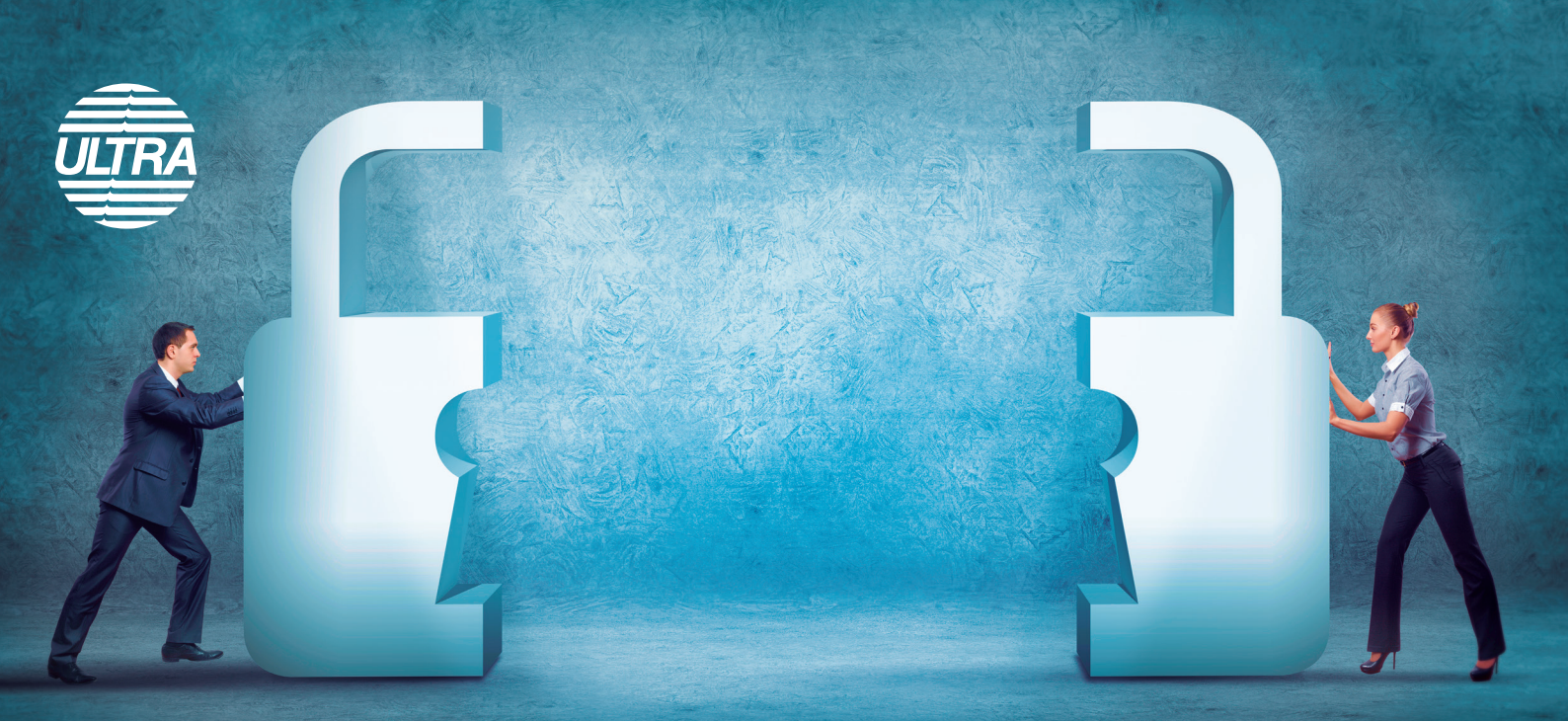

Information Security Booklet

Managing Committee for Information Security

Contents

Dear Employee,

The purpose of this booklet is to share some concepts related to Information Security. Apart from tips on how to handle the resources and the corporate information we deal with in our daily lives, this material seeks to emphasize the responsibility of all employees, interns, contractors, partners and visitors that access information from Ultra.

Protecting the information of the company for which we work is a duty of each one of us!

