Please consider the environment before printing this document

Title	**Regulations for the use of the workstation and IT tools**	
Issue date	20 May 2020	
Effective date	20 May 2020	
To be reviewed by	30 June 2022	
		Signature
Written by:	**Organisation**	L Garrafa
Verified by:	**Information & Communication Technology**	G. A. Martinengo
	Human Resources	M. Gastaldi
	Organisation	A. Ferrando
	Corporate & Legal Affairs	A. Navarra
Approved by:	**Human Capital & ICT** **ERG Group's contact person for the processing of personal data**	G. Coraggioso
Notes:	Original filed by Organisation	

Version/Revision	Date	Main changes
V.1	27/12/2017	
V.2	20/05/2020	• Smart Working-related point entered; • Adequate indication on the use of the "data basket" for mobile devices and included traffic monitoring aspect; • Make changes to the retention of email for outgoing staff with retention times, established in agreement with HR

Please consider the environment before printing this document

CONTENTS

Please consider the environment before printing this document

1. Introduction

Improper use of the workstation (PC, Laptop, Telephone and any other IT equipment) and the company resources used in the course of work exposes ERG (hereinafter referred to as the "**Company**" or "**ERG**") and the entire ERG Group to the risks of involvement in liability of both a financial and criminal nature, potentially creating security and image problems.

Given that the use of company resources must always be inspired by the principle of diligence and fairness, the ERG Group, for its own protection and that of its employees and collaborators, has also adopted this document (hereinafter referred to as the "**Regulation**") to contribute to the maximum dissemination of the culture of security and to prevent unconscious behaviour from triggering problems or threats to security in data processing.

2. Purpose

The purpose of this document is to define a set of rules of conduct with which all employees and third parties operating for the ERG Group must comply, in order to guarantee the need to protect information, in accordance with the general principles of reasonableness and cooperation in the conduct of business activities.

The further purpose of this document is to ensure that users of the ERG Group's IT systems acquire full awareness and understanding of the rules in force regarding access to and use of the IT systems and services made available to them and comply with the provisions of the law in force as well as the provisions issued by the various competent Authorities, in relation to the correct use of the Internet and email.

3. Scope

This Regulation must be complied with by anyone who, for whatever reason, uses IT equipment or services provided by ERG, unless specifically exempted, in whole or in part, by Head of Human Capital & ICT.

4. References

- External references:
  - Italian Civil Code Articles 2086, 2087 and 2104
  - Law 300/1970 - Workers' Statute
  - General Data Protection Regulation EU 679/2016 (also referred to as "**GDPR**")
  - Legislative Decree 196/2003 - Personal Data Protection Code (Privacy Code) and subsequent amendments and/or additions
- Internal references:
  - ERG Group’s Code of Ethics
  - Organisation and Management models pursuant to Decree Law no. 231/2001 possibly adopted by ERG Group companies
  - "Information Security Management" Guidelines
  - "Classification and Information Protection" Guidelines
  - "Computer Incident Management Procedure" Guidelines

Please consider the environment before printing this document

5. Rules for the use of the workstation and IT tools

The IT tools are made up of all the company's IT resources, i.e., infrastructure and application resources as well as digital information assets.

Infrastructure and application resources consist of hardware and software components.

Information assets are the set of databases in digital format and in general includes all the documents produced through the use of infrastructure and application resources.

Each user is responsible, pro rata, for the use of computer tools.

5.1 Digital information

Please refer to the "Classification and Information Protection Guidelines".

5.2 Clean Desk

Please refer to the "Classification and Information Protection Guidelines".

Staff (employee and non-employee) must manage work documentation whilst minimising the risks inherent in unauthorised access, disclosure or loss of confidential information. Therefore, the following directives must be complied with:

- only documents relating to ongoing activities must be placed on desks: all other material must be kept in compliance with security and confidentiality criteria;
- no confidential documents should be left unattended, not even in the event of short-term removals from one's workstation;
- at the end of the working day, any document containing personal data and/or confidential information must be stored in such a way that it is not accessible to unauthorised staff;
- if strangers enter the premises, the employee is obliged to conceal any personal information on paper material or on his or her computer screen;
- all documents must be immediately retrieved from printers, fax machines and copiers, especially network printers;
- any documents no longer required must be disposed of using the appropriate document destroying equipment and, in any case, must be made illegible;
- if you find yourself working outside of the workplace (in smart-working mode from home, or on the move during travel, etc.) and even more so in public places (waiting rooms, transport, etc.) you must be careful that no strangers have the opportunity to see the documentation managed, taking care to orient the laptop in an appropriate way and avoiding leaving any paper documents in sight.

