FCC GROUP

Technological Resources Usage Policy

Version History				
Version	**Date**	**Author**	**Detail**	**Approver**
1.0	April 2009	DSIGRT	Document creation	Board of Directors
1.2	April 2019	DSIGRT	Document review	Board of Directors
1.3	July 2025	DSIGRT	Format standardisation with the rest of the Regulatory Framework Inclusion Artificial Intelligence	Board of Directors
1.4	June 2026	IS	Document review	-

INDEX

1. Scope 4
2. Introduction 5
3. Purpose 6
4. Technological Resources General Rules 8
5. Specific rules relating to equipment/hardware 10
6. Specific rules relating to software 11
7. Specific rules applicable to email users 12
8. Specific rules of use relating to the Internet 14
9. Specific rules relating to audiovisual media and geolocation 15
10. Specific rules of use relating to data networks 16
11. Specific rules of use relating to social networks 17
12. Specific rules of use relating to AI systems 18
13. Power of monitoring the proper use of Technological Resources 19
14. Right to digital disconnection 21
15. Guarantees of information regarding legal representatives, workers and reception of this Policy 22
16. Suspension or termination of the relationship with the user 23
17. Management and response to security alerts and incidents 24
18. Basic data protection information 25

1. Scope

This Regulation has the nature of corporate policy and, therefore, is applicable to all FCC Group companies, irrespective of their activity or place where said activity is carried out.

Notwithstanding the foregoing, and with regard to its application in countries other than Spain, the applicable local regulations and internal policy must be complied with in all cases.

Fomento de Construcciones y Contratas, S.A., as the parent company of the Group, is responsible for establishing the bases, instruments and mechanisms necessary for an adequate and efficient coordination between this Company and the other companies that make up its Group. All this without prejudice or any loss of the employer status and the independent decision-making capacity that corresponds to each of these companies, in accordance with the corporate interest of each of them and the duties that the members of their administrative bodies maintain towards all their shareholders.

2. Introduction

Computer systems, messaging and email applications, the use of the Internet, social networks, data networks and other devices have become necessary and important tools for the operation of each Organisation.

The Companies of the FCC Group, hereinafter referred to as the 'FCC Group', 'FCC' or the 'Company', provide their personnel with different technological resources (hereinafter (“Technological Resources”), the purpose of which is to carry out duties related to their position and to guarantee that the personnel have the necessary technological tools at their disposal to be able to carry out their work.

The nature, provision and availability of these resources require that policies related to their use be established in a way that ensures their correct and optimal use. In addition to this, it is necessary to protect the confidential information handled through the Technological Resources, safeguard intellectual property, prevent cases of liability against third parties, and generate evidence of the infringements that may be committed using the Technological Resources.

Finally, it is a priority for these policies to inform the staff and their representatives of the business surveillance powers over such Resources that the FCC Group recognises, as well as its justification and the means to be used in this regard.

3. Purpose

This Usage Policy (hereinafter, the “Policy”) is framed within the FCC Group's internal regulations, and develops the principles contained in the Group's Code of Ethics and Conduct.

The purposes of the Policy are essentially those that are included below:

- Its main objective is to guarantee that the users of the Technological Resources use them appropriately, responsibly and legally, protecting the security of the information in any case.

  The use of such Technological Resources includes the use, in accordance with the guidelines established by the FCC Group and applicable legislation for Artificial Intelligence systems that are developed, implemented and used at FCC and which are governed by the provisions of the ‘Policy on the Development and Acceptable Use of Artificial Intelligence Systems in the FCC Group’ and other internal regulations developed.

For the purposes of this policy, it must be stated that:

- The term 'user' or 'users' used throughout the document includes the work force or other personnel of the FCC Group with a contract in force or in suspension, or with post-contractual obligations transcending this policy, and its content applies to all Companies of the FCC Group without exception and as long as the transfer and use of Technological Resources is maintained. Any reference to the employment contract, to workers or to the employment relationship, should be considered extendible to other types of civil or commercial services.

