Glossary of Definitions for the FCC Group Information Security Regulatory Framework

January 2026

Document Version Control				
Version	**Date**	**Author**	**Detail**	**Approved by**
1.0	April 2009	IS	Document creation	FCC Executive Committee
1.1	July 2014	IS	General Revision	Chief Information Security Officer (CISO)
	August 2019	IS	Document Revision	FCC Executive Committee
2.0	January 2026	IS	Document Revision	Chief Information Security Officer (CISO)

INDEX

1. Glossary

TERM	DEFINITION
Access Control List (ACL)	List of entities, together with their access rights, that are authorized to access a resource.
Audit Trail	Historical data and information that are available for examination in order to demonstrate the correctness and integrity with which the established security procedures have been followed.
Authorization	Permission expressly granted to an FCC staff member so that they may access certain information assets to which they would not otherwise have access based on their "need to know" in the performance of their duties
Classification Proposal	Document submitted to the authority empowered to classify, proposing the assignment of a classification level to individual pieces of information or sets of information, as well as its validity period, in accordance with the reclassification procedure that governs temporal changes to the assigned level
Contracting Manager	FCC functional unit that decides which external company will be contracted for the supply of goods or the provision of services and, where applicable, any associated services
Demilitarized Zone (DMZ)	Term commonly used to designate a network area where perimeter security measures are less strict. Devices accessible from the Internet are typically placed in this zone to avoid the need for external access to the private network
Electronic Signature	A set of data in electronic form, entered together with or associated with other data, which can be used as a means of personal identification
Environment	Context of the development, operation, and maintenance of an information system
Evidence	Information that, by itself or combined with other information, is used to prove something
Facilities	Any information processing system, service, or infrastructure, as well as the physical location that houses them
FCC Equipment	Any service that participates in the processing of FCC Group information
FCC Information	Information officially generated by internal personnel or collaborators, as well as any information specifically deposited in FCC companies for its processing
FCC Nonrestricted Information	Information that includes FCC Information classified as Public Use

FCC Personnel	Refers to all individuals who, regardless of the type of professional relationship they maintain with the companies that make up the FCC Group or with external companies providing services to them, participate directly or indirectly in achieving FCC's business objectives
FCC Restricted Information	Information that includes FCC Information classified as Secret, Confidential or Internal Use
Information	Name given to an organized set of data that constitutes a message that changes the state of knowledge of the subject or system receiving that message
Information Classification Guide	Document that gathers the relevant data about the information and serves as a reference for the marking of documents
Information Management	The coordinated activities and governance framework used to direct, control, and oversee information throughout its lifecycle, including policies, responsibilities, processes, controls, and continual improvement.
Information Manager	FCC functional unit responsible for ensuring that the information it handles, and for which it is accountable, is properly classified and protected based on FCC's established criteria
Information Owner	The person responsible for ensuring that their information is adequately protected
Information Processing	The set of operational activities performed on information, including creating, collecting, organizing, storing, transforming, transmitting, distributing, modifying or deleting it.
Information Risk	Probability or potential that a vulnerability may be exploited by a threat, compromising confidentiality, integrity, authenticity, traceability, and/or availability
Information Security Incident	Event that is not part of the standard operation of a service and has adverse consequences on the security of information systems
Information Security Information System	Set of reports, regardless of their level of formalization, that enable the management of Information Security at the different organizational levels of FCC
Information and Telecommunications System	Set of equipment, methods, procedures, and personnel organized in such a way as to allow information to be handled
Integrity	Basic security requirement ensuring that information cannot be, or has not been, modified or altered by unauthorized persons, entities, or processes
Internet Service Provider (ISP)	Partner company that provides organizations with Internet access and related services

Intrusion Detection System (IDS)	System, process, or active device that analyzes system and network activity for unauthorized entries and/or malicious activities, with the purpose of detecting security violations
Label	Mark or identifier that enables the identification of information and the classification level of a document
Malware or Malicious Software	Any program, document, or message capable of causing damage and/or harm to information and users
Maintenance	Set of periodic tasks necessary to ensure the proper functioning of computer equipment
Need to Know	Positive determination confirming that a potential recipient requires access to certain information to perform services, tasks, or duties
Network	Communications system composed of a set of transmission and switching devices with the purpose of sharing resources
Node	Any device connected to a communications network
Outsourcing	Contracting a service offered by third parties to carry out activities of the company itself
Personal Security Clearance	Certification establishing that the person holding it can be trusted with classified information at a given level and is trained in information security matters
Proof	Reason, argument, instrument, or other means used to demonstrate and make evident the truth or falsity of something
Proxy	Communications server that channels traffic between a private network and the Internet and contains a physical level firewall
Reclassification	Assignment of a new classification level to previously classified information
Residual Risk	The level of risk remaining for an information security asset after FCC has taken the necessary management actions or applied controls to reduce the asset's exposure to risk
Risk Management	Identifying, analysing, and assessing the risks associated with different processes and/or assets, as well as reducing and containing them within the threshold defined by Senior Management
Security Organization	Structure created within the FCC Group to ensure that decisions and actions regarding information security are carried out and that all necessary stakeholders are kept informed
Spyware	Malicious code designed to collect information from the systems where it resides and send it over the Internet for commercial or fraudulent purposes

User	Personnel authorized by the Information Manager to access information and comply with the safeguards defined by that manager
VPN, Virtual Private Network	Technology commonly used to deploy a secure private scope network over an insecure public scope network
Vulnerability	Weakness, attribute, or loss of control that would allow or facilitate the materialization of a threat