5.3 Login credentials

ERG, where deemed appropriate on the basis of the criticality of the data and information, has adopted appropriate systems to prevent undue access by unauthorised users and alert systems that report any anomalous behaviour to the competent Units.

Specifically, in order to limit access to the company network and systems, the user is assigned a personal identification code (username or user id) and a keyword (password), which constitute strictly confidential company data. Therefore:

- the username to access the company network is assigned and managed by UO ICT which creates a single digital user for each person. This digital username is used to uniquely identify each user who accesses the company's IT resources and applications; subsequently, this user is assigned the appropriate system privileges that allow access only to the information necessary to perform his or her work role;
- the use of personal access credentials is the responsibility of each user;
- it is not permitted to communicate one's access credentials to third parties, including family members or persons close to one another, even if in a top position in the company;
- if there is suspicion or fear of unauthorised use of your login credentials, you must immediately report the suspected breach to ICTsecurity@erg.eu and 3777@erg.euand change your password;

Please consider the environment before printing this document

- Each user must avoid keeping a (plain text) copy of his or her password on a file or on paper that is easily accessible to third parties, as well as reusing or copying company credentials to create other personal accounts.

Rules for the generation and assignment of access credentials:

- the personal identification code (username) must be uniquely assigned to each user. Specifically, the username is composed of [first name initial + surname];
- the first password must be generated randomly;
- the password must be given to the user in a secure manner;
- the first time you log in following a new assignment, the initial password must be changed.

Rules for creating a password:

When creating a personal password, the following criteria must be respected, within the limits of any technical constraints that may exist on the various systems:

- it must be different from the username or user ID (it must not contain all or part of the user's first name, last name and user);
- it must be no less than 8 characters long or, if this is not possible, no more than the maximum number of characters allowed;
- it must consist of upper and lower case characters, numbers and special characters;
- it must be different from the last 5 versions previously used;
- it must not contain references that can easily be traced back to the user or to known areas;
- it must not be based on names of people, dates of birth, animals, objects or words from the dictionary (including foreign ones), taken from personal information;
- it must not have a sequence of identical characters or groups of characters repeated or more than three contiguous characters on the keyboard;
- the same password must not be used for access to business applications as for access to systems managed by other organisations

Rules for keeping the password:

The security of the password, as well as the strength of its construction syntax, depends on the care with which it is kept; therefore, each access key:

- must be known exclusively to the user and must not be communicated to other users;
- must not be written on post-it notes, visible on the desk or applied elsewhere;
- must not be stored in automatic log-in functions, in a function key or in the browser used for Internet browsing.

Rules for changing the password:

In addition to the syntax and how it is stored, the security of a password also depends on its validity period and, therefore, the password:

- must be changed at the time of first use and at least every six months thereafter;
- must be changed immediately in the following cases:
  - when you suspect that someone knows about it;
  - after having remotely accessed the company's information systems through a "public" or shared PC (e.g., the "public" PC): Internet Cafe, public Wi-Fi);
  - following the theft/loss of some company equipment;
- in general, on any occasion on which it may be deemed to have lost its confidentiality requirements.

The password can be replaced with a new one even before the expiry date, by the UO ICT, for justified reasons and after informing the user. In this case, it must be modified again on first access by the user.

To reset/unlock the password, the company self-service tool must be used where enabled. In all other cases, the user must contact the Help Desk through the channels provided (telephone, email); once the identity of the person requesting the Help Desk has been verified, the Help Desk will reset/unlock.

Please consider the environment before printing this document

All holders of users and passwords are responsible for any tampering, misuse or unauthorised disclosure and are consequently liable to any disciplinary/legal sanctions.

5.4 Fixed workstations

Fixed workstation means the unitary set of Personal Computer (hereinafter PC), accessories, peripherals (e.g., monitor, mouse, etc.) supplied by the company to the user and through which the work is normally carried out.

Each PC (accessories and peripherals included), be it purchased, rented or leased, remains the exclusive property of the company and is provided to the user for the performance of his or her work tasks and, in any case, for purposes strictly related to the activity carried out.

Therefore, the following rules must be complied with:

- it is necessary to use the fixed workstations entrusted by the company responsibly and professionally;
- it is not permitted to make changes or modifications to the hardware or software configuration of the fixed workstation independently, but requests for such changes must be addressed to the relevant company structures;
- you are not allowed to leave fixed workstations unattended and with user sessions active when you leave your workstation, but you must lock them with a password or log out of the session, even with the help of a screensaver with password;
- it is not permitted to consume food and drink near the stations themselves, in order to reduce the risk of damage and/or malfunction;
- you may not alter or remove hardware/software components.