- The Technological Resources include: (a) computers, application servers, remote access terminals, desktop or laptop computers, tablets, fax machines, USB devices, external hard drives and similar or equivalent devices, (b) any application or software program, networks and systems, (c) Internet services, Intranet, social networks, email and instant messaging, (d) accounts that give access to the use of hardware, software and information systems, including the systems and cloud services contracted by the FCC Group, (e) landlines, mobile phones, smartphones, GPS, etc., and (f) drones, robots, chatbots, smart vehicles and sensors. Any other technological element or innovation that the FCC Group may acquire in the future, such as artificial intelligence or blockchain programs, must be understood as being included within the foregoing

- Allow the FCC Group to exercise due control in order to prevent the use of Technological Resources being involved, among other things, in prohibited conduct such as the examples listed below:

  - Harassing or discriminating against employees or third parties.

  - Attacking the dignity, privacy and other fundamental rights of employees or third parties.

  - Defaming, slandering, insulting or any other attack against the good honour, reputation and image of FCC Group Companies, their employees or third parties.

  - Disclosing confidential information, during or after the termination of the work contract or service provision.

  - Violating the regulations on data protection in any of its forms, and especially in what may represent an attack on the fundamental rights of individuals.

  - Attacking the security of the FCC Group and its tangible and intangible assets (ownership of property, intellectual and industrial property rights, goodwill, reputation, good image, etc.).

- Putting at risk the security and stability of the equipment, systems, or information contained in them.
- Carrying out acts of unfair competition against the FCC Group.
- Failure to comply with contracts or relationships with third parties.
- Transmitting, distributing, storing, downloading, installing, copying, sending or receiving any kind of content protected by copyright, trademarks, distinctive signs, trade secrets or other intellectual or industrial property rights used without due authorisation, and/or that which is offensive or discriminatory especially if its possession or use constitutes an illegal action.
- Deleting, damaging, deteriorating, altering, erasing or making inaccessible, intentionally, the FCC Group's computer data or computer programs.
- Developing any other conduct that involves a breach of the Code of Ethics and Conduct that governs the FCC Group.
- And in general, making any use of the Technological Resources contrary to the national legal system in force in each State, to this Policy or other regulations in force within the Company.

- In the event that it is detected that the Technological Resources have been misused or to verify the correct compliance by their employees with their work obligations, allow the FCC Group to adopt the necessary measures, among them, to put an end to the prohibited conduct, and adopt the corresponding disciplinary measures. All this, respecting the rights of workers and the requirements established in the applicable regulations.

The FCC Group reserves the right to modify this policy at any time, adapting it to changes and technological developments as appropriate and/or necessary, without prejudice to duly informing the recipients of that policy.

4. Technological Resources General Rules

b) The Technological Resources are Company work tools so their use must be aimed at the fulfilment of the services for which the user was hired, and must be used in a manner appropriate to their nature and their professional purposes.

c) Given that the Technological Resources and the information contained or managed are owned by the Company, and based on this nature of work tools, both are subject at any time to its inspection, monitoring and auditing. Consequently, the worker has no expectation of privacy in the use of Technological Resources.

d) Notwithstanding the above, a private use of them is authorised, provided that it is moderate and punctual and without affecting work and productivity responsibilities. Said use will not generate expectation of privacy nor will it be an impediment for the Company to have access to the professional information stored in the different devices used by the user, and therefore they must refrain from including aspects related to their privacy that they do not wish to be known by third parties. In particular, it is not allowed to treat emails or messages as personal with an expectation of privacy or store personal information in folders identified as such in the Resources to which this policy refers.

e) The different access permits to the Resources, networks, systems, and to the information itself, located in the FCC facilities, or in facilities hired by the FCC Group, will be granted after a formal approval process that will ensure that each user has access, solely, to the resources and information necessary for the carrying out of their duties.

   The remote connections to the FCC network will only be made through the Resources designed for this purpose, this being the only access method allowed, and always with the prior authorisation of the Information Systems and Technologies Division.

   All external teams that intend to connect remotely to the Company's network must have detection, prevention and correction of malicious code controls implemented and correctly updated. It will also be necessary for them to have both the operating system and the rest of the installed software updated.

f) Each user must take due care of the Resources assigned to them, preventing other people from accessing (including mere viewing) the work tools assigned to them for their use.

   In line with the foregoing, users must not access the Resources assigned to other users or the professional information contained in them, unless expressly authorised and for the needs of the Company. In this case, it will be necessary that in the request for access to the Resources assigned to other users, the need for said access is expressly specified.

