

Self Protection



Corporate
Security

Security and General Services Directorate

March 2022

Self Protection Manual

1. Object & security regulations framework
2. Self Protection in FCC
3. Responsibilities for everyone
4. Corporate Security department
5. Security Planning
6. Crisis Management System
7. Traveller Protection
8. Security Tools

Object & security regulations framework



The protection of employees against the security risks arising during their work at FCC is everyone's responsibility. The **FCC Group** must protect its employees according to the Spanish Civil Protection and Health & Safety Laws and Regulations; **Business Area Managers** must promote the security of their staff and their business in accordance with FCC's Security Policy; and **the employees** themselves must contribute to their self protection by using the available FCC security tools and by following a safe behavior that mitigates the risk they face.

The purpose of these self protection guidelines is to promote the FCC employees' security. They briefly introduce the FCC **security framework** (legislation, security policy, responsibilities, security measures & plans); the **basic guidelines for self-protection behavior** and the **security tools** made available by the FCC Group and the Security Directorate.

These contents are just an elementary basis that must be complemented by other training and informative actions, carried out by the relevant departments and focused on the profile and position of each employee. The protection against some specific situations of aggravated risk will be dealt with in separate documents.

Duty of Care and Self Protection

According to Spanish Health and Safety regulations, the employer has a **duty of care** that obliges him to guarantee the health and safety of his employees in all aspects related to work. The employer must inform all employees about the security job related risks they face and the mitigation measures on place. Furthermore, the employer must make sure that all employees receive enough and adequate theoretical and practical training.

On the other hand, Spanish legislation takes into consideration the concept of **self-protection**. This is defined as the set of actions and measures aimed at preventing and controlling risks to people and property, providing an adequate response to potential emergency situations and guaranteeing their integration with the public Civil Protection system. The regulation also establishes the conditions in which premises and buildings must have a specific self-protection plan.

In a broad sense, both the employer's duty of care and the concept of self-protection are applicable not only in Spain, but also abroad, honoring the regulation of each country. Particular attention should be paid to the risks derived from the change in the work environment due to a transfer overseas (geopolitical risks, travel risks, health risks, etc.)

Self Protection in FCC



FCC understands self-protection as the set of actions and measures aimed at preventing and controlling safety and security risks to FCC employees and at providing an adequate response to emergency situations.

The self-protection system is made up of an organization, plans, tools and training.

The risks considered are all those to which employees are exposed:

- In the development of their professional activities, such as extortion, threats, robbery and other antisocial activities that occur in the workplace.
- During travel abroad and in the case of international assignments throughout expatriation, including family members.

The **FCC Group's Security Strategy** abroad establishes the general guidelines for the Group's Security Policy, for the organization of the Corporate Security department and for the setting-up of the Crisis Management System.



Responsibilities for everyone

FCC Group Security Policy (May 2015) points out that:

All FCC Group members:

Should be concerned with creating, achieving and maintaining a secure and steady work environment in which to achieve our goals and purposes free from fear, malicious interruptions or harm to people and assets.

The heads of the Business Areas:

Cooperate in the definition and implementation of the Security Policy

The Departments Directors:

- Are responsible for the dissemination and compliance with FCC security policy
- Cooperate with the Corporate Security Department in the security training of its personnel



Responsibilities for everyone



The main objective of the Corporate Security department is to propose, implement, monitor and control preventive and reactive security measures for the protection of FCC Group employees and assets.

To achieve this the CSD:

- Manages the specific protection that must be provided to travelers, expatriates, executives or own personnel in higher risk situations.
- Prepares Emergency and Crisis Management Plans and contributes to Business Continuity and Resilience Plans.
- Develops security training and awareness programs

All employees:

- Must know, read and comply with the Security Policy
- Are entitled to receive security information and training

Corporate Security Directorate



To support FCC Group personnel the Corporate Security department has:

- A national structure with the Security Directorate at Madrid & Barcelona FCC HQs.
- An international structure and deployment with a person in charge for each of the following areas:
 - Middle East & North Africa
 - The Americas
 - Europe
- A Security Control Centre at Las Tablas – Madrid available 24/7 to attend incidents and emergencies.

