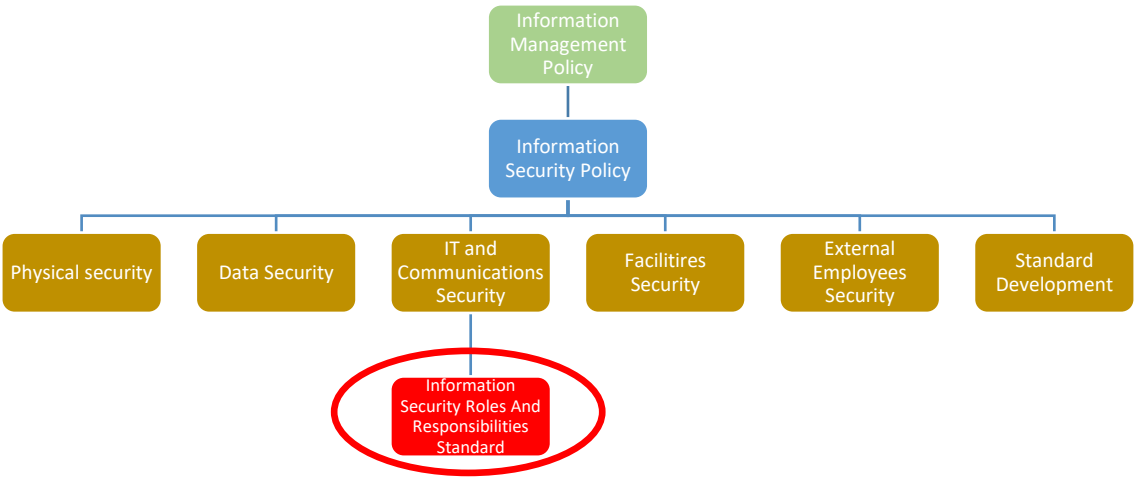
INFORMATION SECURITY STANDARDS

INFORMATION SECURITY ROLES AND RESPONSIBILITIES STANDARD

ID Code:	**NRM-17-EN**
Version:	**1.1 October2019**
Classification:	**FCC_INTERNAL_USE**
Intended for:	**Information Systems and Technology Department**

INDEX

INTRODUCTION



This standard develops roles and responsibilities for staff and FCC representatives. It includes the Policy for Organization and Information Security for FCC aimed to achieve an effective and efficient management of Information Security, as an essential objective for FCC activities in this area.

In addition to these roles and responsibilities for staff and FCC representatives on Information Security, it will be developed supplementary ones regarding outsourcing companies providing professional services to FCC Group.

PURPOSE

The purpose of this Standard is to define the responsibilities and roles played within the Group by FCC staff during the course of their duties.

SCOPE

This Standard applies to all resources and FCC staff accessing FCC information regardless of the functions performed.

The remaining set of FCC policies regarding Information Security develops staff responsibilities stated in this Standard.

ORGANIZATION

The organization of the Information Security Group of the FCC is based on:

The Responsibility rests with:

- CEO and Executive Committee.
- Owner of the Information.
- Head of Department of Information Security and IT Risk Management.
- Systems and Information Technology Department.
- Internal Audit Manager.
- Information systems Users.

Roles:

- Information Security Committee.
- Executive Committee.
- Certification Committee.
- Advisory Committee.

RESPONSIBILITIES

CEO and Executive Committee.

The CEO and Executive Committee of the FCC Group support and provide visibility to the Group's commitment for the development, implementation and improvement of security policy information.

These responsibilities are:

• To approve:

- Organization model and Safety Management.
- Information Security Policies.
- Residual Risk.
- Classification and Information of Asset Management Model.
- Business Continuity Plan.

• Allocate resources to develop:

- Information Security Policies.
- Classification and Information of Asset Management.
- Training and awareness programs about Information Security.

Information Owners.

Information Owners will:

• **Assign the classification level** for Information Assets owned by FCC for which they are responsible.

• **Reclassify information assets** for which they are responsible when necessary.

• **Manage access authorization** to FCC staff with need-to-know needs for information they were responsible for.

• Provide awareness about the **correct use of information assets**.

• Inform to Head of Information Security, about any violation of the internal Standards regarding Information Security.

• Participate in monitoring and resolving any security incidents affecting the information processed.

Department of Information Security and IT Risk Management.

This Department will carry the following responsibilities:

• **Support** FCC staff on **Information Security Issues**.

• **Analyze any Risk** resulting from Information Access, in conjunction to information owners.

• **Verify the implementation of security measures** required to protect FCC information.

• Define and manage the Security Management and Organizational Model.