We hope this guide will help to clarify any doubts and can guide you on how to play the role of "key collaborator" for Information Security.

Enjoy your reading!
Managing Committee for Information Security

It is the protection of information (preservation of Confidentiality, Integrity and Availability) against various types of threats and seeks to ensure the continuity of the business, minimize damages and maximize the return on investments and business opportunities. Following, the definition of the three pillars that support Information Security:

Confidentiality:
Limits access to information only to duly authorized individuals.

Integrity:
Guarantees that information handled will keep all the original characteristics established by the owner of the information, including control of changes and guarantee of this cycle of life (creation, maintenance and destruction).

Availability:
Guarantees that information is always available for legitimate use.

Managing Committee for Information Security

Ultra has established an Information Security Committee which establishes standards and policies to both promote the idea of security and monitor risks and threats and avoids exploitation of security gaps.

Responsibility

All employees are responsible for ensuring the security of Ultra information according to the guidelines of the Information Security Policy and corporate standards.

Ultra's information is invaluable for the company and is considered an asset for the organization.

Access to information is controlled and limited to that necessary for the performance of activities and, to that that end, the following rules have been defined.

- ✓ The use of assets owned by the Ultra can be monitored.
- ✓ All Users are responsible for the assets to which they have access.
- ✓ Users must formally report the occurrence or suspected security incidents by opening a call with the Service Desk.

Ultra adopts safety guidelines for use of the resources available for use. Resource is understood any kind of asset, whether logical (software, systems) or physical (hardware), that stores, processes and/or transmits information.

Your password guarantees access to resources for which you have authorization. The password is personal, non-transferable, and the exclusive responsibility of the User and should be changed according to the rules of the organization.

Passwords should not be simple, to the point of discovery, or complex, have to be written down.

We recommend the use of strong passwords considering a combination of uppercase and lowercase letters, numbers, special characters, minimum length of six (6) characters and which do not derive from a pattern.

Below are some best practices regarding passwords.

Avoid:

- ✓ Name and surname, words found in dictionaries or reversed.
- ✓ Numbers of documents, phones, car plates.
- ✓ Dates that may be related to the client or family.

Recommendations:

- ✓ Make sure you are not being observed when entering your password.
- ✓ Do not write down your password, memorize it.
- ✓ Never share your password.

Suggestions: Set any sentence:

World Cup in Brazil in 2014

Use the first, second or last letter of each word of the sentence interspersed with numbers and special characters:

WCB&2@!4.

Information technology assets are all the devices and information necessary for the performance of their functions, for instance, workstations, servers, software, files, electronic mail, authentication devices and any electronic device or systems related to information technology.

- ✓ The use of assets is restricted to authorized Users only and must be returned in case of termination.
- ✓ Ultra recommends not storing private files in the company's assets.
- ✓ Work information should always be stored in network directories or in specific folders as they have security backup.

Clear Screen and Clear Workstation

We deal with various types of information, from simple newsletters to confidential information. Based on that you should always take care of your workstation, making sure not to show restricted or confidential information.

Whenever you have to leave your desk, ensure that any printed documents are appropriately stored and that your station is locked for access, preventing insider information from being viewed by unauthorized persons.

The electronic mail is a concession of Ultra and, therefore, may be monitored at any time for the purposes of Information Security and audit processes. Thus, everyone should secure its appropriate use.

Some good practices in using e-mail are:

- ✓ Do not use corporate e-mail address for personal purposes.
- ✓ All messages sent to addresses and external emails have a standard disclaimer.
- ✓ One should not send or file messages containing:
  - Subjects that cause harassment, disturbance to others or which compromise the image of the business.
  - Defamatory, discriminatory, obscene, unlawful or unethical subjects.
  - Images, audios or videos that are unrelated to professional activities.
  - Attachments with potentially dangerous (see guidelines on electronic mail).

The internet is a corporate resource available to Users for development of professional activities, thus it can be monitored for their use. Internet brings many possibilities of use, but to enjoy each one safely it is important that some safety procedures are followed.

- ✓ Do not access sexually oriented, profane, obscene, pedophilic, fraudulent, defamatory, racially offensive or illegal material.
- ✓ Do not download files that are not consistent with the business activities.