FCC Control Room

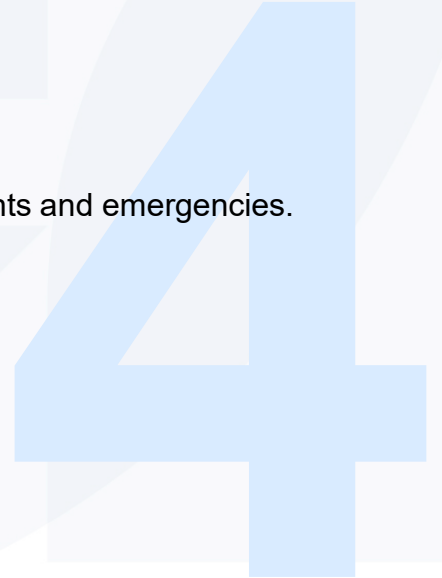
+ 34 91 757 38 00 (24 hours)

+ 8707 7631 6183 (satellite– 24 hours)

centrocontrol-LT@fcc.es

FCC

+ 34 91 359 54 00



Security Planning



Security planning must be naturally integrated into business planning to mitigate security risks for employees and the company.

Security plans consist of a set of measures that are adopted in each country or project according to the level of risk. The Corporate Security department can assist in their preparation. They may contain, among other issues, the following:

1. Security situation and risk analysis in the area or project.
2. Regional, local or project mechanisms for monitoring the situation and for crisis management (Local Crisis Committee).
3. Security indicators and security assessment for the establishment of the risk / activation levels of the crisis management system
4. Security measures to be applied at the different activation levels
5. Evacuation measures / evacuation plan
6. Exercises and drills.
7. Organizational Structure and list of FCC Employees in a Project or country.
8. Communications Directory.
9. Alert and Emergency call procedures.
10. Other.



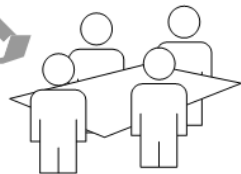
Security Planning



Risk analysis



Security indicators



Local comitee

Alert levels



Plans



- Emergency or CM
- Evacuation
- Personnel protection
- Project Security



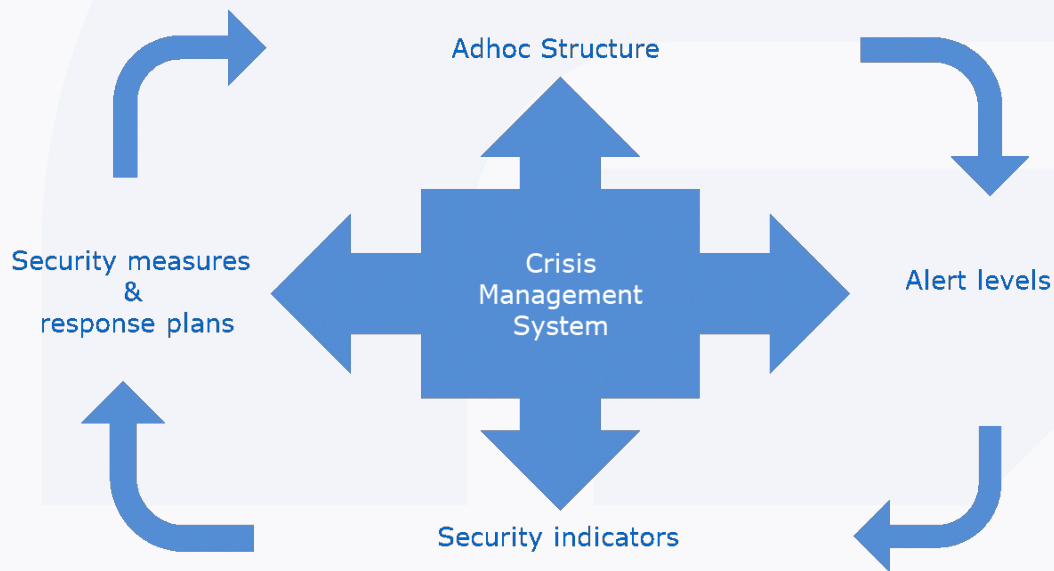
Possible measures



Crisis Management System Elements

To attend to the security of its employees and their families in international assignments, FCC Group:

