[November 2017]

FCC
CORPORATE SECURITY AND GENERAL SERVICES DEPARTMENT

GENERAL SECRETARIAT

Citizen Services

Procedure for managing, sending, archiving, safekeeping, querying and destroying documentation in the Central Archive v02

CONTENTS

1 Purpose

The purpose of this document is to set the principles governing the sending, archiving, safekeeping, querying and destroying of documentation in the FCC Group Central Archive, guaranteeing its confidentiality, integrity and availability regardless of the medium in which it is contained and its location.

The information handled by a company is considered one of its fundamental aspects and must therefore be protected as such until the time of its destruction.

This information may be found on various media (paper, magnetic, electronic, etc.) and may be of various natures – strategic, information protected by the Data Protection Law, confidential, etc.

The purposes of this procedure are:

- The standardisation and definition of the processes to be followed for archiving, classifying and managing documents, custody and security, query and destruction of documents, guaranteeing access to the documentation generated with criteria of quality and effectiveness.
- That the protection, organisational and technical measures applied to the documents be proportional to the level of the risk of the information they contain and to their classification level.
- The use of new technologies and the optimising of management resources to improve the documentation handling processes.
- Compliance with current regulations and, especially, the Data Protection Law, within the regulations of FCC:
  - General Standards Manual
  - Information management policy
  - Information security policy
  - NRM-15 Document security
- Equip the safekeeping centres with the maximum security measures (CCTV, accesses control, anti-intrusion, fire extinguishing, etc.) to guarantee the protection of the documents.
- Check compliance with current regulations and the security measures in the installations considered "departmental archives," outside the Central Archive installations.

- Centralise the safekeeping of the documentation archive to free up physical space in the work centres that generate it, resulting in the optimising of the cost of rentals within the FCC Group space policy.

2 Scope

The contents and directives in this document will apply to:

- In Spain

a) All the documents containing FCC Group information regardless of the place of origin, location, nature or physical medium.

b) All the FCC Group installations in which document management processes are carried out.

- In other countries

a) For new works in the Construction Division it is compulsory to follow these to ensure that the criteria for classifying documentation (groups and subgroups) are consistent.

b) For the other divisions (Environment and Aqualia) we recommend following these guidelines whenever possible to ensure it that the criteria for classifying documentation (groups and subgroups) are consistent.

3 Organisation

To achieve the efficient functioning of document management throughout the FCC Group, the **Central Archive in the Corporate Security and General Services Department** is appointed **document manager at Group level** with the following **functions** and **responsibilities**:

a) **Preparation and updating of applicable regulations (external and internal) for the policies, procedures and processes** relating to document management in the Central Archive: receipt, safekeeping, preservation, distribution and destruction.

b) **Ensuring that the procedure is known to** and suitably used by everyone involved, through:

   a. Global and individualised communication actions.

   b. Control of its proper application.

c) Offer a service of **collaboration, training and information** in the document process with technical personnel who are experts in document management (the entire process is covered with in-house human and physical means).

d) **Centralising of spaces** for documentation archiving in the centres in Madrid and Barcelona.

e) **Provision of the necessary means** for handling documentation (scanner, urgent documentation sending service, etc.) to reduce response times to information requests.

4 Definitions

Coordinator: link person for any type of query related to documentation management sent to the Central Archive. May coincide with the user and/or owner.

User: person who enters data in the archive program in the SAP environment. They coincide with the coordinator and/or owner.

Owner: person responsible for: a) ensuring that the classification of the documentation is made according to FCC regulations and is sent to the Central Archive on the set dates; b) authorising the persons who may make documentation queries once this documentation is in the safekeeping of the Central Archive; c) occasionally authorising any person requesting information who is not on the list of authorised persons.

Deputy: person who authorises any person requesting information who is not on the list of authorised persons if the owner cannot do so.

Authorised person: person who needs to know information to undertake his/her functions and who can query or request the sending of documentation archived in the Central Archive according to the degree of authorisation received.

Document manager: person(s) or department responsible for the receipt, safekeeping, querying, distribution and destruction of the documentation in the Central Archive according to the set policies and standards.

Issuing centre: centre, project, contract, branch, division, company, JV, etc, that originated the documentation.

Documentation: any document, regardless of the medium or nature, containing FCC Group information that must be accessible only to the persons with a need to know the information in it and who have a personal security clearance according to the type of information.