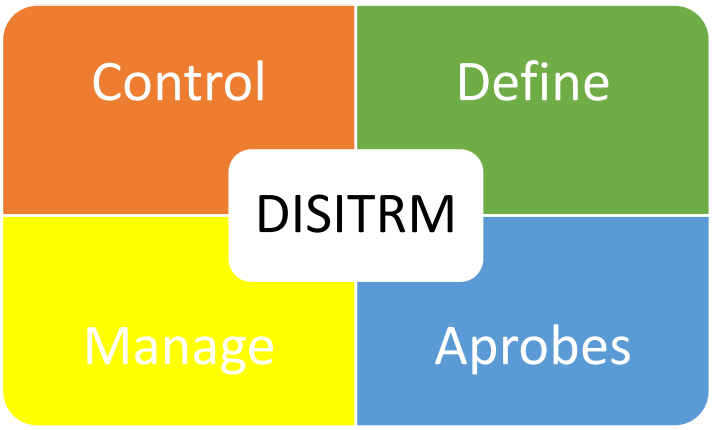
• Define and manage FCC Classification and Information of Asset Management Model.

• Develop policies regarding Information Security.

Head of Information Security will also be responsible for definition, approval, management and control of the following activities:

- Systems connection
- Information Security Technology
- Information security Monitoring
- Infrastructure Security
- Information security awareness and training
- Outsourced 3rd-party services Security
- Business Continuity Plan

- Systems connection
- Information Security Technology
- Information security Monitoring
- Incident Management
- Infrastructure Security
- Information security awareness and training
- Outsourced 3rd-party services Security
- Business Continuity Plan



- Information Security Monitoring
- Incident Management
- Information Security awareness and training.
- Business Continuity Plan

- Information Security Monitoring
- Infrastructure Security

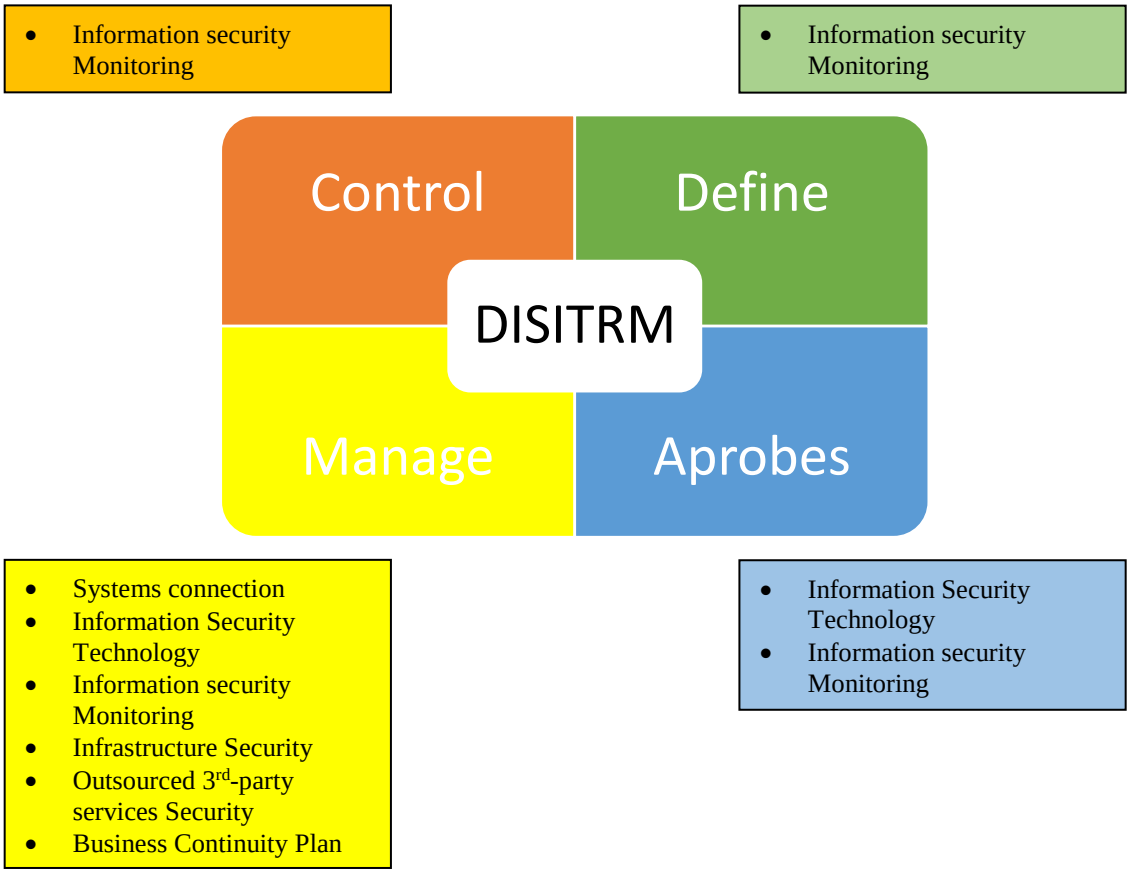
Department of Systems and Information Technology.

This Department will carry the following responsibilities:

• Manage all Information Security Policies.

• Develop and manage Procedures, Technical Instructions and Guidelines on Information Security.

Head of Information Security Department will also be responsible of definition, approval, management and control in the following activities:



Department of Internal Audit.