   With a specific nature, it will be necessary to adhere to the Password Security Standard that is in force at all times. All the Technological Resources will be initially configured so that after a period of inactivity, they show the login screen again requiring the entering of the password for their unlocking. This safeguard will always be active and it is forbidden to disable it.

g) Prevention of malicious code: The most well-known malicious code is the computer virus, but this term is broader and refers to any program that aims to infiltrate the computer, without the knowledge of the user, in order to damage the safety of the machine or other systems. The prevention, detection and correction controls available to the information systems are not enough to fight against the malicious code. To protect against these threats, the user must:

   - Be especially careful when using the Internet or email, as these are the most common means of transporting and transmitting malicious code.

- Do not download or use software or executable files of an unknown or non-corporate origin.

- Contact the Servicedesk and the Information Security and Technology Risk Management Department (sdseguridad@fcc.es) immediately if you suspect the existence of malicious software and/or any similar anomaly.

h) The violation by a user of any rule of this Policy will be considered as a breach of contract that may lead to the taking of appropriate disciplinary measures in accordance with current regulations.

i) In order to ensure digital evidence that could otherwise be destroyed, the FCC Group may remove the user from the Technological Resources that he/she has been assigned with at any time and without prior notice, with the user having to make them immediately available to the Group.

5. Specific rules relating to equipment/hardware

Hardware (or equipment) is the set of physical or material elements that make up an information system, such as desktops or laptops, fax machines, printers, monitors, smartphones, USB devices, external hard drives, memory cards, tablets, landlines, mobile phones or similar or equivalent devices.

The following rules apply:

- Installation and maintenance of equipment: the user may not make any changes, alterations or modifications without the express authorisation of the Information Systems and Technology Division. The installation of new equipment must be carried out only through the corresponding department, being prohibited the installation of any additional hardware element without authorization by the FCC Group. Any different type of maintenance must be consulted with and approved by said Division.

- In the event of loss or theft of a portable device containing information classified as sensitive or that contains personal data, the party responsible for the lost data (Data Controller in the case of personal data) must be informed immediately and the Information Security and Technological Risk Management Department (sdseguridad@fcc.es) to enable appropriate measures to be taken to minimise possible impacts and to be able to comply with the requirements of applicable local regulations.

- In FCC's facilities, work must be carried out with Resources owned by the company. If it is necessary to implement or use third-party Resources, they must comply, at least, with the technical and security requirements established in this document and/or those detailed by the Company at any given time.

- The use in the FCC facilities and during working time of any Technological Resources belonging to the worker must be done with due moderation and respecting the rules established in this Policy, and provided that it does not harm work responsibilities and contribution to productivity.

- It is forbidden to connect the Technological Resources of the worker to the corporate network unless previously and expressly authorised by the Information Security and Technological Risk Management Department.

6. Specific rules relating to software

The software is the set of logical elements of an information system, such as applications, programs, an operating system, databases, etc.

The following rules apply:

- **Acquisition of software:** The applications and programs that FCC owns or holds the right to use will be contracted according to the procedures in force at the FCC Group and taking into account the standards established by the Information Systems and Technologies Division.

- **Software installation:** each equipment or piece of hardware will contain the applications and programs necessary to facilitate the correct performance of the duties of the users for which it is intended. The user must justify his/her requests for the installation of new software, which must be approved by the Information Systems and Technologies Division. It is prohibited, in addition to the conduct prohibited in general in this Policy, to:

    - Download and install, without authorisation from the Information Systems and Technologies Division, or the Department to which it has delegated, any software or computer application on the user's own initiative.

    - Download, install, access and/or use software that is not licensed or 'pirated' (unlawful conduct that can entail serious criminal and civil liabilities depending on the national regulation of each State/Country, in addition to putting in obvious risk both the computer equipment and the information it contains)

    - Install digital certificates that can be used to represent any FCC Group company, without prior authorisation from the Information Security and Technological Risk Management Department.

    - Copy, without authorisation, the software or applications installed in the Technological Resources or try to decompile them, reverse engineer, access their source code or access them through unauthorised means

    - Use software that allows to disable, modify or render ineffective the security measures and controls established by the Company or to carry out actions intended to bypass said controls.

