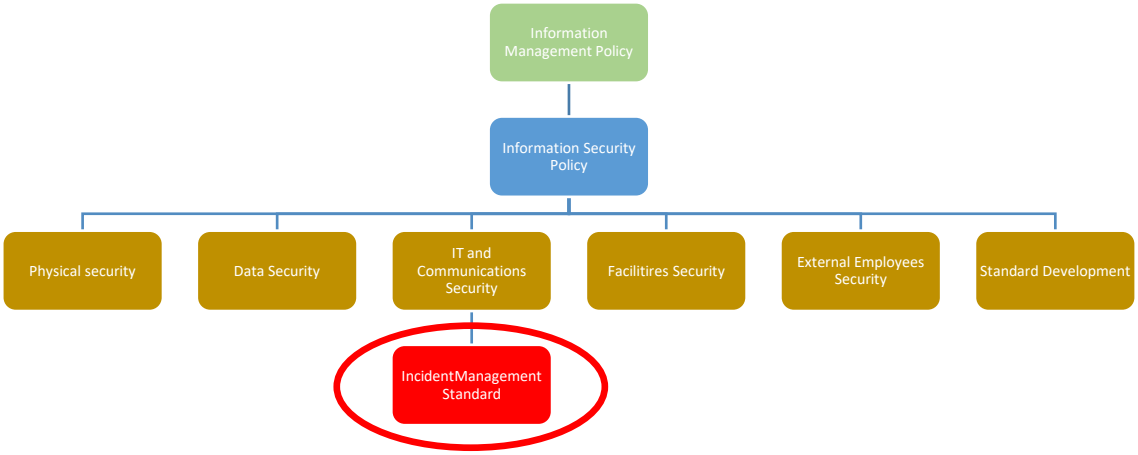
DATA SECURITY STANDARDS

~~NRM-08 II~~INCIDENT MANAGEMENT

ID Code:	**NRM-08-EN**
Version:	**v1.1 ~~July2014~~September2019**
Classification:	**FCC_INTERNAL_USE**
Intended for:	**Information Systems and Technology Department**

INDEX

INTRODUCTION



Data systems are becoming ever-more accessible to communications networks. Not only are cyber attacks on the rise, but the technologies involved and how they are employed are becoming increasingly sophisticated, meaning operating systems and network applications are more exposed than ever to intruders aimed at gaining unauthorised privileges.

The damage that these intruders can inflict on data systems and networks goes beyond just access to an organisation's data, or that of their customers or suppliers - it can also damage their reputation.

Outright prevention of data security incidents - or ensuring their occurrence rate and knock-on effects are kept to a minimum, are key factors for successful data security management.

The purpose of developing Incident Management policies and procedures is to ensure that security incidents are managed correctly. The Response Plans developed for the purposes of Incident Management, set out the performance principles that allow data system attacks to be analysed, detained and removed, which safeguards the confidentiality, integrity and availability of FCC data.

While FCC can analyse threats and plan how to respond to them in order to minimise the number of data security incidents, not all incidents can be prevented. Therefore, a rapid response system is needed for detecting incidents, minimising their impact and recovering the IT services affected.

Incident Management must offer FCC:

- Improved system productivity
- Rapid reinstatement of agreed service levels
- Better process control and service monitoring
- The option to establish an ongoing improvement plan for data security and incident response processes

PURPOSE

This Standard establishes the criteria for responding and resolving security incidents quickly and effectively, in order to minimise or stop any potential or real impacts on FCC Group business units.

SCOPE

This Standard applies to any real or attempted security incidents affecting FCC Group (hereinafter "FCC") systems or installations, regardless of where they are detected in the system, or the resources or data affected.

PRINCIPLES

Incident Management must not be confused with Incidence or Issue Management - which focus on detecting and analysing the underlying causes of a specific hardware or software incidence; for that reason, this document only serves as a reference for restoring security to IT data services.

This Standard defines the activities related to detecting, analysing and resolving data security incidents, whereas the processes of recovering the business activity after such incidents have taken place are defined in FCC's Business Continuity Policy and Contingency Plans.