5.5 Portable workstations

Portable workstations include all the IT tools provided by the ERG Group in order to carry out their work outside the workplace (e.g. notebooks, tablets, etc.).

Users must protect the portable workstations provided from the risk of theft or loss, as a result of which, in addition to causing damage to the company in relation to the value of the computer itself, threats to the availability and confidentiality of data may occur, since any documents stored (temporarily and as an exception to the rule) on the hard disk may become available to third parties.

Therefore, the following security solutions must be adopted:

- it is not permitted to leave the portable workstation unattended or to entrust it into the custody of facilities and/or persons not specifically assigned to the custody of valuables (e.g., do not hand the device over to cloakroom staff in hotels, restaurants, etc.);
- you are not allowed to leave portable workstations with active user sessions when you leave your workstation, but you must block them by using passwords or log out of the session, even with the help of a password screensaver.

The user is responsible for the device assigned to him or her and must guard it diligently both when travelling and when using it in the workplace or remotely. Therefore, the following rules must be followed:

- portable workstations used outdoors (off-site work at conferences, outdoor courses, etc.) must be kept in a protected place in case of removal (e.g., it is not permitted to leave the portable workstation in the car during stops, not even in the luggage compartment, and in case of air travel the portable workstation must be transported as hand luggage and stored in a suitable case). Outside of the company offices, where really appropriate, the security cable must be used to physically lock the portable workstation to a fixed support (e.g., desks);
- any data stored locally on portable workstations (temporarily and as an exception to the rule) must be protected in accordance with *LG Classification and Data Protection.*
- portable workstations are subject to the rules of use for fixed networked workstations, with particular attention to the removal of any files processed on them prior to return. Likewise, the data contained in the removable devices must be deleted before the devices are returned;

Please consider the environment before printing this document

- in the event of loss or theft of a device, the assignee must immediately report the incident to UO ICT, for appropriate insurance practices and must submit a copy of the report filed with the competent authorities as soon as possible.

5.6 Software

The Software represents all programmes installed on physical workstation devices or other hardware tools. They represent the tools with which company data and information are generated/manipulated.
Therefore, the following security rules must be complied with:

- it is not permitted to attempt or make additions or changes to the standard software configuration provided by the company, but requests for such changes must be directed to the relevant company structures;
- it is not permitted to install software for personal use on company workstations (fixed/laptop): such action may result in the introduction and propagation of viruses within company systems or the use of software not in accordance with the licensing rules under which it was issued;
- software from the Internet or copied from external devices is not allowed;
- it is not permitted to install or run unlicensed software (e.g., illegally copied software) on company workstations (fixed/laptop), to modify existing programmes on company electronic devices, to reproduce or duplicate computer programmes;
- you must use the software within the limits specified in the licence agreements;
- it is forbidden to copy the software made available by the company (both internally developed and licensed, except in cases expressly authorised under specific agreements with vendors) to external USB memories or other storage media;
- It is prohibited to install software in breach of copyright rules or other intellectual property rights (e.g., music, files, photos, videos, etc.).

5.6.1 Antivirus

The possibility that computer virus infections can be prevented depends not only on the presence of appropriate tools and their correct configuration, but also and, above all on how they are used.
Therefore, the following guidelines must be followed:

- you may not change the configuration or disable the anti-virus system for any reason;
- you may not use anti-virus products other than those provided by the company;
- it is necessary to promptly report any malfunction of the anti-virus system to the ICT unit;
- it is necessary to promptly report to the ICT Unit the presence of viruses recognised by the anti-virus system and not independently removed by the system itself.

5.7 Portable storage devices

Portable storage devices refers to all devices (e.g., CD-ROMs, DVDs, USB storage devices, MP3 music players, cameras, etc.) that allow you to copy or store data, files or documents outside the company workstations.
Therefore, the following rules must be followed:

- you are not permitted to use personal portable storage devices unless previously authorised by the company;
- where authorised in accordance with the above, once connected to the company's IT infrastructure, the devices must be managed in accordance with this document;
- the storage media, when kept inside one of the company's premises, must be stored in archives with access limited to authorised staff only;
- it is not permitted to take portable storage devices outside the company without applying the necessary security measures provided by *LG Classification and Data Protection*.

Please consider the environment before printing this document

5.8 Printers, copiers and fax

Printers, photocopiers and fax machines are company IT tools and must be used by staff exclusively for work activities, not for personal purposes and with particular attention to minimising the number of prints produced.
Therefore, it is necessary to comply with the following rules when using them:

- printed documents that must not be left unattended on the printer must be collected immediately;
- it is necessary to print all information of a particularly confidential nature exclusively on printers present inside the company offices or in offices where the user is authorised to process the same data;
- if you find that you have made a mistake in printing, you must cancel the printing;
- if you are unable to cancel the printing and you notice, at the time of withdrawal of the print, errors that make the documents unusable, you must destroy them in your offices;
- copies may only be delivered to users authorised to process the specific type of data contained in the documents;
- when making copies of documents containing sensitive data, do not leave the printer during copying to prevent other unauthorised users from coming into contact with the documents.