Conservation period: period set by an external or Group internal regulation for conserving the documentation according to its nature. Once the conservation period elapses, the documentation's owner must authorise its destruction or, as relevant, its extension. Each

group and sub-group has been assigned a default conservation period in the SAP archive program. This datum is filled in in the “DESTRUCTION YEAR” field.

The documentation date on the box is entered in the "TO" field in the archive program but the “DESTRUCTION YEAR” field is filled in with the calculated year according to the date of the final acceptance of the project, contract or service or the termination date of the contract, regardless of whether the documentation in this sub-group has a prior date.

Documents to be conserved indefinitely: documents which cannot be destroyed according to regulations. These documents are detailed in point 5.6.

Group and sub-group: codes that identify the nature of the documentation in the boxes. These codes are entered in the SAP program when entering the lots and are fixed by the relevant areas and divisions. Their purpose is to facilitate the later searching for this documentation. Each group and sub-group has a conservation period assigned by default in the SAP archive program.

Documentation type or classification level: classification of the archived documentation:

- *Unrestricted* documentation: contains information that may be known by all FCC personnel; its querying must be authorised by the owner.

- *Restricted* documentation: contains information that may not be known by all FCC personnel (secret or confidential). It will be identified by a mark that clearly shows this classification level; its querying must be authorised by the owner.

Lot: number identifying the box containing documentation to be archived according to the SAP archive management system. Lots may never be duplicated, that is, two boxes with the same lot number, box being understood as any standardised medium - FCC box, box with lid or trunk.

Label: form that identifies the information in the lot.

Manual - SAP archive management: Manual available to the personnel that explains the functioning of document management for those issuing centres with SAP (Integra production access). Location:
https://fccone.fcc.es/documents/217476/718645/FCC_ARCHIVO_Manual_User.pdf/300d096e-8f6a-4ce8-b430-b516e717db1a

WEB-DYNPRO portal: this portal is accessed at http://portalintegra.fcc.es/irj/portal

Portal archive management manual (web-dynpro): Manual available to the personnel that explains the functioning of document management for those issuing centres without SAP. Location:
https://fccone.fcc.es/documents/217476/718645/FCC_ARVHIVO_Manual_User_Aplicaciones_Web_v1.00.pdf/de462c5d-9353-48da-acbf-7cb9058dc836

Access control list: list of organisations or persons authorised to access an installation or documentation. External organisations must sign an information confidentiality contract with FCC (maintenance, messenger, transport, etc, companies).

Access register: list of persons who have accessed the archive installations, giving their name and entry and exit date and time.

5 Operation

5.1 Generation of documentation

During the duration of contracts for projects, contracts or services, it is essential to carry out a suitable process of classifying documentation in the active work centres, following the guidelines set by the corporate departments and areas (see the group and sub-group annex) to facilitate to a great measure the preparation of the documents for future definitive sending to the Central Archive, avoiding the common problems of lack of persons who know the documentation and the classification processes at the end of the project with the consequent disorder, delay or impossibility of classifying suitably for any future queries.

5.2 Communication of the need to send documentation

Once the need to send documentation to the Central Archive is identified, which may be determined by compliance with the regulations, centralising of documentation or the need to free up space in the centre, it is **obligatory** to contact the *document manager* to receive the appropriate instructions and determine the validity of the documentation to be sent, thus avoiding errors that are difficult to correct once the documentation has been sent.

The persons to contact our:

Madrid Archive: Esther Fernández Pérez (tel: 913 437 265) archivo.madrid@fcc.es

Barcelona Archive: Rodolfo Mitjans Marsa (tel: 934 784 674) archivo.barcelona@fcc.es

5.3 Preparation of documentation

5.3.1 Classification of documentation

The *owner* is responsible for ensuring that the documentation is classified according to FCC regulations and that it is sent to the Central Archive. All the lots must identify the *classification level* assigned to the information they contain by adding a *label* clearly and visibly. There are two types of documentation in the classification level:

- *Unrestricted* documentation: accounting and project, contract or service documentation not considered restricted. The information it contains has a normal confidential level. When creating the lot, mark the "Authorisation Code" box as "Unrestricted" ("N").

- *Restricted* documentation: Presidency documentation, medical check-ups, clinical histories, CVs, personnel accidents, insurance, accident investigation reports, salaries, TC1, TC2, medical tests, employees' contracts, access/psycho-technical tests and any type of document that may contain data on health, ideology, racial origin, gender violence, harassment at work and/or trade union membership. The information they contain has a high confidentiality level. When creating the lot, mark the "Authorisation Code" box as "Restricted" ("R").

