Marko Buuri
Risk management

18 June 2015

Information Security Policy (public)

1 Vision of information security at FICORA

Information security is a critical factor in enabling the success of the Finnish Communications Regulatory Authority. FICORA is a pioneer in information security matters.

2 Information Security Policy

Information Security Policy is the most authoritative document of FICORA's information security management system, outlining the Authority's strategic intent in information security issues. This is a public summary of FICORA's internal information security policy, which is partly secret.

FICORA's information security management procedure covers all of its public authority and support functions. Where applicable, it also covers suppliers and other stakeholders to maintain the defined standard of information security and to protect the Authority's and its customers' information.

FICORA's information security guidelines consist of the Policy as well as information security action plans, management procedures, instructions and process descriptions in line with the Authority's information security management system. The Information Security Policy also covers technical implementations and configurations of FICORA's ICT management designed to achieve the strategic intent outlined in the Authority's information security management system. FICORA's Information Security Policy is regularly reviewed to ensure that it is up to date. This review takes place at least once a year.

In various information security measures, targets are chosen on the grounds of what FICORA considers important. Targets may include information systems, equipment, premises, documents, data, registers, management and steering systems, operations, processes, projects, goals, competencies and people. The tolerance of risks affecting information security is determined according to FICORA's Risk Management Policy.

Information security risks are evaluated regularly, risk management measures are targeted at the identified risks, and the success of risk management measures is monitored.

2.1 Internal and external environment of information security management

FICORA is a public authority belonging to the administrative sector of the Ministry of Transport and Communications.

FICORA's duties are defined in the public statutes concerning its operations. FICORA is the designated security authority referred to in the international information security obligations (Act on International Information Security Obligations, 588/2004).

External requirements concerning FICORA and information security are laws and regulations on information security, such as the Act on the Openness of Government Activities, the Personal Data Act, the Act on International Information Security Obligations and the Emergency Powers Act. In addition, information security in FICORA is guided by the Government Decree on Information Security in Central Government, the principles of good information management, the requirements of the various Government information security protection levels and the contracts and agreements made with stakeholders.

Within its administrative sector, FICORA is guided by the performance agreement drawn up with the Ministry of Transport and Communications. For self-regulation purposes, FICORA has a regularly updated vision and strategic objectives involving critical success factors that include efficient and secure premises and information systems, among others.

To verify the objectives of the measures related to its fundamental tasks and to better target the measures, FICORA maintains an up-to-date operating environment analysis. With respect to external stakeholders, FICORA will introduce systematic stakeholder policies and principles of stakeholder management. As part of stakeholder management, FICORA will identify the stakeholders that set security requirements for FICORA or that receive security reports from it. The purpose of this effort is to ensure that the Authority's security arrangements are in line with the stakeholders' objectives.

Information security is part of FICORA's performance management. Measures that apply to the entire Authority and concern its information security performance and continuous improvement in these matters will become a part of the Authority's performance bonus system and the annual plans of its divisions and units. The key measures affecting information security at FICORA are communicated to stakeholders in its operational and financial plan.

Information security is also part of FICORA's internal risk management. According to FICORA's Rules of Procedure, the Director-General is responsible for general risk management and information security policies, while the Directors of individual divisions are responsible for risk management in their respective areas of responsibility.

Where possible, FICORA uses the information security services provided by the Group management and strives to actively contribute to the improvement of information security in the state administration.

FICORA's information security management is constantly monitored and improved to maintain, at any time, the standard required by FICORA's objectives and requirements.

2.2 Objectives and opportunities for information security management

FICORA’s information security management must maintain a standard that ensures that objectives related to confidentiality, integrity and availability of information are met, meets the requirements for FICORA as a public authority, increases trust in FICORA as a partner and otherwise contributes to FICORA’s objectives.

Well-managed information security makes it possible to

- meet the targets of the performance agreement to be concluded with the Ministry of Transport and Communications,
- meet the targets of FICORA's strategy,
- provide reliable e-Government services and electronic communications to FICORA's customers and stakeholders,
- provide FICORA's employees with tools that support modern and flexible teleworking, mobile working and office working methods
- recover quickly and resume working in spite of disruptions.

The purpose of FICORA’s information security measures is to ensure disturbance-free data processing, protect secret information of the Authority and its customers, and ensure that the data, information systems and services that are essential for the Authority’s operations are always available, regardless of the location where the data is processed.

2.3 Information security management system

FICORA’s information security management system is an administration system designed to support the objectives of its information security vision and policy. The management system is a compilation of processes, practices, tools and guidelines to ensure that information security measures are always measured and targeted accurately. The management system is continuously improved through audits, innovations, reported irregularities, received feedback and other findings.

The target of FICORA’s information security management is to reach, as applicable, the standard defined by the requirements of the standard ISO/IEC 27001:2013, the information security requirements and recommendations of state administration, and the National Security Auditing Criteria (KATAKRI). Audits are conducted to ensure that these targets have been reached.

The targeted scope of the ISO 27001 certification of the management system is to cover FICORA’s public authority and support functions in Helsinki, excluding the tasks of the National Communications Security Authority (NCSA-FI), the

evaluation of public authority information systems, and the accreditation of information security inspection bodies. FICORA applies all management objectives and methods described in Annex A of the standard, since they are elemental in reaching FICORA's information security objectives.

FICORA maintains documents of its information security management targets. These documents may be physical documents or records in a database or in any other form where amendments can be controlled. Essential changes concerning the management targets or the methods to achieve them are discussed by FICORA’s Executive Group.

2.4 Monitoring

The information security management system is monitored by the risk management steering committee. Monitoring takes place through regular reporting, performance indicators, audits and reviews.

2.5 Breaches of the Information Security Policy

FICORA’s information security measures are guided by internal guidelines, but also legal acts and decrees, authority regulations and FICORA’s strategic policy guidelines.

FICORA monitors information security as part of its day-to-day operations. Breaches of the Information Security Policy may, in minor cases, lead to a formal reprimand by a supervisor or the risk management manager, but in worst cases to sanctions referred to in legal acts such as the Act on State Civil Servants or the Criminal Code and compensation paid to the parties involved.

3 Information security rules

Information security requirements concerning FICORA’s operations are delegated, as applicable, to suppliers through service purchase agreements. The suppliers’ employees must follow FICORA’s information security guidelines.

Information security breaches concerning FICORA shall, in principle, be reported to the police.