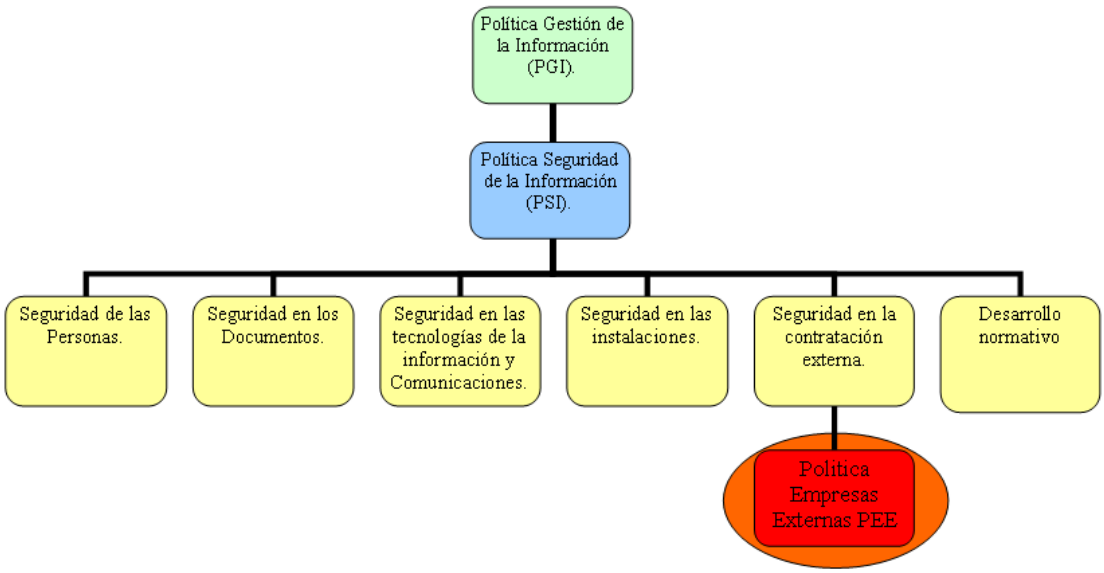
DATA SECURITY STANDARDS

DATA SECURITY POLICY FOR EXTERNAL COMPANIES

ID Code:	**NRM-14-EN**
Version:	1.0
Classification:	FCC_INTERNAL_USE
Approved by:	
Date:	
Intended for:	**FCC Staff Negotiating and/or Receiving Services from External Companies**

INDEX



Given the size of the FCC Group, it is appropriate that certain services required for the achievement of their normal business activities are outsourced, with the intention that these services are supplied more efficiency or under better economic terms.

The protection of data processed and accessed by external companies is crucial to managing FCC data security correctly, considering the nature and volume of the data processed.

The objective of developing a security policy for business activities carried out by external companies is to ensure that external staff also fulfil the data security requirements established by FCC.

The Data Security Policy for External Companies is in line with FCC's current general criteria for selecting suppliers and contracting external companies or partners.

PURPOSE

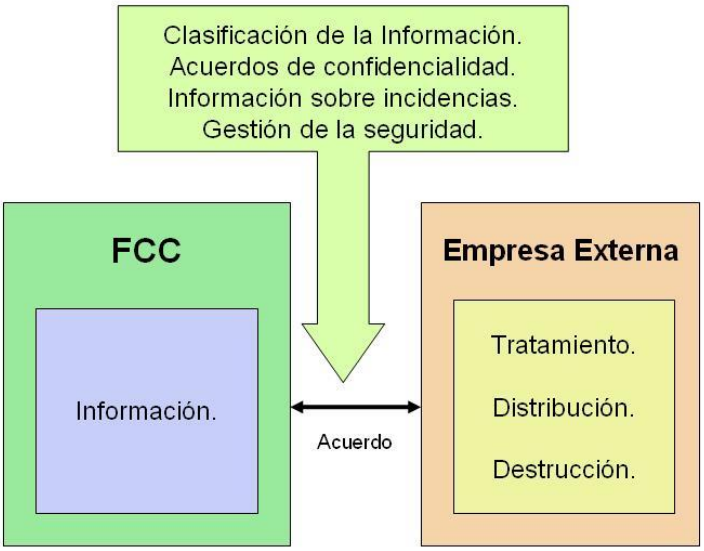
The purpose of this Policy is to protect the confidentiality, integrity and availability of FCC data that is processed by external companies (hereinafter External Companies) for the entire duration of their working relations with FCC.