    - Any request to install corporate software that may alter security settings (e.g. modify operating system firewalling rules, etc.) or disable information security tools (e.g. disable EDR, etc.) must be previously agreed and authorised by the FCC Group's Information Security and Technological Risk Management Department.

- **Software maintenance**: software maintenance includes its entire life cycle (installation and configuration, maintenance, repair, destruction and testing). The user cannot carry out any maintenance on the applications in any of the phases of their life cycle, unless expressly authorised by the Information Systems and Technologies Division.

7. Specific rules applicable to email users

Electronic mail (or email) is a network service that allows users to send and receive electronic mails (also called emails) through electronic communication networks. Its use must be carried out primarily for professional purposes, and personal use must be occasional. In both cases, the employee must not include information that may affect private or intimate matters that he/she does not want to be known by third parties, given the control powers of the Company to which reference has already been made in this Policy, without any expectation of privacy or intimacy in this regard.

Additionally, the following rules apply:

a) Mass emails cause problems for the Company, since, among other damages, they can collapse the network and can generate very costly losses in work time of all the users who receive the message. Therefore, in general, communications with general content or intended for large groups of people within the organisation should preferably be channelled through other information, communication or dissemination tools other than email (such as: circulars, news, announcements, etc. Displayed on the Intranet), that on the one hand do not put the network at risk and on the other hand do not cause the interruption of the recipients' work activity.

   In the event that a user needs to send mass email for business reasons, they should contact the Information Systems and Technologies Division to initiate the process of sending mass emails.

   The use of email distribution lists will be carried out restrictively for the organisation of work or the operation of the business.

b) In order to avoid the breakdown of the email service and the involuntary congestion of users' mailboxes, the size of documents, files, etc. that are attached to an email must not exceed the maximum size in any case authorised by the Information Systems and Technologies Division.

   In the event that for business reasons it is necessary to attach something of greater size than that allowed, the user must request authorisation from the Information Systems and Technologies Division.

c) The correct use of the email service, which in no case should harm the worker's work responsibilities or productivity, means that the user must not use it for the actions generally prohibited in this Policy or for the following:

   - Violating the Information Management and Information Security and Cybersecurity Policies of FCC Group.
   - Accessing and/or using the email account of another user without prior authorisation.
   - Impersonating, or attempt to impersonate, another user using technical resources.
   - Pretending to belong to a company outside the FCC Group.
   - Starting or participating in the spreading of chain letters or similar actions.
   - Using private mailboxes offered by any Internet provider for professional purposes related to the FCC Group.
   - Using email as a communication tool for sales or other commercial purposes that are separate from the Company.

- Sending or requesting messages, information, files or materials with explicitly sexual content, or that are discriminatory, which may be offensive, defamatory, threatening or insulting to any person.

- Sending or requesting messages that include audiovisual, musical, multimedia or any other kind of content that, not being related to the user's duties, may hinder the traffic of the corporate network.

- Deliberately forwarding emails sent or received (or their attachments) through a corporate email account to external email accounts. Also, the blind carbon copy (BCC) feature must not be used to send the aforementioned information to external accounts.

- Sending emails of a professional nature or related to the FCC Group Companies from the user's private email addresses (hotmail, gmail or other accounts) or from names outside the FCC Group.

- Carrying out (or attempt to carry out) technical actions that prevent the emails of a corporate mailbox from the last six months from being kept online, in such a way that the FCC Group is prevented from maintaining a backup of them.

In this regard, in relation to the emails sent or received through the Company's mail server and other channels that may contain information, in order to avoid the loss of the information contained within them, a full backup of all items will be stored. Said backup copy shall be used for due care regarding relations with customers, suppliers, public authorities, administration and employees of the Company, as well as the control of compliance by users of the instructions established in this document.

The above rules, with the necessary adaptations, are applicable to any other digital communication system, especially messaging services or similar.

8. Specific rules of use relating to the Internet

The Internet is the global computer network that uses a telephone line to transmit information.

The FCC Group Companies provide users with access to the Internet based on the responsibilities or tasks assigned to them. The user is responsible for the material displayed and downloaded from the Internet. Therefore, they must use the Web responsibly and lawfully.

