

The Finnish Government Information Security Development Plan

This document contains extracts of the Finnish Government Information Security Development Plan for the years 2004-2006. The implementation of The Plan has been started with wide participation.

1 FOREWORD AND ABSTRACT

Ministry of Finance is responsible for steering and development of information security in the Finnish Government and has set up The Government Information Security Management Board VAHTI for co-operating, steering and developing Government information security. The results of VAHTI co-operation are also widely utilised in local government and private sector as well, besides the Finnish Government.

Members of VAHTI represent various administrative sectors and levels of public administration as well as broad information security experience. The group is well known for its data security publications and guidelines. A recent study acclaimed VAHTI as the best working organisation of cross-government ICT and information management coordination.

In autumn 2003 VAHTI set up a task force to draw a development plan for information security in the Finnish government. This document presents the plan.

The Finnish Government Information Security Development Plan covers 6 main development areas, including altogether 28 development initiatives. Development initiatives have been prioritized and implementation has been scheduled.

The Ministry of Finance has the overall responsibility for the Development Program. VAHTI group assists the Ministry in the preparation, coordination, control and alignment of the program.

2 EXECUTIVE SUMMARY

Information security plays an important role in the information society and in government. Everyday operations of public authorities depend on systems and people working in a data secure way. Therefore, information security should not be considered as a separate activity but as an integral part of all processes and services and developed as such.

Information security incidents may have serious effects on a government agency, and in the worst case they may bring activities of the society into a halt. Security threats occur more and more frequently, and counter measures are increasingly difficult to take. In order to deal with all this and to prepare for future threats, VAHTI has prepared The Development Plan for Finnish Government's Information Security.

Development of information security should be based on each government agency's strategy and it should be linked to agency's operational and financial planning (*toiminta- ja taloussuunnittelu*). Otherwise, data security may not be taken into account when processes and services are being developed. Management by results and performance of government agencies (*tulosjohtaminen*) should be employed when appropriate. A guide on this is being prepared by VAHTI.

Public administration needs to be trusted by its clients and its employees. A high level of information security is an all-important ingredient in building of trust in public services and eGovernment in general. Furthermore, a good level of information security properly implemented will not impede improvement on efficiency and service level. To accomplish this, processes, systems and know-how have to be developed in concert.

Information security has gained in importance as the eGovernment services have proliferated and the number of customers has picked up rapidly. Consequently, government has completed many information security development activities, many of which embrace local government. The results of these are also utilized in private sector as well.

Information security is characterised by rapidly changing threats, which call for prompt, precise and well organised counter-measures. New technologies have a dual effect. On one hand, new more efficient services and ways of working become available. On the other hand, they introduce new data security problems and add to an ever increasing complexity of system management.

Compared to many other countries, the level of information security in Finland is high. Data security and privacy have been a concern to legislators, but the number of laws governing data security and privacy is high and increasing, and the overall situation in data security legislation can be considered as rather perplexing. Responsibility for certain areas of information security have been given to selected government agencies.

Each civil servant and each government agency should assume the final responsibility for data security. Ability to develop data security varies from one agency to another. Some may be self-sufficient and have the necessary expertise and resources to carry out major development projects on their own. Others, especially small agencies, rely more on external help and services. They need how-to -guides, outside IT and consulting services and government joint procurement schemes more than their big counterparts.

Investment in data security depends on nature of agency's activities and services, and on the confidentiality of information in its possession. Co-operation between government agencies will yield better results at less cost than every agency working on their own.

As a part of preparations for the development plan a survey on data security in the Finnish government was conducted. The survey revealed that the most acute problem at hand is e-mail spamming. Other topical areas include the lack of resources devoted to information security, negligence toward data security and malicious programs, especially viruses.

Traditional data security, especially that of printed documents, should not be neglected, but it should be developed along with Internet-related security issues.

The six main development areas to guide the overall development of data security:

1. **The creation of culture for data security.** This includes various initiatives ranging from use of management by results and performance (*tulosohjaus*) to security training programs. Various metrics should be developed and employed to monitor the development of data security. They should be accompanied by security audits.
2. **The general strengthening of government information security development.** This is done mainly by assuring that both the Ministry of Finance and the Government Information Security Management Board VAHTI have enough resources to meet the growing demand for data security information. Along with VAHTI other means of co-operation and coordination will be promoted. The need for and methods of regulation for Government on data security issues will be investigated.

3. **Data security in communication and IT-systems** will become increasingly important. This development area includes fighting against spam, introducing new secure means of communications, and other ways to assure that the information technology of eGovernment will operate smoothly.
4. **IT and data security professionals work** in the front line of data security. Their time is scarce and all too often their valuable know-how is sidelined by assigning them with responsibilities which are of secondary importance. This problem will be tackled by providing them with first class and ready-to-use information security guides and by use of cross government procurement and project schemes in data security products and services.
5. **Service and process developers work needs to be supported**, so that data security and privacy protection are taken into consideration from the initial phases of service development. This minimises the possibility that a new eService would infringe privacy or data security laws.
6. **The end user data security.** Data security training and efficient and transparent data security environment are important ingredients in end user data security as well as managers' practice-what-you-preach -attitude.

Good level of information security cannot be attained without adequate investments and expertise. Having computer security programs installed and devices up and running is a must, but information security development should not be stopped once this has been achieved. Employee computer literacy, IT managers cutting edge knowledge and service agreements inclusive data security are a prerequisite for the information security development. Funding for information security and its development programs have to be included in budgeting process.

The Ministry of Finance has the overall responsibility for the Development Program. VAHTI group assists the Ministry in the preparation, coordination, control and alignment of the program.

3. FURTHER INFORMATION

For further information, please contact Mr Mikael Kiviniemi, tel. +358 9 160 33269, email firstname.lastname@vm.fi.