SCOPE

This Policy applies to all FCC data processed by External Companies as a result of their participation in programmes, projects or agreements with FCC.

PRINCIPLES

- Staff from External Companies are only granted access to FCC data that they need to access A Personal Security Authorisation will be required to access restricted data
- External Companies must apply the protective measures established by FCC for FCC data - most notably the confidentiality measures
- The following actions will require the express authorisation of FCC:
    - The distribution of Restricted Data by External Companies to third parties
    - The declassification or reclassification of FCC data by External Companies
- External Companies cannot use FCC data for purposes other than those stipulated in the partnership agreement
- The processing of FCC data must fulfil the current legislation on privacy and data protection
- Programmes, projects or agreements involving restricted data must not come into force until the principles set out in this Policy have been fulfilled
- External Companies are forbidden from outsourcing services, in full or in part, unless they are expressly authorised by FCC, in accordance with the following criteria:
    - The services outsourced and the identification of the company they have been outsourced to must be stated in the tender or agreement signed between FCC and the External Company
    - All FCC data processed by the outsourcer must comply with the provisions of this Policy



SPECIFIC SECURITY INSTRUCTIONS

The Person in Charge of Contracting, together with the Data Security and Risk Management Department, will determine the need to establish specific security instructions for each project, programme or agreement.

Agreements with External Companies that involve the use of FCC data must state the following as a minimum:

- The methods and procedures regarding the management, classification, processing and safeguarding of data
- The security measures established by the applicable legislation in force
- The security obligations applicable to outsourcing work to third parties
- The requirement for External Companies to provide FCC a list of staff who will access FCC's data, upon FCC's request
- External Companies' commitment to report any security incident that may occur
- The requirement for External Companies to destroy or return data to FCC once the partnership has terminated With regards to the destruction of data, External Companies must provide a certificate accrediting the complete destruction of the data

MANAGED IT DATA SERVICES

IT processes managed by External Companies must **expressly** state in the agreement the requirement for FCC to be aware of and approve:

- The security operating procedures associated to the provision of managed services
- The security measures implemented in the installations where the service is provided
- The security measures established for the communications between centres, provided there are connections to installations outside FCC
- The security metrics and indicators required to analyse the levels of confidentiality, integrity and availability offered by the services
- The option to carry out security audits on the systems where the managed service is provided

TEMPORARY BUSINESS ASSOCIATIONS

Temporary Business Associations, Economic Interest Associations and other types of associations managed jointly with third parties outside the Group, will be subject to the governing principles and responsibilities established in this Policy.

CONFIDENTIALITY AGREEMENTS

External Companies processing FCC Data are sworn to secrecy regarding data confidentiality, and undertake to not disclose, publish or make it available to unauthorised third parties. These obligations will remain in place for two years from the date their relationship with FCC terminates, as stated in the Annexe of this Policy.

The confidentiality agreements included in the Annexes of this Policy must be signed.

DATA DISTRIBUTION

The distribution of FCC data must take place in accordance with the criteria established in this Policy.

The levels of protection for the data must ensure that the media format, transmission and storage are suitable for the classification of the data distributed.

Logs must ensure that all actions carried out during data distribution can be traced.

DATA DESTRUCTION

The destruction of FCC data held by External Companies must consider the following:

- The destruction process carried out must ensure the confidentiality of the data handled and the impossibility of data being recovered or reconstructed
- Certification will be required stating that the data has been destroyed in accordance with the criteria established by FCC

RESPONSIBILITIES

The Person in Charge of Contracting must:

- Include the contents of this Policy in agreements signed with External Companies
- Ensure that External Companies and their installations are capable of safeguarding FCC data
- Process and log the personal security authorisations required for staff of External Companies participating in the programme, project or agreement
- Immediately inform External Companies of any changes to the security levels of data provided to them

- Report any possible data losses (total or partial), or the disclosure of data provided to External Companies, to FCC's Data Security and Risk Management Department

The Unit Responsible for their own data must:

- Authorise the data to be distributed to External Companies' staff, and any staff from companies they have outsourced services to
- Authorise the declassification or reclassification of FCC data held by External Companies
- Be aware of the security controls implemented for FCC data processed by External Companies

External Companies that process FCC data must:

- Ensure that all FCC data processed is protected
- Notify the Person in Charge of Contracting of any incidents affecting the confidentiality, integrity and availability of data
- Inform all third parties they have outsourced FCC data processing services to of the measures established in this Policy

The Data Security and Risk Management Department must:

- Investigate any indication of loss or unauthorised disclosure of FCC data processed by External Companies
- Establish and approve the distribution and destruction methods required to ensure the minimum protection level for FCC data processed by External Companies
- Check the installations and security procedures implemented by External Companies for processing FCC data

REVIEW OF THIS POLICY

This Policy may be reviewed in the following circumstances:

- Whenever there are significant changes to FCC's working processes
- Whenever there are improvements suggested as a result of audits carried out

- Whenever there are changes to the current legislation regarding the provisions established in this Policy

- Whenever there are major technology changes

The information used for the review of this Policy must be notified to the Data Security Department, who must then notify the Data Security Department Committee of this information.