- The management of a data security incident must include all stages of its life cycle - from initial suspicion or detection, to final resolution - and all corrective actions arising from analysing the causes must be logged and implemented.

- All suspected incidents must be assumed as real, until it can be proven that this is not the case.

- If the impact of an incident cannot be assessed accurately, the worst case scenario must be assumed until a more in-depth analysis can be carried out.

- Whenever multiple incidents occur, the priorities must be established based on how serious or critical they are for the FCC business or user affected.

- Whenever an incident type is not included in the corresponding SLA, the response priority must be analysed objectively based on the impact, or the urgency or acceptable delay in restoring the business process.

- Participation in the various stages that make up the resolution cycle of the Incident Management and Response Plans will depend on the responsibilities assigned in the IT Data Services Datasheets.

- In the event that no service datasheet is defined for a data service, the unit responsible for the service must participate in Managing Incidents.

- To facilitate effective incident management, FCC staff must be familiar with all Incident Management procedures related to each security area they are responsible for.

- The FCC data classification will determine the extent that security measures will be implemented in order to prevent, detect and correct incidents affecting data security.

- In accordance with the Data Protection Act, the Security Document required by each company that forms part of the FCC Group must include the procedures for reporting, managing and responding to incidents that could affect the security of personal data processed and managed by them.

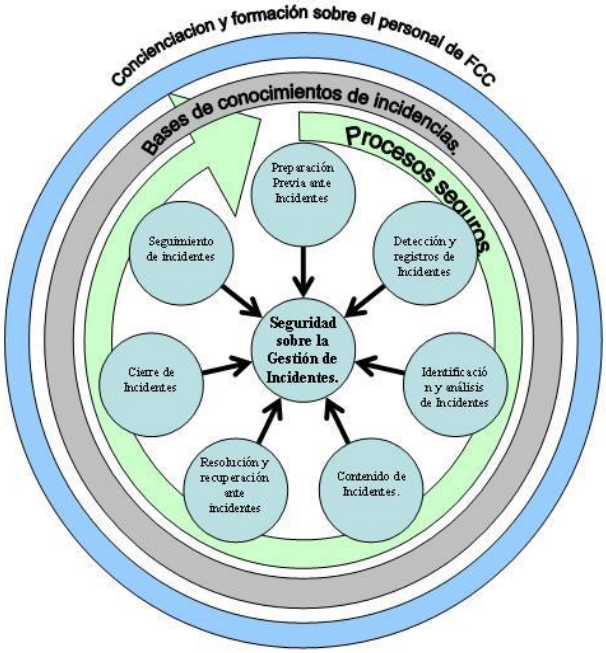
- Any incident involving loss of confidentiality of FCC data managed by external Companies must be reported as soon as possible to the Data Security and Risk management Department, in accordance with the FCC External Companies' Policy.

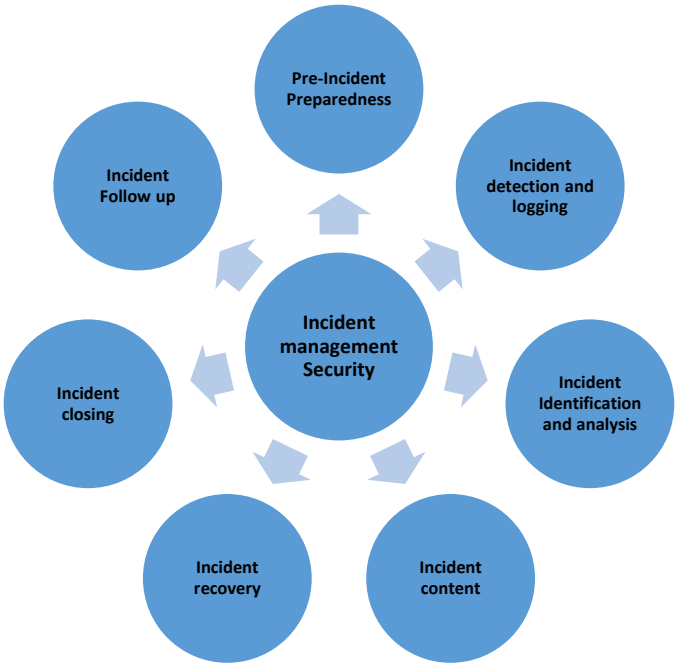
Whenever technically possible, the following must be in place:

- Systems and applications must be configured to detect and report incidents and alerts automatically

- System performance patterns must be established, scanned and monitored to quickly detect any anomalies in the behaviour of Information Systems.

