends on whether or not it is reasonable for the person in question to be traveling in Ukraine. This is a traditional email scam, and most likely some hacker has taken control of our friend's email account, and is sending emails asking for money to our friend's entire contact list. In any case, the best thing to do is to simply call the person on the phone, or locate them in some other way to confirm the veracity of the problem.

d) Implementation

This document must be implemented in accordance with current legislation, national regulations and standards, as well as international standards and those of each country where an asset is located, as applicable. This includes all provisions related to current labor, environmental, non-discrimination, and inclusion regulations, among others.

In the event of a conflict between the principles and rules defined in this Policy and any of these regulations, the provisions of the latter shall always prevail.

The monitoring and control of compliance with the Policy shall be the responsibility of the responsible area.

The Manager in charge of the Policy will report on the progress of its implementation to the Executive Team or respective Committee on an annual basis, as well as any situations of non-compliance detected and the corrective measures adopted as a result.

Plans, procedures, and/or implementation or improvement actions shall be periodically disclosed by the Company to its stakeholders via appropriate channels.

e) Complaints and claims

Anyone who believes that any of the principles or rules contained in this document have been violated may report the matter confidentially and anonymously through the following channels:

- Email csilberberg@territoria.cl
- Reporting channel: http://denuncias.mut.cl/

Complaints will be heard by the Crime Prevention Officer, when appointed, who will implement the procedure established in the Company's Code of Ethics and Conduct, thus safeguarding the anonymity and confidentiality of the complainant, as well as the principles and rules of due process.

f) Revision

The Policy will be revised periodically to ensure its suitability and effective implementation. All revisions shall be subject to approval by the Executive Team or respective Committee.

g) Dissemination

The General Manager shall be responsible for taking all the measures he/she deems appropriate to make the Policy known and train the different stakeholders, with special concern for the Company's employees, investors, tenants, and suppliers as well as regulatory bodies, local authorities, and the general public.

The content associated with this Policy must be disseminated in a way that guarantees non-discriminatory and respectful access by different cultures, without negatively affecting the most vulnerable groups, such as children, the elderly, and immigrants.

In addition, contracts and communications must be clear and simple, written in language as close as possible to that normally used by the people to whom the message is addressed. They must also abide by statutory legislation, without using evasive or improper practices; be exhaustive and not omit any

relevant elements that may affect decision-making; be made available on the Company's websites; and establish mechanisms to respond to the needs of people with disabilities.

h) Validity

This policy has been in force since it was approved and has not been modified to date.

i) Glossary

Browser: Software that allows you to view web pages. There are many different brands of browsers: the best known are Chrome and Chromium (from Google), Firefox (from Mozilla Foundation), Opera (from Opera Foundation), and Safari (from Apple). The Internet Explorer browser (from Microsoft) is being discontinued, and its use is not recommended. In its replacement use EDGE from the same manufacturer.

Personal contacts: With respect to a company user, this refers to contact data of people who do not have a work relationship with the user.

Personal accounts: All those email or social network accounts that belong to a company user, but are for private and individual use, and are not controlled or provided by the company.

Institutional e-mail: E-mail account assigned to a company user and managed by the company. Institutional e-mail addresses are always in the form of nombredeusuario@territoria.cl; for example, if the user "John Smith" has the user name jperez, his institutional e-mail will be jperez@territoria.cl.

Personal email: Any email account that belongs to a company user, but is provided by an external provider, not contracted by the company; e.g., Gmail, Yahoo, etc.

Institutional electronic equipment or Institutional equipment: Any electronic device that is the property of the company, and that is temporarily made available to a user to help him/her perform his/her work. For example, a desktop computer, a laptop computer, a cell phone (smarphone), a landline phone, a printer, a router, a switch, etc.

Personal electronic equipment: Any electronic device that is not assigned to a company user.

IT Area: Group of people who provide support services to company employees in the following activities:

- Facilitating the development, implementation and operation of technological projects.

- Installation and support of institutional electronic equipment, along with the networking of this equipment.

- Installation and administration of applications and programs on the above equipment.

Working hours: Monday to Friday, from 09:00 to 18:00 hours, except holidays.

Non-business hours: Any time that falls outside the definition of business hours.

Security Incident: Any event involving institutional equipment or networks that contravenes any of the company's rules.

Blacklists: Public lists of domain names, URLs or IP addresses that have been reported for distributing malware or sending spam. These lists are usually managed by security companies or large corporations (e.g., Google, Apple) to protect users who make use of their products or services.

Temporary password: A password that is temporarily assigned to access an institutional digital resource or service for the first time. Usually, a temporary password is communicated to the holder either verbally or in writing.

Institutional digital resource: Any website, database, digital directory, e-mail lists, intranets, applications, or in general any software or digital object that belongs or is leased to the company, and that is used and shared between two or more users.

Social networks: Facebook, Twitter, LinkedIn, Instagram, Pinterest, Tiktok and in general any other mass communication service on the Internet.

Institutional networks: All those networks and communications equipment owned by the company, which are used to communicate two or more users with each other and the Internet. This denomination includes network cables, network points, routers, switches, firewalls, ISP, and in general any other communications equipment in use in the company's facilities or in the commercial centers it manages.

User name: User name used to uniquely identify a user.

User or collaborator: Any person who works for the company, regardless of the type of employment relationship he/she has with the institution. In this document both terms are used interchangeably.

User Profile: Set of attributes assigned to a user name for its performance in the institutional digital resources, this user profile is directly established from the user's job description.