POLICY VIOLATIONS

Any violations of this Policy will be disciplined in accordance with the current FCC disciplinary system, without prejudice to the provisions of the legal regulations in force.

ANNEXE I: MODEL OF CONFIDENTIALITY AGREEMENT BETWEEN COMPANIES

CONFIDENTIALITY AGREEMENT

_____, _____ of _____ 20____

BY AND BETWEEN

THE PARTY OF THE FIRST PART: Mr _____, holder of ID no. _____, acting on behalf of _____ (hereinafter "FCC"), with address at 280__- Madrid, _____, ___- __ floor, holder of corporate tax code _____, authorised in this act by the power of attorney granted before the Notary Public of Madrid Mr _____, on the _____ of _____ _____, under protocol no. _____ .

THE PARTY OF THE SECOND PART: Mr/Mrs _____, holder of ID no. _____, acting on behalf of _____ (hereinafter "The Company"), with address for these purposes at _____, _____, holder of corporate tax code _____, authorised in this act by the power of attorney granted in _____ before the Notary public of_____ Mr _____, on the _____ of _____ _____, under protocol no. _____ .

The parties herein recognise each other's legal capacity to execute this document, and hereby

DECLARE

A Whereas FCC and The Company wish to discuss the possibility of engaging in future commercial relations to _____ (hereinafter the "Purpose").

B Whereas, in accordance with the foregoing, the Parties may exchange confidential data to analyse the achievement of the Purpose, therefore, both Parties covet that such data is understood as Confidential Data. To this end, the term "Confidential Data" shall be understood as any data of this nature, including all explanations or data, even those classified as "personal data" provided under any form, format or media - specifications, diagrams, designs, business plans, strategies, projections and financial statements, technology architecture studies, implementation budgets and know-how, amongst others - provided by FCC or The Company to the other Party of this Agreement, irrespective of how such data is provided (orally, written, visual, pictures, computer files, etc...) and that is facilitated by either party through, under or in consequence of This Confidentiality Agreement; both parties hereby declare their intention to restrict the use and disclosure of this Data.

C Whereas, in accordance with the foregoing, the parties hereunder are governed by the following

S T I P U L A T I O N S

1. The Party receiving the Confidential Data (hereinafter the "Receiving Party") shall treat all data received from the sending Party (hereinafter the "Disclosing Party"), regardless of how the data was received, as strictly confidential and must not disclose or transfer it to third parties without the prior written consent of the Disclosing Party.

2. The Receiving Party shall not use the Data for any purposes other than the Purpose without the prior written consent of the Disclosing Party. Notwithstanding the foregoing, the Parties agree that the use of this Data for any purposes other than the Purpose shall require the execution of another agreement between the Parties.

3. Both Parties agree to restrict access to the Data received from the other Party, which may only be accessed by their employees, representatives or advisers who require access to the Data in order to fulfil the Purpose. Such individuals shall be subject to the confidentiality restrictions established in this Agreement.

4. Both Parties agree to implement the same security measures required to prevent the disclosure of this Data as those implemented to protect their own confidential data and trade secrets. Specifically, whenever Confidential Data includes “personal data”, the Receiving Party shall implement the security measures in accordance with the requirements of the data protection regulations.

5. The aforementioned obligations shall not apply to:

a) Data available in the public domain at the time of its disclosure, or that becomes available in the public domain thereafter, provided its disclosure is not attributable to a violation carried out by the Receiving Party.
b) Data available to the Receiving Party before its disclosure by the Disclosing Party, provided that this fact can be demonstrated via the files of the Receiving Party.
c) Data communicated to the Receiving Party by a third party who obtained the Data from a source other than the Disclosing Party.
d) Data that is independently produced by the Receiving Party at any given time, provided that this can be demonstrated via their files.
e) Data that is disclosed as a consequence of a legal request, injunction or administrative proceedings (in which case, the Receiving Party shall inform the Disclosing Party as comprehensively and as quickly as possible; the data disclosed must only be that requested and must be subject to confidentiality as far as possible).

