~~NRM-01~~ GLOSSARY OF DEFINITIONS SECURITY POLICY

ID Code:	**NRM-01-EN**
Version and Date:	**v1.1 July2014**
Classification:	**FCC_INTERNAL_USE**
Intended for:	**All FCC Group Staff**

INDEX

INDEX 2

GLOSSARY 3

RESPONSIBILITIES 8

REVIEW OF THIS STANDARD 8

EXCEPTIONS TO THIS STANDARD ..... ¡Error! Marcador no definido.~~9~~

VIOLATIONS ..... ¡Error! Marcador no definido.~~9~~

REFERENCES ..... 8~~9~~

DOCUMENT CHANGE CONTROL ..... 9~~10~~

GLOSSARY

Term	Definition
Environment:	The development, operation and maintenance of an IT system.
FCC Facility:	Any service that participates in the processing of FCC data.
Tag:	A label or badge that allows identification of a document's data and classification.
Evidence:	Data that is either used on its own, or in combination with other data, to prove something.
Outsourcing:	The contracting of services to third parties to carry out activities on behalf of the FCC Group.
Electronic Signature:	A set of electronic data that is assigned to users and used as a means of personal identification, together with other associated data.
Data Management:	Creating, submitting, storing, processing, moving or destroying data.
Risk Management:	The identification, selection and implementation of controls based on the risks identified, and reducing those risks to an agreed level, as defined by General Management.
Classification Guide:	A document containing data pertaining to the information stored in documents, which serves a reference for classifying documents.

Security Staff Authorisation: Certification stating that the holder can be trusted to manage classified information to an agreed level, and is qualified in data security.

Authorisation:

The authorisation expressly granted to FCC staff members to access specific data asset sets, which are predefined based on the user's "functional role".

Security Incident:

An event that is not part of the standard operating procedures for a service, which compromises the security of the IT systems.

Data:

Any data that can be communicated, submitted or stored in any format.

FCC Data:

Any data that is formally generated by staff from companies of the Group - or any third parties explicitly contracted to carry out works for the same; and any data that is specifically submitted to FCC companies for processing.

Non-Restricted FCC Data: Any non-restricted FCC data that has been classified for "Internal Use" or "Public Use".

Restricted FCC Data:

Any restricted FCC data which is classified as "Private" or "Confidential".

Installations:

Any data processing system, service or infrastructure, as well as the physical location that hosts them.

Integrity:

The basic security requirements to ensure that data cannot or has not been modified or altered by unauthorized persons, companies or processes.

Access Control List (ACL):	The list of companies authorised to access a resource, as well as their access rights to that resource.
Malware:	Any program, document or message that is likely to damage and/or harm information or users.
Maintenance:	A schedule of regular works that must be carried out to ensure the smooth running of IT equipment.
Functional Role:	The role that determines the specific data sets a user can access in order to carry out their services, tasks or duties.
Node:	Any device connected to a communications network.
Security Structure:	The organisational structure created by the FCC Group to ensure that all necessary agents are kept informed of any decisions or actions taken in matters of IT security.
FCC Staff:	Refers to any person directly or indirectly involved in achieving the business goals of the FCC Group, regardless of the type of working relationship they have with any of the companies comprising the Group, or any third parties that may be servicing the same.
Audit Trail:	The historical data and information that is available for inspection, in order to verify that the established security procedures have been fully and correctly followed.
Spyware:	Malicious code that is designed to gather data from infected systems and send it for commercial or fraudulent uses via the internet.
Data Ownership:	

	Data owners are ultimately responsible for ensuring it is properly protected.
Classification Change Requests:	A change request document used when individual or group access to data requires modification, as well as the duration these changes are required for, which must be submitted to the authorised classification department for approval, in accordance with the reclassification procedures that govern temporary variations to assigned access.
Internet Service Provider (ISP):	A third party that provides internet access and related services to organisations.
Proxy:	A communications server with a firewall physically installed, that is used to channel traffic between a private network and the Internet.
Proof:	Grounds, arguments, instruments or other means used to show and demonstrate whether something is true or false.
Reclassification:	The assignation of new access classification levels for classified information.
Network:	A communications system used for sharing resources that consists of a transmission and switching device set.
Procurement Unit:	The FCC functional unit responsible for deciding which external companies can be contracted to supply goods and/or services - as well as any other services these entail, where appropriate.
Data Unit:	The FCC functional unit responsible for ensuring that all data processed is duly classified and protected in accordance with the criteria established by FCC.

Data Risk:

The likelihood or potential of a threat exploiting a system vulnerability, which could compromise the confidentiality and integrity of data, and/or the availability of the system.

Residual Risk:

Any data security asset risk that remains after FCC has taken management action, or implemented the controls necessary to reduce the asset's risk exposure.

Intrusion Detection System (IDS):

An active system, process or device that scans the system and network for security violations such as unauthorized access attempts and/or malicious activities.

Data Security Information System:

A series of formal reports which allow Data Security to be managed at various organisational levels of FCC.

IT and Telecommunications System:

A set of equipment, methods, procedures and staff, organised in such a way that allows data management.

Data processing:

Creating, submitting, storing, processing, moving or destroying data.

User:

An staff member authorised by the Data Unit to access data assets, in accordance with the safeguards laid down by this Unit.

Virtual Private Network (VPN):

Technology commonly used for deploying secure private networks over non-secure public networks.

Vulnerability:

Any weakness, attribute or loss of control that would allow or facilitate the materialization of a threat.

Demilitarized Zone (DMZ):	A term commonly used to designate an area where the network perimeter security measures are less stringent. Internet-accessible devices are normally placed in this area, which cuts out the need for external access to private networks.

RESPONSIBILITIES

The Data Security and Risk Management Department must:

- Update this glossary as needed.

REVIEW OF THIS STANDARD

This Standard may be reviewed in the following circumstances:

- Whenever there are changes to the responsibilities undertaken by Committees and/or Security Authorities and/or FCC departments.
- Whenever improvements are suggested as a result of audits carried out.
- Whenever there are changes to the current legislation regarding the provisions established in this Standard.

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

REFERENCES

- **Related Regulations**

- FCC Data Security Policy.
- FCC Personal Data Policy.
- FCC Code of Use of Technological Media.
- NRM-02 Database Security Standard
- NRM-03 Encryption Security Standard
- NRM-04 Access Control Standard
- NRM-05 Configuration Control Standard
- NRM-06 Portable Devices' Standard
- NRM-07 Backup Management Standard
- NRM-08 Incident Management Standard
- NRM-09 Systems Laboratories' Standard
- NRM-10 Network Security Standard
- NRM-11 Password Security Standard
- NRM-12 Password Security Standard
- NRM-13 Development Security Standard
- NRM-14 External Company Standard
- NRM-15 Document Security Standard
- NRM-16 Physical Security Standard
- NRM-17 Security Responsibilities Roles Standard
- NRM-18 Return and Disposal of Technological Media Standard

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
1.1	2014 July	General Revision	Information Security and IT Risks Department	
1.1~~0~~	August 2019	Revision of the document	Information Security and IT Risks Department	FCC Executive Committee

CLASIFICATION: FCC_INTERNAL_USE

Please Note: Hard-copies are not controlled

END OF DOCUMENT