Granting access to social networks must be authorized by the area manager of the User who requires access for the performance of the function by means of called to the Service Desk and can be monitored.

The following recommendations should be followed in the use of social networks:

- ✓ When finding offensive comments relating to Ultra, any situation that may jeopardize the confidentiality of corporate information or the image of the organization, immediately report to the Service Desk stating the event.
- ✓ Never post addresses, financial data or document numbers.
- ✓ If the use is not related to your professional activities, always use a personal email and not the corporate email.
- ✓ Do not allow anyone to view your profile without your permission.
- ✓ Never post information owned by Ultra without prior authorization from your manager.
- ✓ Do not post subjects that cause harassment, disturbance to others or that compromise the image of Ultra.
- ✓ Choose carefully the information, videos and pictures that will be shared and do not post topics considered defamatory, discriminatory, obscene or illegal.

Systems are information technology resources used by Ultra Company to collect, process, transmit and disseminate data that represent information for the User and that contribute to the business process.

- ✓ The license for use of the systems is grated by Ultra to Users who require this resource to perform their duties. This access requires manager approval and its use is monitored.
- ✓ Sharing access credentials are not allowed. They are personal, non-transferable, and exclusive responsibility of the User.
- ✓ The criteria for the creation of passwords for systems must be met as per item Creation and Use of Password, except in cases where the systems themselves impose limitations.

Ultra provides a unique wireless network to Users credentialed for the performance of their functions, and another, exclusive to visitors only for internet access. Both have the same corporate rules for content control.

A wireless network specific for mobile devices is also available only for eligible Users. Users who have such access must immediately communicate the Service Desk in the event of an incident with the mobile device.

The networks mentioned are a grant from Ultra and, therefore can be monitored at any time as to their use.

Ultra provides solutions that allow information technology resources to be accessed outside the corporate environment, in order to enable the sharing of information, ensuring confidentiality and integrity of information over the internet.

Use the remote access only from trusted locations. In case of connection from a public network, make sure that your privacy is being respected.

The approved mobile devices and of eligible Users are configured according to a minimum Information Security standard and, under such conditions, access to Ultra network resources is available for these devices.

Do not enable sharing features of your device.
Be careful!

We are all responsible for the Information Security of the Company we work for. So, we need to know the sensitivity of data accessed in our daily lives and treat them according to their classification.

Our Security Policy determines the following levels for the classification of information:

- **Public information:** may be distributed without restriction, including exposed on the internet.
- **Internal information:** use should be limited to Ultra internal public.
- **Restrict information:** should be to the limited group of Users involved in the subject.
- **Confidential information:** should be to the limited to the minimum of Users necessary.

Use of telephone is designed for professional activities and it is up to each one to use it in correct way. Telephone calls are usually not protected, and there is the possibility of other people to overhearing your conversations.

Some calls may refer to confidential matters, therefore, is not recommended to disclose such information on the phone.

Ultra permits the use of print resources for private purposes, subject to compliance with the legal and regulatory provisions in force. Such use must not interfere with the performance of very professional or of any other User, degrade the performance of resources available or compromise the business image.

Printed documents are more difficult to be controlled and, therefore, require more care in the case of restricted or confidential documents.

Disposal of printed documents should be performed safely, ensuring the destruction of information.

At first, we defined what Information Security means and concluded that means preserving the status of confidentiality, integrity and availability of information. Considering such definition, we elucidated the responsibility and general provisions to which we are submitted at Ultra.

Understanding our role in Information Security, we have described in general terms how to proceed safely regarding the use of resources. In case of suggestions and questions, please contact the Managing Committee for Information Security at the address: **comite.seguranca@ultra.com.br.**

In the Corporate Intranet you will find information on the Information Security rules and policies, as well as all the settings required to insert the address.

Access: http://intranet.ultra.corp/si/


Extrafarma


Ipiranga


OXITENO
uma empresa do grupo ULTRA


ULTRACARGO


ULTRAGAZ
uma empresa do grupo ULTRA


ULTRA