6. Both Parties herein declare to be part of an organisation constituted by multiple entities that are subject to different jurisdictions, and that they may need to provide the Data to their subsidiaries. To this end, the Parties (both the Disclosing Party and the Receiving Party) agree that:

a) The Receiving Party shall be entitled to disclose Confidential Data to its subsidiaries (as defined below) solely when the Subsidiary requires such Data to fulfil the Purpose. In this case, the Receiving Party shall notify the Disclosing Party of the name of the Subsidiary provided with Confidential Data, and agrees to transfer the Receiving Party’s obligations arising from this Agreement to the Subsidiary.
b) The disclosure of data by/to a Subsidiary shall be deemed a disclosure carried out by/to the Party related to that Subsidiary.

c) Both Parties warrants that their Subsidiaries will strictly fulfil the conditions, terms and obligations indicated in this Agreement.

For the purposes of this Clause 6, "Subsidiary" shall be understood as a legal entity controlled by/controlling/under joint control of one of the Parties; "control" shall be understood as the direct or indirect ownership of more than 50% of the shares which grants the right to vote on the appointment of Directors and/or members of the Board of Directors for as long as the control remains in place, or a similar entitlement that allows control of the Governing Bodies.

7 The confidentiality obligations undertaken through this Agreement will begin on the date the Agreement is executed, and shall remain in force for the entire duration of the relationship between the Parties, and for two years after this relationship terminates. Should there be any breach of the obligations undertaken through this Agreement that resulted in the obligation to compensate for damages caused by the Party who committed the breach, the confidentiality period shall be extended until the resolution of the arbitration or judicial proceedings regarding the obligation to compensate for damages.

8 Data shall be considered the property of the Disclosing Party; upon receipt of a written request from the Disclosing Party, the Receiving Party agrees to return all Data to the Disclosing Party or destroy it, along with all document copies containing such Data.

Regardless, once the Purpose of this Agreement has been achieved, or the Agreement has been terminated, the Receiving Party must return or - if the Disclosing Party expressly requests so - destroy all Confidential Data they has accessed, transmitted or communicated to fulfil the Purpose of this Agreement.

9 Neither Party shall use the name, trademark, commercial name or any other rights without the prior written consent of the other Party.

10 In addition, the Parties acknowledge that, with the exception of this Confidentiality Agreement, neither Party shall be binding upon the other Party in any way until the Agreement has been executed, and neither Party is obliged to execute this Agreement. The Parties agree not to perform, issue or publish any advertisement, announcement or declaration regarding this Confidentiality Agreement, the negotiations carried out between the Parties or regarding any opinions expressed by either Party, without the prior written consent of the other Party, with the exception of when it is required by law.

11 The Parties acknowledge that any breach or threatened breach of this Confidentiality Agreement may pose irreparable damages to the Disclosing Party; therefore, the Disclosing Party, together with others with the right, shall be entitled to implement the necessary measures to prevent any recurring breach or threatened breach of this Confidentiality Agreement.

12 A failure or delay in exercising either Party's contractual rights (including but not limited to the right to request the fulfilment of the terms and obligations under this Confidentiality Agreement) shall not be deemed a waiver of those rights, unless otherwise stated in writing by the Party concerned. This Confidentiality Agreement contains all accords reached between the Parties regarding the aforementioned matters. Neither Party shall terminate, amend or revise this Agreement, or relinquish it verbally, without a written document signed by both Parties' representatives. No representations or warranties have been made other than those expressly set forth herein. Neither Party shall assign or transfer this Confidentiality Agreement to third parties, without the prior written consent of the other party. For the purposes of this Agreement, transfers between FCC companies shall not be understood as "transfers", as well as that resulting from the mergers, conversions or divisions of FCC businesses.

13 All notices, requests, demands, instructions, notifications or other communications made or sent under the terms of this Agreement, must be made in writing and posted (with acknowledgement of receipt) or sent to the corresponding address or fax, which are indicated below. Notices sent by fax shall be deemed effectively received once the receipt confirming the transmission has been issued; notices delivered personally shall be deemed received upon delivery; notices sent by post shall be deemed received upon receipt of the delivery confirmation.

To FCC

_____

_____ - MADRID

FAO: Mr _____

Telephone: _____

Fax: _____

To _____

_____

_____ - MADRID

FAO: MR _____

Telephone: _____

Fax:

14 The Company agrees not to seek or maintain contact with other companies regarding the Purpose of this Agreement, or provide Data related to the same.