The Department of Internal Audit will carry the following responsibilities:

• Conduct independent audits about update and observance of the FCC policy regarding Information Security.

Users of information Systems.

Users of Information Systems will carry these responsibilities:

• Follow all the statements included in the FCC Policy concerning Information Security and understand the consequences of non-observance.

• Manage FCC Information for the execution of their duties exclusively.

• Notify without delay any security incidents or misuse of information assets as soon as aware.

ROLES

Information Security Committees

FCC adopted a structure of Safety Committees for the definition, creation, development and control of activities related to Information Security.

Information security is a specific need for a good business development and all FCC areas should contribute to. Safety Committees have, as a main goal, to coordinate any steps adopted regarding Information Security.

Additional Committees may be stablished at the request of the Executive Committee or Head of the Information Security Department.

Executive Committee

The Executive Committee is the highest body to rule over Information Security coordination.

This Committee will have the following functions:

• Approve Training and Awareness programs for Information Security.

• Approve the Business Continuity Plan.

Certification Committee

This Committee will have the following function:

• To approve the interconnection of information systems.

Advisory Committee

This committee will serve to share the ideas and interests of each of its members on decisions that can be taken on Information Security.

Advisory Committee will have the following function:

• Advise the Department of Information Security.

CHANGES TO ROLES AND RESPONSIBILITIES

Committee of Information Security Management will be in charge of approving changes in roles and responsibilities. This Committee will submit its decision to FCC General Manager for signature and dissemination within the Group.

REVIEW OF THIS STANDARD

The Security Responsibilities and Roles standard should be reviewed periodically. This Standard may also 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 Standard
- Whenever there are major technology changes.
- Whenever there are changes in Organization and Security Management Model.
- Whenever there are changes in the roles and responsibilities assumed by FCC committees or departments.
- Suggestions for improvement made by audits.

The information used for the review of this Standard must be notified to the Information Security Department by the departments or services affected by it, who must then notify the Information Security Department Committee of this information.

EXCEPTIONS TO THIS STANDARD

Any exception to this Standard should be justified in writing and authorized by DSITRM.

The only way to communicate the exceptions will be the official mailbox INFOSECURITY@fcc.es and/or any other channel managed by "Service Desk FCC" to receive request.

The person responsible for the exception will be a hierarchical superior (beginning in Head of Department or C-level).

The protocol to communicate this exception will use this form:

EXCEPTIONS TO THIS STANDARD	
Applicant	
Responsible	
Policy/Code of use/Standard	

Non-compliant Section	
Description of the Exception and justification	

VIOLATIONS

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

ANNEX I. ROLES AND RESPONSIBILITIES ASSIGNATION GRID REGARDING INFORMATION SECURITY

For a detailed description of these roles and responsibilities, please visit the Responsibilities and Roles Sections.

Activities \ Groups	CEO and Executive Comitee	Information Security and IT Risk Management	Department of Systems and Information Technology	Department of Internal Audit	Certification Committee	Managing Comitee of Information Security and IT Risk Management
Security Organization and management	Aprobes	Defines, Manages		Controls		
Information Security Policies	Aprobes, Manages	Defines	Manages	Controls		
Information assets classification and management	Aprobes, Manages	Defines		Controls		
Systems connection		Defines, Controls	Manages	Controls	Aprobes	
Information Security connection		Defines, Controls	Aprobes, Manages	Controls		
Information Security monitorizing		Defines, Aprobes, Manages, Controls	Defines, Aprobes, Manages, Controls	Controls		
Incident management		Defines, Aprobes		Controls		
Infrastructure Security		Defines, Aprobes, Controls	Manages	Controls		
Information Security awareness and training	Aprobes	Defines, Manages, Controls		Controls		Aprobes
Outsourced 3rd-party services Security	Aprobes	Defines, Controls	Manages	Controls		
Business Continuity Plan	Aprobes	Defines, Controls, Manages	Manages	Controls		Aprobes

Defines
Aprobes
Manages
Controls

REFERENCES

- **Related Standards**
  - Information Management Policy
  - Information Security Policy.
- **References to the ISO/IEC 27002:2007 Standard**

6. Corporate Security Management

6.1 Establish an internal information security organization

6.1.1 Allocate information security roles and responsibilities
6.1.2 Segregate conflicting duties and responsibilities
6.1.3 Maintain contact with all relevant authorities
6.1.4 Establish relationships with external organizations
6.1.5 Make information security part of project management

DOCUMENT CHANGE CONTROL

Document Information

FILE NAME:				
VERSION	DATE	CHANGE	AUTHOR	REVIEWED BY
1.0	April 2009	Document creation	Department of Information Security and IT Risk Management	FCC Executive Committee
1.1	September 2014	General Review	DISITRM	
1.1	October 2019	General Review	DISITRM	

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
V1.1	September 30th 2014	DISITRM	Update and General Review

CLASSIFICATION: FCC_INTERNAL_USE

END OF DOCUMENT