Faxes must be sent and received in accordance with the following requirements:

- it is necessary to ensure the utmost confidentiality of information by protecting the document from prying eyes as far as possible;
- users must return both the document sent and the "transmission report" to the office and make sure, if the fax device is not in their office, that they do not leave anything at the office where the fax was sent;
- in the event that incorrectly addressed faxes are received, it is necessary that the users of the receiving organisational unit treat such documents with the utmost confidentiality as they may contain personal data or confidential information belonging to third parties;
- in the event that incorrectly addressed faxes are received, it is necessary that users do not reply by fax to the sender's number, but check the presence on the received document of a telephone number to contact to warn of the wrong sending: only after contacting the sender or the recipient of the fax can the received document be permanently deleted, using a document shredder.

5.9 Corporate Smartphones

Depending on specific work activities, the ERG Group provides its employees with a company mobile phone or smartphone. Employees may also use the smartphone provided in their personal capacity (mixed-use assignment), generally paying reasonable attention to cost containment, especially when using it abroad and the "hot-spot" mode to service the laptop that may be in use, if enabled, and avoiding any abuse.
The assigned device is owned by the company and is given as a priority for work support purposes (except for mixed use); therefore, the following rules must be complied with:

- the appropriate use of the mobile phone is the responsibility of the recipient of the device;
- the assignees of company mobile phones are not allowed to lend, rent or otherwise give them for use to third parties, internal or external, not assignees;
- the responsibility for the care and use of the appliance lies with the assignee of the appliance;
- the configuration in which the device is delivered must not be changed;
- in case of malfunction or failure of the device or SIM, the employee must contact UO ICT;
- in the event of theft or loss of the device, the employee must notify UO ICT immediately in order to immediately block the user and remotely delete the device. The employee must then submit a formal report of theft or loss and send a copy to UO ICT for subsequent compliance. If the theft or loss occurs in circumstances or at times when it is not possible to communicate with UO ICT, the employee must follow the following procedure:
  - Verification by Geolocation of the phone position (via www.icloud.com)
  - Remote phone lock (via www.icloud.com):

Please consider the environment before printing this document

"Please return to ERG SpA +3901024011"
- Remote Formatting (via www.icloud.com)
- Blocking the SIM by contacting your mobile phone provider
- Change of network password (ERG) and any other relevant passwords;

- It is prohibited to acquire administrative privileges (e.g., root privileges), jailbreak or tamper with the operating systems of corporate mobile phones;
- the use of the SIM security PIN and the unlocking code of the device according to what is centrally set through the "Mobile Device Management" platform adopted by the Group is mandatory; in both cases disabling is forbidden. Specifically, the unlock code must:

  1. be at least 6 characters long
  2. not be in ascending or descending sequence (e.g. 123456)
  3. not contain more than 3 consecutive times the same character
  4. be different from your personal PIN
  5. request re-authentication after 1 minute of inactivity;
- the SIM is delivered with a phone profile that draws on a shared company data basket (by email, app and internet). In order to comply with cost budgets and to guarantee an adequate level of service to all users, the Group reserves the right to
  - periodically monitor the volumes of traffic generated, notifying users of any anomalies with respect to normal and appropriate use, considering the purposes with which the equipment is assigned;
  - assign to each user, through appropriate technical configurations, a predefined share of traffic appropriate to normal use, and activate appropriate alert mechanisms to users according to the level of traffic reached, possibly and temporarily blocking the use if the traffic threshold considered reasonable is significantly exceeded;
- internet browsing via mobile phone/smartphone is subject to the rules provided for and defined in the relevant paragraph of these Regulations;
- the Group reserves the right to limit or inhibit, by means of appropriate blocks or warnings on the device, the installation of apps that are not consistent with the ethical principles adopted by the Group, that do not comply with the regulations in force or that may constitute risks for the functionality of the device;
- the use of free and available Wi-Fi networks is allowed if considered reliable and safe and is recommended in case of downloading large amounts of data to limit the consumption of the data basket;
- particular attention must be paid to the management of telephone communications in public environments (e.g., premises, stations and means of transport, etc.), in order to prevent the dissemination of company information by unauthorised third parties.