15 In the event that any of the stipulations set forth in this Agreement are deemed or declared invalid, null, illegal or non-applicable, regardless of the reasons for declaring them as such, the remaining provisions shall not be affected and will remain valid and fully applicable.

16 This Confidentiality Agreement is governed by and must be interpreted in accordance with Spanish Law. The Parties agree to submit any dispute or controversy arising from the interpretation, fulfilment or execution of this Agreement to the Courts and Tribunals of Madrid, expressly waiving any other jurisdiction that could apply.

In witness thereof, the Parties' representatives sign this Agreement, produced on two four-page counterparts with the same content and effects (one copy per Party), in the place and on the date stated in the heading.

FCC _____

pp _____ pp _____

ANNEXE II: MODEL CONFIDENTIALITY AGREEMENT FOR EXTERNAL COMPANIES

CONFIDENTIALITY AGREEMENT

_____, _____ of _____ 20____

_____ (FCC company name), holder of corporate tax code _____ (hereinafter the "COMPANY") and _____ (name of company contracted by the FCC company), holder of corporate tax code _____ (hereinafter the "SERVICE PROVIDER") have entered into a _____ (state type of legal relationship - agreement, contract, partnership agreement - between the Company and the Service Provider, by virtue of which the Service Provider's staff will provide their services at the Company's premises) on _____ (date).

By virtue of the foregoing, the SERVICE PROVIDER's staff shall be relocated to the COMPANY's premises in order to provide the services included in the scope of this relationship.

To this end, the COMPANY uses this document to notify and inform Mr/Mrs _____ (state Partner's name), holder of tax ID no. _____ and employee of the SERVICE PROVIDER (hereinafter the "EXTERNAL PARTNER"), of the following:

1. For the purposes of this document, all data directly or indirectly accessed by the EXTERNAL PARTNER to carry out his/her professional works at the COMPANY shall be understood as Confidential Data.

Confidential Data may include economic, financial, technical, business, strategic or administrative data, and specifically any data relating to reports, technical know-how, software components, facilities, methodologies, products, services, service users, customers and business activities, as well as personal data stored in any paper or electronic media, and any other documentation classified as exclusive or confidential in accordance with their nature and the circumstances in which their creation or disclosure occurs must be deemed in good faith as such.
PLEASE NOTE: The broad concept of Confidential Data included herein may require clarification in order to fit the factual assumption its use is intended for in this document.

2. The disclosure of Confidential Data by the COMPANY to the EXTERNAL PARTNER shall not be deemed a transferral or rights, expressly or implied, granted to the EXTERNAL PARTNER on any patents, trademarks, copyrights, trade secrets, know-how or other intellectual or industrial property rights currently owned by the COMPANY, or acquired in the future, concerning the Confidential Data disclosed by the COMPANY.

The EXTERNAL PARTNER accepts that Confidential Data shall remain the property of the COMPANY.

3. As the EXTERNAL PARTNER will access, use and process Confidential Data provided by the COMPANY in the exercise of their functions and service provision, they must fulfil the following obligations:

- Follow the instructions established by the COMPANY regarding the use and processing of Confidential Data; this data must not be used and/or processed for purposes other than those previously indicated by the COMPANY.
- Process and use the Confidential Data solely required for providing services to the COMPANY; this data shall be related to their work functions.
- Act diligently to prevent the publication or disclosure of Confidential Data.
- Observe the COMPANY's policies regarding the storage, preservation, custody and destruction of hard-copy Confidential Data.
- Comply with the security measures established by the COMPANY; these measures shall be notified to the EXTERNAL PARTNER in advance.
- Comply with the security measures implemented and required by the COMPANY regarding the processing of Confidential Data during the works, regardless of the media used to store such data. Specifically, the EXTERNAL PARTNER agrees not to provide the password for accessing the COMPANY's Data Systems to third parties, and to use these Data Systems with the required authorisation and for the sole purposes of their works and functions.
- Return all Confidential Data to the COMPANY upon termination of their professional role at the premises of the COMPANY and/or upon termination of their relationship with the SERVICE PROVIDER; the EXTERNAL PARTNER expressly waives their right to keep or preserve any such data.