As is the case with the other Group Resources, users can only use the Internet provided by the Company for lawful and professional purposes and without harming their work and productivity responsibilities. Use for personal purposes may only be occasional. In both cases, the user must not disclose with their connections any information that may affect private or intimate matters that they do not wish to be known by third parties, given the powers of control of the Company to which reference has already been made in this Policy and also applicable to these connections, without there being any expectation of privacy or intimacy in this regard.

It is strictly forbidden to use the Internet for the prohibited conduct included in this Policy and also to:

- Download and/or install software, executable files or databases from the Internet on to equipment. If the user needs it to carry out any duties, they shall request authorisation from the Information Systems and Technologies Division.

- Use software to download or exchange peer to peer files or folders as well as any other software, downloading music, films, videos and/or games or multimedia playback services for leisure purposes, or viewing any video and/or streaming any multimedia product or similar use.

- Access websites expressly forbidden by the Group's internal Policies or that contain inappropriate content or that generate doubts about their legality, avoiding also those websites that automatically redirect to others on which it is not possible to establish control or any supervision. Likewise, it will be forbidden to try to modify the security parameters implemented in the Corporate Internet Network and Systems in order to try to access these websites.

- Use the connection provided by FCC for access to the Internet with any private device or outside the group, unless authorised by the Information Systems and Technologies Division.

- Include or upload personal data, restricted information (confidential, secret and internal), sensitive or strategic information for FCC on websites/URLs that use artificial intelligence, unless they have been previously authorised by the Information Systems and Technologies Division.

- Using systems, interconnecting with corporate applications and/or using web pages/URLs that have artificial intelligence, unless expressly authorised in advance by the Information Systems and Technologies Division.

When accessing the Internet or any other computer network, the technical and security requirements specified by the FCC Group in the corresponding internal regulations must be met.

9. Specific rules relating to audiovisual media and geolocation

For reasons regarding supervision and control of the provision of work and safety of people and goods or avoidance of occupational hazards, the Company may install means of capturing images or movement (cameras, sensors, etc.) in facilities or other technical resources that belong to it. Initially and regularly, both legal representatives and workers will be informed of said installation and it will be carried out with the minimum limitation of rights involving privacy and the image of those affected and excluding places such as changing rooms or toilets.

The means of recording sounds can only be used when they are strictly necessary for supervision, security or risk prevention reasons, with minimal impact on the rights of those affected and adequately informing them and their representatives

Also for reasons regarding supervision and control of the provision of work or safety of people and property or avoidance of occupational hazards, the Company may install the appropriate geolocation systems in its vehicles and other resources owned by it. Initially and regularly, both legal representatives and workers will be informed of said installation, with the minimum limitation of their right to privacy.

Said systems must be disconnected exclusively when the resources supporting such systems are held by workers in temporary periods that are not considered working time, in accordance with the rules that are determined in this regard.

The data that may be obtained by the resources and systems included in this section will be subject to the regulations on protection of personal data provided for this purpose.

10. Specific rules of use relating to data networks

A data network is an element of infrastructure designed to support information transfer via data Exchange.

The use of the data networks of the Companies of the FCC Group must be governed by the correct use of the resources that form part of them, being expressly prohibited the following activities in addition to those generally prohibited in the Policy:

- Attempting to access, read, delete, copy or modify the files of other users without the knowledge and consent of the author or, as the case may be, the Company.
- Trying to access restricted areas of FCC's computer systems, its other users or third parties.
- Destroying, altering, deleting, rendering useless or damaging the data, programs or electronic documents of FCC, its other users, or third parties.
- Trying to modify and o/or increase a user's level of privileges in the system.
- Trying to decrypt the keys, systems, encryption algorithms or any other security element that is included in the FCC Group's telematic processes.
- Voluntarily obstructing the access of other users to FCC equipment and systems, for the mass consumption of computer and telematic resources, as well as carrying out actions that damage, disrupt or generate errors in said equipment and systems.
- Introducing programs, viruses, macros, applets, ActiveX controls or any other logical device or sequence of characters that cause or are likely to cause any type of alteration in IT resources and/or in the information managed therein.
- Introducing, reproducing or distributing computer programs not expressly authorised by FCC, or any other type of work or material owned by third parties under intellectual or industrial property rights.
- Making the information, equipment and software provided by the Company available to unauthorised third parties.
- Sharing resources and information (files, directories, etc.) without the necessary security mechanisms (depending on the risk and the type of information) and available in each operating system and/or applications that guarantee the security of its computer and the network.
- Connecting using FCC Group technology via VPN services, anonymous proxies or any other anonymisation service not authorised by the FCC Group.
- Access the FCC Group's technological resources through any browser that allows connectivity to/from the Dark Web or Deep Web (such as the Tor browser).