5.10 Internet browsing

The use of the Internet and browsing the net are permitted, for the purposes of work and in line with the tasks assigned, unless otherwise specified.
Internet access is provided for the purpose of enabling the retrieval of any information necessary to carry out the work or to access web-based applications/systems. Given that it is a work tool, the persons to whom the Company assigns access are responsible for its correct use in full compliance with the reference regulations in force, as well as according to normal standards of correctness, good faith and professional diligence.
The company, with these Regulations, has intended to define a specific code of conduct for users in order to avoid conduct that could, through improper use, unwittingly damage it.
Specifically, the following rules must be observed:

- browsing websites contrary to ethics, morality or illegal content is prohibited;

Please consider the environment before printing this document

- it is forbidden to download programmes, even if unlicensed or on trial (freeware and shareware), unless expressly authorised by the UO ICT; downloading files from the Internet is, in fact, an inherently dangerous operation as it can be the vehicle for the introduction of viruses into the company network;
- you are prohibited from transmitting or downloading and installing material in breach of copyright;
- It is forbidden to create, transmit, publish and/or archive in any form (images, texts, films, voice recordings, etc.) any kind of material:
  - that breaches copyright and intellectual property laws;
  - that includes content that is harmful, threatening, harassing, abusive, slanderous or vulgar;
  - that breaches privacy laws;
  - that encourages criminal acts and that, in general, may harm the company;
- any form of registration with company credentials is not permitted for websites the contents of which are not related to the work activity;
- file sharing in peer-to-peer mode is prohibited;
- It is prohibited to enter on the network or servers software that is harmful to systems or otherwise unauthorised;
- it is forbidden to use the company's technological infrastructure to procure and disseminate material in breach of the regulations in force;
- use must comply with the principles of the Group's code of ethics and the principles of fairness;
- any use for personal purposes (e.g., participation in social networks, making financial transactions or other types of purchases, etc.) must be made in compliance with normal criteria of reasonableness in terms of time and continuity and, in any case, through private credentials.

In order to reduce the risk of improper use of "browsing" on the Internet, the Group has adopted, where applicable, appropriate measures to ensure the correct use of company devices and systems in compliance with the provisions of these Regulations; it has therefore configured the systems and used filters so as to prevent operations deemed inconsistent with the work activity, such as access to certain web pages or specific categories of websites. For the same reasons, the uploading or downloading of files with particular characteristics of data type are prevented.

5.11 Instant messaging tools/Collaboration

Instant messaging/collaboration tools (e.g., Skype, WhatsApp, etc.) are real-time communication systems over the network, typically Internet either network which allow its users to exchange short messages.

The use of these tools is permitted to all users in order to facilitate communication between them. Therefore, the use of these instruments must comply with the following Directives:

- information classified as CONFIDENTIAL or INTERNAL may not be exchanged;
- they must not contain messages of a sexual, discriminatory and defamatory nature and in any case in breach of the regulations in force;
- they may be used for private communications with users outside the company but only within the limits of fairness and measurement, i.e., they must not be excessive, i.e., they must not be such as to affect work performance.

5.12 Social media

This includes both the private use of Social Networks (e.g., Facebook, Twitter, LinkedIn, etc.) by employees or collaborators and the use by the company itself for internal purposes (e.g., communication with employees, sharing information within work groups, etc.) or business purposes.

Therefore, the use of Social Networks must be in compliance with the indications contained in the "Social Media Management" Procedure and in accordance with these Regulations.

The use must be carried out in compliance with the regulations on email and Internet (Privacy Guarantor Measure dated 01/03/2007).

The users' profile, if it allows them to relate to the company, must be adequately protected by password and strict privacy settings must be adopted.

Specifically, users must not:

Please consider the environment before printing this document

- attempt to access websites or content that contain inappropriate or, in any case, contrary to ethics, morality or illegal content;
- make disparaging statements, publish information or participate in activities that could defame, slander or damage the reputation of the organisation, persons and/or third parties working with the company. This includes the use, conduct or behaviour online and/or on social media, including outside of the workplace;
- use social networks and forums irresponsibly and not in accordance with the principles of the company and Italian laws;
- disseminate information, documents and any personal data relating to customers, employees or suppliers of the Company, including confidential information of the Company, online, on social networks or forums;
- use their company email address to register for external non-work related social networks and/or forums;
- voluntarily post, send or receive, upload/download, obtain, save or share any content or material that infringes, misuses, or otherwise violates the intellectual property, privacy or publicity rights of any individual, group or entity.

5.13 Conference and video conferencing tools

Conference or video conferencing tools are widely used to reduce travel costs and speed up business processes, but they are not risk-free.
Therefore, the following safety directives must be complied with:

- care must be taken when transmitting information classified as CONFIDENTIAL;
- conference/videoconference participants must be positioned in such a way that unauthorised third parties cannot listen to or view the conference (it is preferable to use a specific conference room);
- in the case of videoconferences, it must be ensured that the camera only frames the individual and that the microphone volume is at the minimum necessary to allow communication;
- users must log on with a password and log off for each conference/videoconference session;
- it is necessary to verify that only the persons actually invited and authorised participate in the conference/videoconference, verifying their identity.