The documentation must be classified and labelled according to the classification model in the FCC regulations. Any lot not classified will be considered unrestricted by default. The restricted documentation must be differentiated from the unrestricted by filing it in different boxes even if the volume of documentation does not fill the box. Any lot containing information with different classification levels will be treated with the security measures for the most restrictive classification level as long as it is not possible to apply the specific measures to each level.

5.3.2 Archive material: FCC box and label

All the documentation must be placed in standardised material. It is obligatory to use the materials specified below which is available in the office material catalogue. The sizes of the boxes to be used must match the size of the documentation they contain to avoid using boxes that are half full or too full.

- FCC box/definitive filing box (obligatory)
  Reference: 4772889
  Measurements: 11.2 cm wide, 38.5 cm long and 27.0 cm high.
  Catalogue description: packet of 10 units, definitive filing box Fol. Ppl FCC

- Small FCC box
  Reference:
  Measurements:
  Catalogue description:

- Label (obligatory)
  Reference: 4847855
  Catalogue description: packet of 30 units, Label Mult 105-x148 A5 Apli 7107

- Packing box (recommended model):

Reference: 6680316
Measurements: 500 x 400 x 300 (single channel)
Catalogue description: packet of 20 packing boxes (each holds four FCC boxes)

- Box with lid: (not in catalogue)
  If the documentation to be inserted does not match the format of the box described above, contact the document manager before sending.

- Trunk: (not in catalogue)
  This format is allowed for specific cases of technical documentation (projects, contracts) with the prior authorisation of the document manager.

Boxes that do not meet the above specifications will not be accepted for entry into the Central Archive.

5.3.3 Computerising of the documentation and printing of labels

Basic notes

- One lot number per box

The box must have an identification number called lot in the system that is assigned automatically by the archive program. It is obligatory to computerise each box with a different lot number; this cannot be duplicated and more than one box with the same lot number must not be sent to the Central Archive.

- Groups and sub-groups

Documentation is classified by groups and sub-groups (see Annex). During the currency of project contracts, contracts or services, it is essential to classify documentation suitably in the active work centres following the guidelines set by the corporate departments and areas into the defined groups and sub-groups. The data of each lot must be informed according to the “Archive Management Manual.”

- Documentation dates and destruction year

The dates of the documentation in the box must be entered in the program fields called “PERIOD FROM” and "PERIOD TO."

The relevant here must be calculated and ended in the “DESTRUCTION YEAR” field according to the data the final acceptance of the project, contract or service or the termination date of the contract, regardless of where the documentation in this

sub-group has an earlier date, the data provided by the program must be changed manually.

The destruction year date is given by the system automatically but can be modified when the user considers it necessary, depending on the contents of the group, sub-group and period to boxes.

The following details two possible accesses using the SAP system in the archive management program and its manuals which explain the entire computerising process. However, a help manual is attached to this procedure for persons who are already familiar with the program's functioning.

5.3.3.1 Users with production SAP-Integra

Available in these archive management programme. The "*SAP Archive Management Manual*" is available for any query. Access is through the FCC Archive users folder.

5.3.3.2 Users WITHOUT SAP

These must request access to the *WEB-DYNPRO portal* through the *document manager* who will provide an access template (X) which must be filled in and sent to Servidesk, which will provide passwords for access to the portal. For any query, see the "*Portal archive management manual (web-dynpro).*"

SAP access portal (dynpro Web site): http://portalintegra.fcc.es/irj/portal

After correct classification, insert the documentation in an FCC format box. **Two labels must be placed on each box.**

5.3.4 Sending the documentation

The sending must be made in the most orderly form possible with classification by date, numerical, groups, sub-groups, etc., depending on the documentation type.

The FCC boxes must be placed in a larger box (packing box) which may not contain more than five FCC boxes to ensure sending, by lot number order from lowest to highest and this new packing box must be clearly identified on the outside top with a reference – box 1/10, 2/10, etc – and the name of the department, project or contract.

Once the documentation has been prepared, the *owner* must fill in the required information in the "Documentation entry request" form (Annex) and send it to the e-mail address given by the *document manager*. The requests must be sent sufficiently beforehand so that the document manager can organise the physical reception of the documentation.

Remember that it is essential and the owner's responsibility to specifically identify whether the documentation to be sent to the Central Archive includes restricted information (see point 5.3.1).

As stated above, restricted documentation must be differentiated from unrestricted documentation, filing it in different boxes even if the volume of the documentation does not completely fill the box.