11. Specific rules of use relating to social networks

This Policy, which develops the provisions in this regard in the Code of Ethics and Conduct, applies to the use of social networks for both corporate and personal use, the latter only in cases where personal use may have significant consequences or implications for the Company. It also applies to its use either during the working day or outside of it, and applies regardless of whether social networks have been accessed through Company equipment or the worker's personal devices.

In this sense, the image of the Group is one of its most valuable assets that, as such, must be protected, and this is in order to preserve the trust of shareholders, customers, partners, employees, suppliers, authorities and society in general.

The Company uses its corporate networks in accordance with the principles, values and rules reflected in its internal policies, and especially in its Code of Ethics and Conduct, as well as current legislation. Any user accessing said networks must do so in accordance with that regulation.

Therefore, if the duties of an employee require him/her to make use of the corporate network, this must be done in a responsible manner and he/she must have the appropriate authorisation in this regard. Any information published in the Company's internal channels cannot be published on external media without the authorisation of Communication, Corporate Marketing and Branding Management.

In any case, the user should never use the corporate channels for their own personal communications. The user must not create or register an account or channel on social networks on behalf of the Company, or any member of it or their own, without the prior authorisation of the person in charge of the Company. Only Communication, Corporate Marketing and Branding Management is authorised to open digital channels (social networks, websites, blogs, etc.) on behalf of the Company. In the event of detecting profiles not authorised by the FCC Group that make unauthorised use of its trademarks/logos or impersonate its identity (or that of any of its member companies), FCC Group may immediately request the removal of the unauthorised profile from the corresponding network or website.

The use in the FCC facilities and during the working time of any personal social networks of the worker must be done with due moderation and respecting the rules established in this Policy, and provided that it does not harm the work responsibilities and contribution to productivity.

The personal use of social networks cannot be carried out in breach of the Code of Ethics and Conduct, in particular, regarding discrimination, harassment or intimidation of other members of the Company or third parties related to it. Likewise, no comments may be published on confidential or reserved business aspects of the Company, or others that may damage its reputation.

12. Specific rules of use relating to AI systems

In a work environment, Artificial Intelligence models or systems (hereinafter '**AI System'**) can improve efficiency, optimise processes and increase productivity by automating tasks, analysing large volumes of data or supporting decision-making. However, their use must be responsible, ethical and aligned with the principles of transparency, security and fairness.

The use of AI systems by employees working for FCC Group companies must comply with the following guidelines:

- Cybersecurity: Only AI systems approved by the FCC Group may be used, and the use of unauthorised platforms or services is therefore prohibited.

- Review of instructions and Terms and Conditions: AI Systems have Terms and Conditions and, in many cases, instruction manuals. Without prejudice to the training on AI Systems provided by the FCC Group, users must read these texts before using the AI Systems, in case they need further details to understand their purpose, characteristics, shortcomings, etc.

- Human supervision: it should not be assumed that the results generated by AI systems are always correct or free from errors or biases. Therefore, they must be reviewed and validated before use or application, particularly and mandatorily in the case of high-risk AI systems. This review consists of a simple validation of the veracity and accuracy of the result.

- Input data quality: When entering data into AI systems, it is essential to ensure that it is representative and accurate to avoid bias or inaccurate results.

- Transparency and notification: information and transparency will be particularly relevant in the practices of those FCC Group departments linked, where applicable, to high-risk AI systems, as defined in Article 6.2 and Annex III of the EU AI Act, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence.

- Intellectual property: content generated by AI systems such as audio, images, videos, etc. may be protected by intellectual or industrial property rights (for example, if it includes a trademark or a work of art). Therefore, the use of such content must be duly aligned with applicable legislation and the policies and practices of the FCC Group.