5.14 Email

The Group provides two types of email addresses: personal addresses (built as <initials-of-name><surname>@erg.eu) and addresses shared between several users (for example, <functionXYZ>@erg.eu).
The email box assigned by the ERG Group to the user and its address, as well as incoming and outgoing messages, are the property of the company. They represent a working tool entrusted to the user for the sole purpose of enabling him or her to carry out the task entrusted to him or her. The persons assigned to the mailboxes are therefore responsible for their correct use.
The assignment of the personal mailbox is made at the same time as the creation of the user at the time of recruitment; at the time of termination of employment, the personal user is automatically blocked and the relevant mailbox is automatically deleted after 30 days, unless otherwise provided in this document.
As regards the email of "Managers & above" or persons whose role is considered important for the activities carried out, for which the maintenance of company email is necessary to ensure business continuity, HR must assess on a case-by-case basis whether a back-up copy should be maintained after the exit of the Employee and communicate this explicitly to ICT by the date of exit, in addition to the outgoing Employee. Any back-up that may be archived in accordance with HR's instructions must not be made available to anyone other than the Head of Human Capital & ICT and/or its delegates for the purposes set out in this document. Such a backup may be provided to the Employee prior to his or her departure with explicit

Please consider the environment before printing this document

authorisation from HR. The same is kept for the time strictly necessary to ensure the aforementioned business continuity.

Rules for the use of email

Correct behaviour must be maintained when using the email tool. Specifically, the following rules apply:

- email messages contained in a user's inbox are considered to be related to the work carried out for the Group: following any exceptional use of company email for personal purposes, users must delete messages of a personal nature from the system as soon as they are transmitted and/or read;
- confidential information must not be disclosed to third parties, whether confidential or otherwise owned by the ERG Group, without the express authorisation of the Company itself;
- email messages or, more generally, data, programmes or other material of a computer nature with offensive, harassing, vulgar, blasphemous, xenophobic, racial, pornographic or otherwise inappropriate or illegal content must not be sent or stored;
- all incoming emails are controlled by anti-virus/anti-malware/anti-spam software and any infected email is quarantined and reported to the recipient or placed in the user's system folder. It is however necessary to be very careful when opening attachments to received emails, regardless of whether or not the sender is known, as some emails may still exceed the filters set on the central system. Specifically, documents with "anomalous" names must not be opened, nor must files or macros received as attachments to emails from an unknown or suspicious sender (in this case, immediately report the incident to UO ICT by writing to 3777@erg.euand ICTsecurity@erg.eu);
- you must not connect to websites using links contained in emails from an unknown or suspicious sender, but you must immediately report the incident to UO ICT ERG SpA by writing to 3777@erg.euand ICTsecurity@erg.eu;
- attachments to sent emails must be small in size so as not to make it difficult for the company's email server to operate;
- the automatic execution of programmes (e.g. activeX) attached to email messages must be deactivated;
- sending unwanted or requested email messages, including the sending of any advertising information to persons who have not specifically requested such information (spam), is a clear breach of the rules dictated by the Privacy Act. In compliance with the aforementioned rule and what can be traced back to it, users are expressly forbidden from using the company's resources for:
  - any form of harassment by email, either through the content or the frequency of sending or the size of the message;
  - unauthorised use of the email header or the creation of false headers;
  - the creation or forwarding of emails belonging to chains or similar.
- the distribution lists, the use of which is reserved for the relevant company functions, must not be misused;
- the number of distributed copies of the same email must be limited. A notice must of course be sent to all interested parties and a copy must be sent to the other persons mentioned in the notice;
- using the features made available by the email system, your default signature must be inserted at the bottom of the email according to the standard set by the Communication Department and made available on the Intranet. The signature must also be entered in the mailboxes of the function boxes;
- company structures that send and/or receive work communications that may require consultation by several users belonging to the structure itself, must make a request through their manager for a function mailbox appropriately shared and protected (e.g., <FunctionXYZ>@erg.eu). These boxes guarantee operational continuity in the event of prolonged absence (e.g., holidays, maternity leave, illness or off-site work) or termination of the employment relationship of one of the members of the structure itself;
- in the event of prolonged and unscheduled absence, the user must also make use of the features made available by the email system that guarantees each user, owner of a mailbox, the possibility of:

Please consider the environment before printing this document

- automatically sending, in the event of absence, reply messages containing only the period of absence and the "coordinates" (also electronic or telephone) of another person or other useful ways of contacting the structure to which they belong;
- authorising a trustee to view the content on condition that he or she has a valid account on the same domain. This delegation can be set using the featured known as "mail delegation" directly by the user who owns the mailbox or through the Help Desk.