- An encrypted signature log file must be available for system and application files, to quickly verify system integrity.





Pre-Incident Preparedness

FCC's capacity to respond to security incidents largely depends on its capacity to prevent them and how prepared it is to tackle them as an organisation. In addition to establishing security controls for the Group's systems, networks and applications, it also needs to consider aspects such as training, logistics and techniques to facilitate rapid, effective and efficient responses to any security incidents that may arise.

Experience, organisation and knowledge of the IT data services - and the threats they are exposed to, are key to effective Incident Management that minimises the impact on business processes. For that reason, those responsible for data, and the departments involved in managing it, must define:

- A catalogue of potential incident types for each specific system, and the risks involved in each scenario
- An Incident Response Plan for each scenario defined
- The combinations of indicators or precursors that generate the signs required to conclude that an incident may be materialising
- The assignation of functions and tasks for each incident type
- Training on technical aspects, as well as the legal implications and violations of privacy rights that could arise from tasks related to incident resolution
- The allocation of technical resources and staff for incident resolution

Incident Detection and Logging

- Any suspicion, doubt or knowledge of a data security incident must be reported in detail and as soon as possible to the manager stated in the IT Data Service Datasheet, or failing that, the technician responsible for the system that may be compromised by the incident. The manager stated in the Service Datasheet, or the technician in charge, will notify the relevant members of the Incident Management Team, who will fully or partially participate in managing the incident.

- The Incident Management Team will be formed of the manager stated in the Service Datasheet/technician in charge, a member of the Data Security Department, and the person(s) responsible for the data affected by the incident, as a minimum.

- Any data system security incidents detected can be reported by both FCC staff and those of External Companies.

- FCC staff who detect potential incidents must not carry out any action other than the reporting the incident to the person in charge of the system affected, unless otherwise instructed by that person.

- As the FCC contact point for data security incidents, those in charge of Incident Management must be available and capable of providing suitable and timely responses.

- Once confirmed as such, all data security incidents must be logged by the Data Security Department.

- Maintaining this log is essential for both analysing possible attacks to FCC Data, and for identifying those in charge of it.

- The procedures developed by this Standard establish the minimum incident data that must be logged.

- Whenever incidents affect the security of personal data owned by FCC, the reporting and management procedure must include a log containing:

    - The incident type
    - The time it took place
    - The person who reported it
    - The person it was reported to
    - The consequences of the incident

- For medium to high-impact security incidents concerning personal data, the log must also include the following information:

    - The procedures carried out to recover the data (indicating the person who executed the process), the data restored, and the data that was manually recorded during the recovery process, if applicable.
    - The written consent of the person responsible for the data, in order to carry out the data recovery procedures.

Incident Identification and Analysis

- Logged incidents must be identified and analysed to assess their impact on the normal running of the business processes affected.

- To assess an incident's impact, the levels of criticalness stated in FCC's IT Data Services and Communications Catalogue must be referenced, or failing that, the estimated downtime and costs involved must be assessed.

- When not enough information has been reported to analyse and classify an incident, those in charge of the IT Data Services, or those responsible for the data itself, may take whatever actions they deem appropriate to gather more information about the incident.

- The incident management process will begin by carrying out a quick analysis of the situation to determine the scope of the incident, as well as the underlying causes and circumstances in which it took place.

- Before implementing any containment, response or recovery measures for security incidents, staff must first check the system for previously resolved similar incidents, in order to establish similar measures.