13. Power of monitoring the proper use of Technological Resources

Automatic or manual search

In accordance with the rules established previously, and especially regarding the guarantees of regular information to users and their representatives on the rights of supervision and control of the Company and the absence of expectation of privacy or intimacy that they have when using Technological Resources, said surveillance power will have as main general rules the following:

- As a general rule, there will be two types of controls over the Technological Resources. One of a regular, preventive and random nature, tending to identify any use of those means contrary to the rules set out in this Policy, and especially violations of fundamental rights of individuals or obligations that may jeopardise the security and assets of the Company or its staff. Another, of a research and specific nature, when the Company has an indication that a user or group of users are carrying out acts or actions contrary to this Policy.

- In equipment, the access made by the FCC Group will consist of detecting, through automatic or manual searches, whether the equipment store illegal software that infringes (or may infringe) the intellectual or industrial property rights of third parties, or software that is not authorised by the Company. Likewise, it will also consist in searching through automatic or manual searches for terms that could reveal improper conduct such as harassment, discrimination, anti-competitive behaviour, disclosure of secrets, etc. Likewise, it will also consist of identifying calls made from or received on a Technological Resource.

- Regarding email folders and the information contained in the emails, it will consist in searching through automatic or manual searches for terms that could reveal improper conduct such as harassment, discrimination, anti-competitive behaviour, disclosure of secrets, etc.

- A full backup copy of all email items sent or received through the FCC mail server and other channels likely to contain information will be stored.

- The ability to monitor and control corporate email accounts is not limited to the content of messages issued and received through them, but also to headers, traffic data and any other information related to emails.

- Regarding the use of the Internet and the Intranet by the user, it will consist of automatically accessing the registration of web pages opened by the user to detect content not related to the activity of the FCC Group (for example, time and date of start of session, IP address that allows to identify the equipment from which it is accessed, user, web page or URL accessed, date and time of access). Likewise, terms will be searched for that could reveal improper conduct such as harassment, discrimination, anti-competitive behaviour, disclosure of secrets, etc.

- The Company may also block the possibility of carrying out certain actions (for example, sending certain information by email), and creating an alert in case a user tries to perform them.

- The criteria and rules set forth will be applied in a similar way to the other Resources made available to users.

Extraction of information

In the event that any breach of this Policy is detected or there are reasonable grounds for suspicion of such a breach, the FCC Group will assess the possibility of extracting information from the corporate assets involved in order to verify whether or not misconduct has occurred, with a view to taking the appropriate measures within its power of management and control.

Any request made by an area, department or internal part of the FCC Group, regardless of its functional or hierarchical dependence, to obtain information related to the use of Technological Resources must follow the corresponding process regulated in the Group, and comply with the following suitability, necessity, reasonableness and proportionality requirements already included in the surveillance and control powers provided in this Policy:

Be suitable and necessary	It is considered that there is no other measure that allows obtaining the necessary information for the matter under analysis or investigation, or that if it exists, it is not sufficient or viable.
Be reasonable	Be due to objective reasoning, justified and not arbitrary, not incurring abuse of the rights that the law gives to the employer.
Be proportional	Be respectful of the right to privacy, seeking minimal interference, and is limited only to the matter or issues under investigation or analysis and to the person or persons involved, in a specific period of time. In all cases, key terms that are relevant and appropriate to the purpose to be achieved will be identified, not using generic terms that do not sufficiently limit the content that includes relevant information. They can be words or strings of words and/or characters, as well as email addresses or proper names.
Be duly approved	It must receive approval by the responsible parties in each case.

14. Right to digital disconnection

The users of the Company's Technological Resources that imply information and communication should not be connected to them outside of their working hours, provided that during this time they do not have to fulfil any obligation or responsibility that cannot be postponed for their job.

All FCC Group Companies are committed to the well-being of their workers and recognise the right to digital disconnection as a vital element to achieve a better organisation of working time in order to respect personal and family life. In this way, and in general, we will try not to send messages or make calls outside of the working day.

In order to promote and guarantee the right to digital disconnection, the Company will develop training activities, raising awareness among staff on the reasonable use of technological tools.

When the user must regularly and conveniently authorise their work remotely, including that carried out in their own home, or be subject to a particularly flexible work time distribution, they will also be subject to the previous regulation regarding digital disconnection, with the characteristics that may be considered.