- A user's mailboxes cannot be kept active after leaving the ERG Group for any reason whatsoever; in order to guarantee operational continuity, the Managers of Organisational Units must organise themselves with shared function boxes. Exceptionally, after evaluation by the competent Department, an automatic reply message containing the contact details of another person or other useful ways of contacting the structure concerned may be activated on the outgoing employee's mailbox contact for a maximum period of 30 days;
- you may not configure access to your company's inbox on private fixed and mobile devices including mobile phones, smartphones and tablets. The access configuration would, in fact, result in the download of company data to the private device without the possibility for the company to guarantee an adequate level of protection through the adoption of appropriate security measures. The only way to consult emails with such devices is via browser.

5.15 Request and Delivery of corporate IT tools

The request for one or more company tools must be made in accordance with the "IT Equipment Allocation" Procedure and through the Request Management System (SMART).
After receiving the equipment, the user, for the cases in which it applies, must close the relevant SMART, confirming the receipt of the goods and accepting the use according to these Regulations.

5.16 Return of corporate IT tools

At the end of the job or employment contract, any tool supplied or produced during the working period must be returned to the company (subject to any exceptions explicitly authorised by HR and communicated to ICT by the date of termination of employment, including with reference to the back-up of the mailbox), for example:

- any device or tool assigned to ensure physical access (e.g., badges, keys) or logical (e.g., tokens) to company services;
- any documents, files, data, projects, software (including source codes), books or manuals prepared or edited by you for the purposes of your business;
- all computer tools (laptop, mobile phone, tablet, USB, portable hard drive, CD/DVD, etc.) and/or company asset (e.g., car) assigned.

5.17 Checks on the use of the Internet connection and the company mailbox

The company reserves the right to carry out, in compliance with the principles of pertinence and not excess and through instruments that minimise the processing of personal data, the checks it deems appropriate and necessary for the following legitimate purposes:

- to protect the security and preserve the integrity of IT tools;
- to ensure that the use complies with laws and regulations and avoid the commission of offences;
- to oversee the correct use of IT tools (including Internet browsing and the use of electronic mail, as regulated in these Regulations) by users;
- to verify the functionality of the system and IT tools, ensuring business continuity;
- where there is a suspicion, to investigate or identify inappropriate uses, as well as breaches of this Regulation or other company specific policies or assert or defend the rights of the ERG Group;
- to respond to requests from the competent authorities.

In carrying out the checks for the purposes specified above, the company guarantees the absence of

Please consider the environment before printing this document

interference or unjustified breaches of the fundamental rights and freedoms of persons receiving or sending electronic communications of a personal or private nature. The company also guarantees that no remote control of the work performance is carried out through the following checks.
The Company adopts appropriate technical measures (e.g., filters, system configurations, etc.) to prevent damaging events or situations of computer danger; in the event of any problems, the Company reserves the right to carry out appropriate technical checks on the anomalies found, by carrying out analyses on aggregate data referring to the entire working structure or its sub-areas.
Aggregate checks are performed either periodically or for reasons of evidence of an anomaly, are of a statistical nature and are not related to lawful or illegal conduct of the individual user
The aggregate verification, which is anonymous in nature, may end with a generalised warning regarding a use of company tools detected as being "anomalous" and with an invitation to scrupulously comply with assigned tasks and instructions given. The warning may be restricted to employees in the area or sector in which the anomaly was detected.
Where collective checks, related warnings or the presence of other anomaly situations occur, checks may be carried out on individual devices and workstations on a named basis. In this case, a prior individual notice shall be sent, with due confidentiality, to the person subject to the check, stating the legitimate reasons for the check and the technical means by which it is carried out.
The only persons authorised to carry out the aforementioned checks are the following persons and/or the System Administrators appointed by them:

- Head of Human Capital & ICT also as Contact Person for the Processing of Personal Data;
- Head of Human Resources;
- Head of Information & Communication Technology;
- ICT Governance, Integration & Security;
- ICT Infrastructures & Services;

The persons in charge are obliged to carry out only those operations that are strictly necessary for the pursuit of the purposes related to research and examination of anomalous situations and maintenance activities of the Systems.
It is forbidden for persons not specifically appointed by the company to carry out any kind of activity aimed at controlling email and Internet access, including for lawful purposes.
The list of System Administrators is available from the Organization Department.