- Has an Alert and Incident Response System to facilitate the communication of any incidents by the employees while travelling and to be able to attend them swiftly.
- Has a Crisis Situation Management System to respond to these types of situations, when incidents lead to a crisis.
- Keeps active evacuation plans in countries with aggravated risks..



6

Evacuation Plans

The reason to evacuate FCC Group Employees from a country can be:

- A gradual worsening of the security situation.
- An unforeseen and sudden emergency situation.

FCC Group Evacuation Plans are based on a contract with companies specialized in this type of operations.

The decision to evacuate a country is a responsibility of FCC Group's senior management, and is normally taken within the framework of the FCC Crisis Management System.

Evacuation Plans consist of a land evacuation section, in charge of FCC (business area + security department) and an air evacuation section provided by a specialized operator.

Traveller Protection

In order to protect our travellers, they are required to plan their journeys, to adopt an appropriate attitude and to acquire certain skills. **All this is included in these six principles of personal security:**

- 1. Preparation:**
preparation of your displacement is a key principle that constitutes the bedrock for traveler's security.
- 2. Security Awareness:**
stay alert and understand that you are in different environment than usual.
- 3. Low Profile:**
do not attract attention, and don't stand out from the crowd.
- 4. Avoid Routine:**
do not display a recurrent behavior to avoid unnecessary risks.
- 5. Tell where you are:**
keep your contacts, company and relatives informed of your travel plans.
- 6. Self Protection:**
adopt a posture and behaviour that will help reduce your risks.

Travelling is an extraordinary situation, especially when it is abroad. We must be alert and assume that we find ourselves in a different environment, with disparities in temperature, humidity, time or food ...

Acting in advance and spending time preparing for the trip will reduce exposure to risk and allow the traveler to take control of the situation.

1. Preparation

- **Find out** about the destination before travelling.
 - ✓ Check government sites such as the Ministry of Foreign Affairs or the International SOS web site
- Check all the **details** of the trip:
 - ✓ Information about flights, hotels and transport
 - ✓ Contact points at destination
- Check your travel **documents**:
 - ✓ Visas, medical insurance and all necessary permits.
 - ✓ Make a copy of all your important documents and have them available in the email.
- Check the **medical aspects** of the destination with FCC Medical Services:
 - ✓ Medical and dental check-up (fit to travel?), daily medication, vaccinations, malaria pill-type prophylaxis..
 - ✓ Medications: carry prescriptions and original packaging, (with a letter explaining the medical prescription in case of controlled type of medication).
 - ✓ Glasses or contact lenses
- Avoid **social engineering**:
 - ✓ Watch if someone seems especially interested or wants to make contact in a seemingly casual way.
- Make a responsible use of **social networks**:
 - ✓ Some criminals use social networks to obtain information and personal data about employees and their family
- Distribute the **luggage** in a proper way:
 - ✓ Carry essentials in the hand luggage: personal documents, computer, medicines, phone, charger, etc.
- Check that you have a suitable **power outlet adapter**:
 - ✓ Some countries have different outlets than those used in Europe.

Mores.

Are there any cultural "rules" you need to know to avoid offending someone? How do you have to dress? Is it acceptable to show affection in public? Can you take pictures of people? How is alcohol consumption seen in that culture?

Corporal language.

Hand gestures and facial expressions can have very different meanings in different parts of the world.

Manners.

Invitations: If you refuse a meal, will you offend the one who invites you? Should you decline gifts? It is advisable to know at least a couple of words in the local language, so you will show interest, and, in many cultures, it is a gesture that is greatly appreciated.

Personal opinion.