15. Guarantees of information regarding legal representatives, workers and reception of this Policy

The Company will initially inform the legal representatives of the workers, and the workers themselves, of the implementation, development and conditions of establishment, use and purpose of the Resources and systems included in this Policy, as well as their updating. This information may be provided individually and collectively, and will be developed by any means, digital or physical, to ensure effective reception and knowledge. Both representatives and workers must acknowledge receipt of said information and knowledge.

16. Suspension or termination of the relationship with the user

The assignment of the use of the Resources to users for the carrying out of their professional service is only maintained while the relationship with the Company is ongoing.

From the moment in which the termination of the relationship occurs for any reason, access to said Resources will be denied. The foregoing provision may be applied in the case of the opening of contradictory proceedings for very serious misconduct by a user.

Notwithstanding the foregoing, in a manner that is contemporary or immediately prior to the termination of the relationship, the user will be allowed access, under the supervision of the Information Systems and Technology Division or the person delegated by this Department, so that it can erase and/or extract personal information.

After the termination of the employment relationship, the Company will have access to the Resource and to the information contained within it without any limitation, erasing the personal information if the worker has not done so already.

In the event of termination of the relationship with the Company, the user in possession of any Resources will have to return them on the contract's termination date, complying with the expected return process.

In turn, the responsible party of a user who ends their relationship with the Company will have the obligation to request the return of the Resources.

The above rules, with the adaptations considered necessary, may also be applied when the employment relationship is suspended, especially for a long duration.

17. Management and response to security alerts and incidents

The FCC Group's Information Systems and Technology Division has a team of professionals responsible for providing support in all matters relating to information system applications and tools.

For its part, the FCC Group's Information Security and Technological Risk Management Department provides cybersecurity monitoring services (which review everything that happens in the technological environment at all times to detect any type of threat to the FCC Group with the intention of applying any type of technical measure that helps to reduce or mitigate the security risks detected). Among others, the security operations centre (SOC) and similar services such as Cyberthreats and Threat Hunting stand out.

1. Any user who experiences an incident relating to information systems must immediately report it to the FCC Group's Information Security and Technological Risk Management Department, without taking any action on their own regarding the resource that has suffered the incident, nor turning it off, restarting it or resetting it. The FCC Group's Information Security and Technological Risk Management Department will assess and classify the incident as soon as possible and respond to the user who has suffered the incident.

2. All users must comply with the content of the information security alerts issued by the FCC Group's Information Security and Technological Risk Management Department, as well as respond to any requests for information they may receive from the latter for the purpose of clarifying a specific event or suspicion.
   In the event that no response is received from the user in a timely manner, the FCC Group's Information Security and Technological Risk Management Department may apply appropriate technical and/or organisational measures to reduce or mitigate the potential threat to the Technological Resources (such as blocking applications, isolating equipment or servers, deactivating users, rotating credentials, revoking active sessions, etc.).

18. Basic data protection information

	Additional information about the processing of Personal Data
Data Controller	Fomento de Construcciones y Contratas, S.A., with Spanish Tax ID A28037224, Information Security and Technological Risk Management Department. Federico Salmón, 13. 28016 (Madrid). Web www.fcc.es and contact through protecciondedatos@fcc.es
Purpose	Preventing information leaks from FCC Group entities, monitoring professional activity, verifying that there are no data breaches and/or improper and/or illegal uses of technological resources, and compiling and processing information security in the Group's systems.
Lawfulness of processing	Purposes based on the processing necessary for the satisfaction of legitimate interests pursued by the Data Controller (Entity) and for the performance of a contract, where applicable. (The legitimate interest of the Data Controller lies, among other things, in controlling the security of networks and systems and controlling information leaks to competitors and third parties, as well as, where applicable, verifying the correct performance of the services provided).
Rights of data subjects	Access, rectification, erasure, portability, restriction, withdrawal of consent or objection (where applicable) by emailing protecciondedatos@fcc.es. If you believe that your data has not been processed in accordance with data protection regulations, you can contact the Data Protection Officer directly (protecciondedatos@fcc.es). In any case, you may file a complaint with the Personal Data Protection Agency.
Additional Information	The User may have additional and complete information through the 'Data Protection' section located on the FCC Intranet (https://fccone.fcc.es/) or by request to protecciondedatos@fcc.es or through a request in paper format to the Human Resources Department