5.3.5 Analysis of the request by the document manager

The *document manager* will check the request received and ensure that all the data given are correct. After the analysis, he will send the reply to the *owner*, giving the sending date as well as the reception centre to which the documentation must be sent. Currently, the archive centres are in Madrid and Barcelona.

5.3.6 Contracting of transport and sending of documentation

The *issuing centre or owner* is responsible for sending the documentation securely and for paying the transport costs. The transport company must be given beforehand so that the *document manager* can check that the supplier has signed the *confidentiality clause*. If it has not, it will be sent to the supplier for signing before undertaking the sending.

5.3.7 Receipt of the documentation in the Central Archive

The packing and FCC filing boxes must be received in good condition, properly identified and clean, as described in the entry request, otherwise the solution for the incidents (dirty boxes, broken, without labels, etc.) will be set with the *coordinator*. Once the proper entry of the documentation has been handled (entry file) the *document manager* will inform the user and/or *owner* of the entry of the documentation in the system, the file number, all relevant data and any incidents that occurred.

5.4 Documentation query

Once it is in safekeeping, the *authorised person* can request one or more boxes or documents with response times ranging from a normal delivery on the following day to an urgent delivery within hours, whether it is the original document or a digitised copy sent by e-mail.

Any query on the documentation deposited in the Central Archive must be requested through SAP except for users that do not have SAP in which case they can be made by e-mail, sending the "Documentation consultation form" (Annex).

Access to the documentation must in all cases have the prior authorisation of its *owner*. To provide this authorisation, the documentation *owner* must fill in the "Documentation consultation. Authorised persons" form (Annex) and send it to the *document manager* who is responsible for safekeeping these authorisations and keeping them up to date. The authorisations must specify the type of query for which the user is authorised and which company, department, project, division or contract and type of information.

There are two types of queries.

Type 0 query. The user is not authorised to query the indicated documentation.

UNRESTRICTED information

Type 1 query. Queries on boxes, documents, photocopies and scanned documents within the Central Archive premises.

Type 2 query. As well as type 1 queries, also includes the sending of scanned documents and the temporary exit of boxes and original documents for later return to the Central Archive.

Type 3 query. As well as types 1 and 2 queries, also includes the definitive exit of boxes and original documents without later return to the Central Archive.

RESTRICTED information

Type 4 query. Queries of boxes, documents, photocopies and scanned documents within the Central Archive premises.

Type 5 query. As well as type 4 queries, also includes the sending of scanned documents and the temporary exit of boxes and original documents for later return to the Central Archive.

Type 6 query. As well as type 4 and 5 queries, also includes the definitive exit of boxes and original documents without later returned to the Central Archive.

Documents from the Central Archive are distributed to applicants through means that ensure:

-The unequivocal receipt by the authorised person.

- The confidentiality and integrity of the information.

Restricted information sent from the Archive by e-mail is encrypted. The addressee will receive separate files, one with the documentation and another with the key that allows the file to be opened to ensure confidentiality and the unequivocal receipt by the authorised person (see point 5.7).

In the case of the physical sending of documentation, the receiver must return the documentation in the same condition in which it was received, ensuring its security, confidentiality and integrity. Documentation or a box must not be returned without being duly wrapped or protected.

5.5 Documentation destruction

On dates approaching the expiry of the documentation, the *document manager* will send the *owner* or *issuing centre* a list of that which has exceeded the conservation period for it to decide on the suitability or otherwise of its destruction. Document destruction must have the approval of the *owner or the Director of the issuing centre* before its destruction.

Exceptionally, accounting information must also have the approval of the central administration services in the area to which it belongs. If the issuing centre allows the destruction and the central administration services states that it cannot be destroyed, the owner must be changed in the program, entering the latter as the new owner.

For better use of the space in the Central Archive and because of the volume of documents generated by the FCC Group, it is essential that the reply to the above point reaches the Central Archive within 20 days.

The documents are destroyed using means that ensure that the information is unrecognisable and unrecoverable, maintaining the confidentiality of the information in them throughout these actions.

If document destruction is outsourced, the agreements signed with the suppliers must include a confidentiality commitment that extends to all the persons working for the external supplier who are directly or indirectly involved in the service, regardless of the additional requirements of current legislation according to the nature of the information contained.

When information destruction is outsourced, the agreement between both companies must require the company providing the service to give a certificate guaranteeing the destruction of the documents, accrediting the complete elimination of the information contained in them.

Transport to the place in which the documents are to be destroyed must be made such that during the transfer there is no removal, loss or filtrations of the information.