Be careful what you say. It is not convenient to talk about politics or to joke about the government; or about history, religion or the political system.

Meetings.

Do you know how people greet each other? Is it appropriate to shake hands or should you bow your head?

A large, light blue circle is positioned on the right side of the slide. Inside the circle, the text '2. Security Awareness' is written in a bold, blue, sans-serif font. The circle's border is a slightly darker shade of blue.

2. Security Awareness

Do not attract attention. Do not display money, jewellery, credit cards, wallets, purses, cell phones, or cameras. Hide your money in a money belt under clothing. Do nothing to stand out.

Avoid making eye contact with strangers. However, keep momentary eye contact with police officers or security guards. Shunning their gaze can raise suspicion and draw their attention to you.

Avoid talking to strangers. If you have questions, ask uniformed personnel.

Dress appropriately for the circumstances. Avoid looking like a tourist.

Do not leave valuables in sight. Your wallet and phone could be stolen, especially if you're distracted. If you can't leave these items in a safe place, hide these types of things in an inconspicuous bag, such as a backpack.

What in some countries is seen as a normal object, in others it can be a sign of wealth and can attract attention.

Be careful when talking on the phone: It is very common to speak out loud without being aware of it and discuss professional or personal matters in front of strangers.

3. Low Profile

Routine increases vulnerability and multiplies the chances of an assault. Therefore, whenever circumstances allow it, try to:

- ✓ Alter your daily departure and arrival **times**.
- ✓ Use different **routes** and places to get on and off the vehicle.
- ✓ Change vehicles and means of **transportation**.
- ✓ You don't have to be a master of disguise, but try to change your look and not to **wear items** that make you stand out such as hats, certain models of glasses ...
- ✓ Don't **socialize** always in the same places, even if there are few options for it. Make sure to change places, schedules and routes both privately and on your daily work.
- ✓ Use **social networks** properly and make sure your family are discreet as well.

4. Avoid Routine

Report your trip.

Communication is vital for travel security. If no one knows where you are, your chances of getting help if needed will be reduced.

Someone should know your whereabouts both in the office and at home.

A large blue circle is positioned on the right side of the slide. Inside the circle, the text '5. Information' is written in a bold, blue, sans-serif font. The number '5.' is on the top line, and the word 'Information' is on the bottom line.

5. Information

In brief...



6. Self Protection

Security Tools



FCC security department has several security tools to support employees and business:

- 24/7 assistance from Las Tablas Control Center
- International SOS App
- Geolocation and Emergency Call System SAFE ZONE
- COMSEC smart phone call encryption system
- Satellite telephony for emergencies
- Web page



Las Tablas Control Center

The Las Tablas Control Center (LTCC) acts as an assistance center for personnel in transit or personnel in a situation of aggravated risk.



It is attended 24/7 and has the following capabilities:

- Communication systems, including satellite telephony and COMSec.
- Tracking platforms: SafeZone, traveler tracking, ISOS, etc.

LTCC staff can:

- Monitor and assist FCC staff traveling overseas or in a situation of aggravated risk.
- Sends alerts 24/7 to all expatriates and travelers who get their tickets through the FCC Group travel agency.
- Monitor and attend alerts from the SafeZone system.

Situation monitoring and alert messages for employees

En la actualidad contratado con la empresa ISOS.

Se puede acceder a la aplicación a través de equipos de sobremesa o teléfono inteligente.



It offers the travellers different services:

- Access to security information about the country of destination.
- Pre travel advisory.
- E-mail alert subscription for one or more countries of interest. The alert messages refer to travel risks such as:
 - Strikes affecting land, air or sea transportation.
 - Any event that may hamper the mobility in a city or region.
 - Serious security incidents.
- Telephone assistance 24/7 for consultation prior to or during the displacement covering the following aspects:
 - Security assessment
 - Reference of Security services, secure transportation or advice in case of alarming news.