4. The EXTERNAL PARTNER shall be expressly forbidden to:

- Carry out any communications, assignments, transfers, storage, shipments or deliveries of any Confidential Data accessed to provide their services that has not been expressly authorised; this includes COMPANY staff members not authorised to access the data, or third parties that are not part of the COMPANY's business structure.
- Record and/or reproduce Confidential Data via magnetic, electronic, mechanic, photographic or other media, or print or extract it outside the physical premises where the services are provided.
- Carry out any sort of copying of software programmes that they access while providing their services.

The will be exceptions to the prohibitions stated above whenever the execution of works and the provision of the services require so; in this case, the EXTERNAL PARTNER must notify the COMPANY in advance to obtain an express written authorisation to carry out the activities initially prohibited under the provisions of this paragraph.

Upon termination of the agreement between the COMPANY and the SERVICE PROVIDER, or the employment relationship between the EXTERNAL PARTNER and the SERVICE PROVIDER, the EXTERNAL PARTNER shall be prohibited from using and/or disclosing Confidential COMPANY Data accessed during the provision of the services. All copies or original documentation or media containing Confidential Data must be returned to the COMPANY.

5. The EXTERNAL PARTNER must observe the requirement to maintain confidentiality regarding all Confidential Data accessed during the execution of their works at the COMPANY's physical premises as a result of the legal relationship established.

The confidentiality requirement will be extended for 2 years after the termination of the relationship between the EXTERNAL PARTNER and the COMPANY and/or the SERVICE PROVIDER; however, personal data must be kept confidential for an unlimited period, even after the termination of the relationship between the EXTERNAL PARTNER and the SERVICE PROVIDER.

The EXTERNAL PARTNER agrees to protect the security, integrity and confidentiality of all Confidential Data with the same care it extends to the Confidential Data of the SERVICE PROVIDER; the EXTERNAL PARTNER must carefully and diligently prevent unauthorised use, disclosure or publication of Confidential Data.

This obligation shall not apply to public Confidential Data disclosed by third parties when the EXTERNAL PARTNER had no involvement in this disclosure, or to unrestricted data legitimately disclosed to the EXTERNAL PARTNER by a third party.

6. The obligations and prohibitions under this Agreement do not imply any restrictions to the fulfilment of any other applicable legal requirements, court or administrative orders, without prejudice to the EXTERNAL PARTNER's obligation to notify the court or administrative body of the confidentiality of the data to be disclosed, as well as notify the COMPANY of the Confidential Data to be disclosed.

7. The EXTERNAL PARTNER shall be liable for any violations of the terms, conditions or obligations arising from this document. To this end, the EXTERNAL PARTNER must compensate the COMPANY for any lawsuits, fines, sanctions, actions and/or claims lodged against the COMPANY, provided they result in actions or omissions attributable to the EXTERNAL PARTNER and/or arising from a total or partial breach of this Agreement. The COMPANY shall be entitled to initiate the applicable legal proceedings and/or claim compensation for damages, including reasonable attorneys' fees.

In witness whereof, I hereby expressly and formally declare my commitment to fulfil this Agreement under the terms stated therein.

Signed: Mr/Mrs _____

ID no. _____

REFERENCES

- **Related Regulations**

  - Data Management Policy
  - Data Security Policy
  - Security Policy for Individuals

- **References to the ISO/IEC 27002:2007 Standard**

6.2 Third Party Access Security
- 6.2.1 Identification of Third Party Access Risks
- 6.2.3 Security Considerations for Third Party Contracts

8.1 Security of Activities Prior to Contracting
- 8.1.1 Implementation of Security for Work Functions and Responsibilities
- 8.1.3 Employment Terms and Conditions

10.2 Managing Third Party Services
- 10.2.1 Service Provision
- 10.2.2 Supervising and Reviewing Third Party Services
- 10.2.3 Change Management for Third Party Services

10.8 Data Exchange
- 10.8.1 Policies and Procedures for Data Exchange
- 10.8.2 Data Exchange Agreements

DOCUMENT CHANGE CONTROL

Document Information

FILE NAME:				
VERSION	DATE	CHANGE	AUTHOR	REVIEWED BY
1.0	2009 April	Document creation	Information Security and IT Risks Department	FCC Executive Committee
1.0	October 2019	Revision of the document	Information Security and IT Risks Department	FCC Executive Committee

Please Note: Hard-copies are not controlled

Distribution List

FROM:		DATE	EMAIL
TO:	ACTION	DATE EXPECTED	EMAIL

Action Types: Approve, Review, Report, Archive, Make Decision, Other (please specify)

Version History

VERSION #	DATE	CARRIED OUT BY	DESCRIPTION

END OF DOCUMENT