5.17.1 Checks on compliance with Internet usage patterns

For security and technical management reasons, all Internet connections require authentication by qualified users to a proxy server that records the following information in special log files:

- IP and/or name of the PC and/or user name making the request;
- Date and time of request;
- Device name, IP and/or address, destination port of the request;
- Processing time, received bytes, sent bytes,
- Protocol, HTTP method, URL;
- Network of origin;
- Target network

These log files may only be accessed by authorised persons for internal security reasons or at the request of the judicial authorities. In no way can they be used to profile user traffic habits, including the websites visited, or for remote control thereof, except in aggregate and anonymous data.
The reports built to carry out the aggregate controls described above are anonymised through the elimination of any information that allows immediate identification of the user (user name and IP of the location that originated the request).
The log files are stored for a maximum period of 30 days after which they are automatically deleted (through over-recording procedures such as log file rotation).

Please consider the environment before printing this document

5.17.2 Verification of compliance with the way email is used

No regular checks are carried out on the email, nor are any checks carried out on the content of both incoming and outgoing emails.
The ERG Group accesses the email inboxes entrusted to users within the limits set out in this document.
The Company applies the following methods for the management and control of company email accounts:

- mailboxes are subject to automatic backup, which means that stored information is not lost, even in the event of an incident;
- information relating to incoming and outgoing messages from company email addresses and the related details technically necessary to carry out the email service are recorded and stored in log files;
- logs are stored for a maximum period of 30 days and are deleted periodically and automatically (through over-recording procedures, such as log file rotation).

6. Computer security incident reporting

Computer security incidents are regulated by the Computer Incident Management Procedure to which reference must be made.
Each user is required to promptly report, to 3777@erg.eu and to ICTsecurity@erg.eu, any accident or anomaly found in the use of the computer tools provided, in the management of access credentials or in internet browsing and in the use of email.
Timely reporting is a necessary prerequisite for ensuring rapid and effective detection and resolution of any compromise or breach of confidential information, as well as for countering possible attacks and mitigating any impacts.

7. Disciplinary sanctions

Information identified during any checks may be used and retained for the duration of any investigation, disciplinary or regulatory proceedings and may be disclosed to third parties (e.g., lawyers) when necessary.
Specifically, the company, in view of what has been defined above, if it finds that email and/or the Internet network are being used improperly, may take disciplinary action against the User recognised as responsible by applying the sanction system in force.
This is notwithstanding the right to report it to the competent authority if the conduct constitutes a criminal offence.

8. Roles and responsibilities

The following paragraph sets out the main roles and related responsibilities that play a key role in ensuring the correct use of company IT tools and their operation.

8.1 HRBP

HRBP is responsible for:

- supporting the relevant company structures in defining, reviewing and updating the security requirements included in these Regulations;
- ensuring that the requirements set out in these Regulations are disclosed appropriately and brought to the attention of employees and third parties;
- defining and initiating disciplinary proceedings against individuals for whom a breach of the principles of these Regulations has been verified.

8.2 Legal Affairs

Legal Affairs, for the purpose of this regulation, is responsible for:

Please consider the environment before printing this document

- supporting the relevant corporate structures during the definition, reviewing and updating the protection requirements included in this regulation and ensuring that they comply with applicable laws and regulations;
- ensuring that investigations are conducted in accordance with applicable laws and regulations;
- taking legal action against persons or entities involved in a breach of this Regulation.

8.3 Organization

Organization is responsible for the following tasks:

- supporting the relevant company structures in defining, reviewing and updating the security requirements included in these Regulations;
- supporting and/or managing any anomalies, problems or incidents related to GDPR.

8.4 ICT Governance, Integration & Security

ICT Governance, Integration & Security is responsible for:

- defining, reviewing and updating the security requirements included in these Regulations;
- supporting the ICT UO in identifying the technical and organisational solutions implemented to meet the requirements included in these Regulations;
- managing any breach of these Regulations.

8.5 Organisational Unit Managers

The Organisational Unit Managers are in charge of:

- ensuring that the rules within these Regulations have been respected by those subject to their responsibility;
- notifying the relevant company structures of any breach of the requirements set out in these Regulations.

8.6 User

"User" refers to any individual (e.g., employee, collaborator, supplier intern, etc.) who uses the company's IT tools.
Therefore, the user:

- is personally responsible for the use of the IT tools entrusted to him or her by the company as well as the related data processed for business purposes;
- is required to protect (to the extent of its competence) the company's assets from improper and unauthorised use, damage or abuse, also resulting from negligence, imprudence or inexperience;
- is required, in relation to his or her role and the duties actually performed, to work to protect the company's IT security, reporting to his or her manager, without undue delay, any risks of which he or she is aware or breaches of these internal regulations.