Geolocation and Emergency Call System

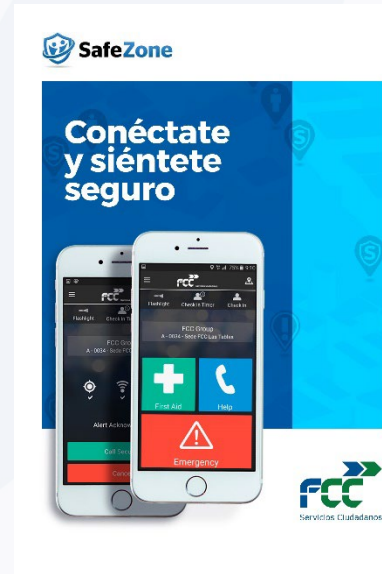
Currently contracted with Critical Arc (SafeZone system)

It is a smart phone application that once downloaded allows to:

- Voluntarily share a user's location with the Security Department.
- Send an emergency health or security message to an FCC Control Center. The emergency message conveys the location of the employee in distress.
- Receive telephone assistance from the FCC Control Center.
- Establish a chat with the Control Center or Country security manager.
- Receive messages by various means in case of emergency situations, generated from the Control Center or Security Department.
- Schedule an alert to go off at a certain time if it is not stopped sooner.

The App is used as the basis for the Alert Management and Incident Response System.

Can also be used for Crisis Management and Evacuations.



Telephone call encryption system

Currently contracted with Indra (COMSec System).

COMSec provides the possibility of encrypted communications to senior managers or those who handle confidential information.

COMSec can be used with any commercial smart phone and provides privacy in real-time communications including Voice over IP (VoIP) and data, using any public operator in the world and through 4G / HSDPA / 3G / EDGE / GPRS wireless networks.

All communications are made through encrypted VoIP systems, so its use requires a data connection.

The system can also provide other services such as encrypted video calls or encrypted instant messaging.

Satellite phone system



FCC Group has a contract to facilitate access to satellite telephony in countries with increased risk.

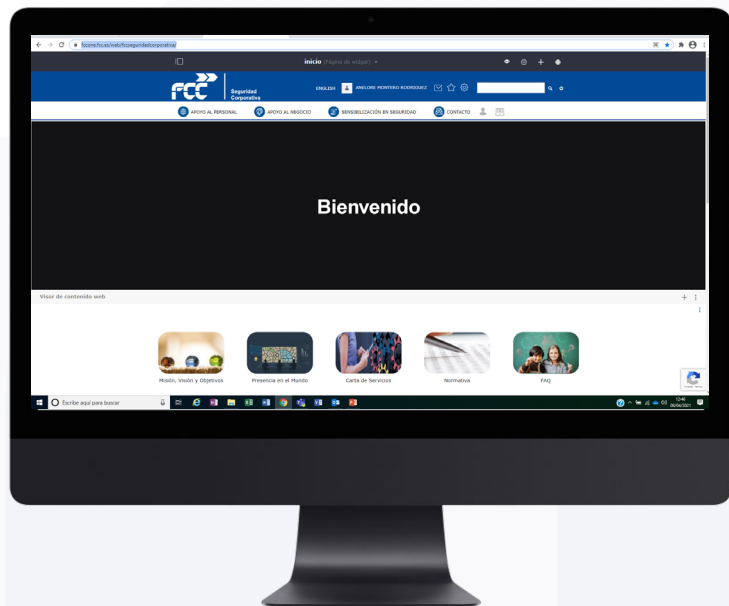
The availability of satellite telephones guarantees communications in case that terrestrial, GSM or GRPS networks are saturated or closed

A satellite phone can make calls to another satellite phone, to landlines or to mobile phones.

In general, FCC Group has a satellite terminal:

- For the Country Manager
- For every project
- For the Regional Security Director

www.seguridadcorporativa.fcc.es



The web page is accessible both from the intranet and from the internet and is meant to:

- Facilitate access to relevant and updated security related information to FCC staff.
- Promote security awareness and knowledge of the Group's security regulations.
- Disseminate security assessments and recommendations.
- Provide support to operational and administrative security processes.



Corporate
Security

Security and General Services Directorate
March 2022