- Multiple incidents occurring simultaneously will be prioritised according to their seriousness. Priorities are established according to the level of criticalness assigned to the business data.

- Once the priority of a security incident has been evaluated, the management procedures for that specific incident will be implemented, and all steps carried out will be documented.

- Once analysed and prioritised, the incident must be notified to FCC or External Companies' staff or business units, so that they can notify any third parties that may be interested.

- Whenever technically possible, all logs and documentation related to incident management must adhere to a common standard format, which uses entry consolidation and a single retention policy.

Incident Containment

- Once an incident has been identified, the incident management team must decide whether to contain it, in order to stop the impact from growing.

- For that reason, an assessment must be made on how best to ensure the validity of the chain of custody whenever evidence might be required for legal or disciplinary purposes in the future and to establish what the implications are in terms of risks.

- A containment strategy for each specific incident must be implemented as part of the Incident Response Plan.

- The Incident Response procedures must ensure the segregation of duties and dual control, in order to strengthen the integrity of evidence gathered.

Incident Resolution and Recovery

Once an incident has been resolved, the person in charge of managing it must ensure:

- That all systems affected has been duly sanitised

- That the likelihood of a similar incident occurring in the future has been minimised

- That the security controls have been reviewed in order to assess the need to correct, extend or establish new controls

Any actions carried out during recovery operations are governed by the operating procedures approved by those responsible for the IT Data Services.

Incident Closure

- Once the systems are back to normal, the person responsible for managing the incident must notify this situation to all business units and department involved.

- The incident closure report must state that there is sufficient information to be able to follow the progress of the incident, the effectiveness of the measures implemented and the time invested in resolving it.

Incident Follow-up

- The information gathered from data security incidents must be documented in order to identify recurrent or high-impact incidents. By analysing this data, improvements or additional controls can be established to limit the occurrence rate and damage caused by future incidents.

- Given the rapid technological advances of data systems, the incident management team must hold six-monthly meetings to discuss new threat scenarios.

- This team must also meet after significant incidents have taken place, or when new attack techniques have been employed, in order to analyse them and figure out improved data security measures to those implemented.

- The information gathered in these meetings must facilitate improvements to incident management processes and the Data security policies and procedures, as well as provide new content for the Data Security training programmes available to both users and technical staff.

RESPONSIBILITIES

The Data Security and Risk Management Department must:

- Oversee the resolution of data security incidents, as well as implement preventative and corrective measures
- Provide FCC's Data Security Department Committee with incident resolution status reports
- Maintain relations with all organisations and legal representatives that may cooperate in the resolution of security incidents
- Report any security incidents detected while monitoring the critical systems managed by them

The Information Systems and Technology Department must:

- Produce the Incident Response Plans
- Ensure that FCC's technical staff receive sufficient training on Incident Management, so that incidents can be identified and reported as efficiently as possible
- Carry out verification testing of the Incident Management and Response Plan procedures.
- Review the audit logs periodically and notify the Data Security and Risk Management Department of any evidence of a security incident or any suspicious activities.

The security incident management team must:

- Take the decisions required to resolve incidents in accordance with the service levels agreed before the incident took place
- Effectively manage the human and material resources consigned to them for resolving incident

The Units Responsible for their own Data must:

- Ensure that all staff that access the data systems under their responsibility have received sufficient training to detect and report security incidents

- Cooperate with those responsible for Incident Management in resolving incidents and provide any information requested

The Users must:

- Immediately report and suspected security incidents to those responsible for the Service, the technicians in charge or the Data Security and Risk Management Department

- Maintain the required training and remain vigilant at identifying security incidents

REVIEW OF THIS STANDARD

This Standard may be reviewed in the following circumstances:

- Whenever there are significant changes in the FCC Group
- Whenever improvements are suggested as a result of audits carried out
- Whenever there are major technology changes

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.

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.

REFERENCES

- **Related Regulations**

  - FCC Data Security Policy
  - External Company Standard
  - Backup Management Standard

- **References to the ISO/IEC 27002:2007 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
1.0	2019 August	General Revision	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