When electronic documents containing personal data are involved, distribution must be made by enciphering the data or using any other mechanism that guarantees that the information is unintelligible and not altered during its transport.

In no case may the elimination be authorised nor documents be destroyed while there is probative value of rights and obligations of individuals or organisations or the periods set by regulations or current legislation for its conservation have not elapsed.

If it is necessary to extend the documentation safekeeping period, the owner must send a signed request to the document manager giving the reason. This request will be revised by the Security Department for the information when considered necessary.

5.6 Documents to be conserved indefinitely

As far as possible, this documentation type must be kept in different folders from the rest of the documentation that can be destroyed to prevent its accidental destruction.

The documentation that must be conserved indefinitely includes:

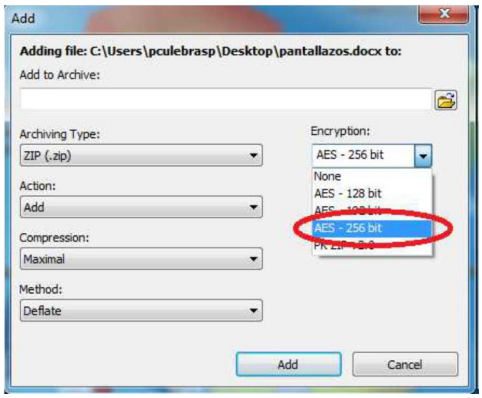
- Real estate title deeds.
- Final certification of each project detailing the origin of the various units and suitably signed by the project management and owner.
- Those for each December in all the services provision contracts.
- The final invoices for the sale of supplies or any other item for an amount greater than €6,000. This therefore excludes those issued for deliveries on account or the partial delivery of the contracted supply.
- Documentation that the owner identifies as such in the group and sub-group table (giving 99 years).

5.7 Procedure for sending sensitive information

In accordance with the data protection regulations, when restricted data are to be sent over public or wireless electronic communications networks, the data must be enciphered or any other mechanism used that guarantees that the information is unintelligible and not altered by third parties.

All users who must send information of this type by e-mail must do so in the following way:

- Encipher the document beforehand using the IZARC compression system (or the corporate compression system approved in the organisation at the time).
    - Right click on the file to be sent.
    - IZArc
    - Add to Archive File
- Mark that the password has the AES 256 algorithm (in the encryption section).



In all cases, the password must have sufficient consistency to prevent its vulnerability. For this, robust passwords must be used with eight digits including uppercase and letters. The password must be sent to the recipient in another, different, e-mail to that used to send the documentation.

When the recipient wishes to decompress the file sent, the program will ask for the password.

6 Documentation storage installations

The premises and installations for storing documentation must be equipped with security measures that allow access only to authorised persons. Their identification and location must be controlled.

Dangerous and/or combustible materials must not be stored in the security area in the documentation facility.

6.1 Secure access areas

6.1.1 Protected access areas

The Central Archives are in these areas. Access to these areas is limited and controlled through identification mechanisms or the impossibility of access to minimise environmental risks and unauthorised accesses.

A permitted access list must be available for access to these areas.

The access records must contain the identification and date and time of entry and exit.

The entry of anyone outside normal working hours must be authorised and registered.

Visitors entering these areas must be accompanied by a person on the permitted access list.

Cleaning, disinfection, etc., work must be supervised by a person responsible for the room who can warn of and avoid accidents or intentional acts on the documentation.

6.1.2 Restricted access areas

These areas contain the departmental archives of the areas where information is stored, distributed geographically by different areas and for which the companies owning the information are responsible.

A permitted access list must be available for access to these areas.

When the type of information stored so determines (e.g., restricted documentation), the access records must contain the identification and date and time of entry and exit.

The entry of anyone outside normal working hours must be authorised and registered.

Visitors entering these areas must be accompanied by a person on the permitted access list.

Cleaning work must be supervised by a person responsible for the room who can warn of and avoid accidents or intentional acts on the documentation.

6.1.3 Controlled access areas

These areas contain the FCC offices where documentation necessary for undertaking the activity is stored. These areas are open to FCC personnel with no specific environmental safeguards to protect the information systems.

In this case, the documentation must be kept locked away, either in cupboards with a lock or in offices or rooms with locked doors.

A list must be kept of the person(s) who have a copy of or access to the key.

7 Annexes

- Group and sub-group
- Documentation entry request
- Web-Dynpro portal access template
- Documentation consultation by e-mail form
- Persons authorised to query documentation
- Central Archive help manual