MINISTRY OF TRANSPORT AND COMMUNICATIONS
Communications Policy Department, Communications Networks

1.12.2008

GOVERNMENT RESOLUTION ON NATIONAL INFORMATION SECURITY STRATEGY

"Everyday security in the information society – a matter of skills, not of luck."

Objectives of the Strategy

The National Information Security Strategy aims to make everyday life in the information society safe and secure for everyone in Finland – for people as individuals and for businesses, administrative authorities, and all other actors in society. The Strategy's vision is that people and businesses will be able to trust that their information is secure when it is processed in information and communications networks and related services. There must be a high overall level of information security skills and knowhow, and the different actors in society need to work seamlessly together to improve information security. By 2015 Finland will be the leading country in the world in terms of information security.

Priority 1: Basic skills in the ubiquitous information society

Priority 2: Information risk management and process reliability

Priority 3: Competitiveness and international network cooperation

Measures

Priority 1: Basic skills in the ubiquitous information society

Everyone's actions in the information society have impacts both on their own information security and on that of others. It is therefore important that everyone has adequate basic skills in the field of information security. Trust in the information society is built up when both users and service providers understand their rights and their responsibilities.

Users of electronic services must be able to identify, and be aware of, the underlying principles of secure and reliable service. Internet literacy and a basic national level of skills in using electronic communications are necessary preconditions for the secure use of online services. The ability to anticipate, identify and take precautions against risks can spare the user from many unpleasant surprises. **Service providers** in particular must ensure the security of services and, for their part, also take care that confidential information is identified and protected. The service provider is also responsible for making sure that service security is continuously maintained in the changing service and operational environment.

The provision of clear transparent information about the security of services and the possible risks involved lays the groundwork for the trust that is needed in the ubiquitous information society. The responsibility of the service provider cannot be outsourced. In practice, the service provider is responsible for ensuring that the operations of all players involved in providing the services are secure. The task of the National Information Security Strategy is to integrate information security firmly into the basic structures of the information society. This requires improvements in general information security awareness and skills, and better consideration of information security aspects in the purchase of systems and the procedures for making agreements.

- **Increasing information security awareness and competence**
    - The National Information Security Day project will be developed.
    - Awareness of information security will be improved, the level of awareness will be monitored and information security skills will be developed.
    - A proactive plan for communications will be drawn up.

- **Providing secure electronic services and ensuring confidentiality**
    - Information security requirements will be incorporated in every invitation to tender, including the planning phases of solutions and services.
    - More extensive use of information security solutions will be promoted.
    - The possibility of introducing special certification for secure services will be investigated.
    - An increase in the number of certified information security professionals in Finland will be promoted.

Priority 2: Information risk management and process reliability

Electronic services and communications are increasingly to be found at the heart of the service system in both the public and the private sectors. At the same time, dependence on information technology is making services more vulnerable than ever. People using the various communication services must be able to trust that the services are secure and that no confidential data will end up in the wrong hands. When a breach of information security occurs, for example in identity theft, people and businesses must be able to rely on adequate support from the authorities.

It is essential to take a holistic approach to information security when services are outsourced and chains of acquisitions are formed. The security of data in the entire network should be evaluated when services are being planned. The primary responsibility for this lies with the service provider. Confidentiality and intactness of data, together with accessibility, are essential elements in the services.

The proper functioning of critical information society infrastructure and the security of ICT systems and services must be ensured at all times, both in normal and emergency conditions. The continuity of business activities and the public's access to services must be fully safeguarded.

- **Improving risk management and service reliability**
    - Support will be provided for the wider adoption of risk management models for businesses.
    - Training related to risk management will be arranged.

- **Safeguarding functions that are vital to society in all circumstances**
    - Research will be carried out as to how procedures and response capabilities should be developed for ever more complex networks and network administration.
    - The possibilities of supporting preparedness and risk management in businesses will be explored.
    - Legislative support will be provided to safeguard the communication networks and services necessary for the functions vital to society.

Priority 3: Competitiveness and international network cooperation

Finland should aim to develop a simpler and more predictable national regulation environment for businesses, and actively seek ways to influence the drawing up of international regulations. Clarity of national legislation and the removal of obstacles to business will improve Finnish competitiveness and companies' willingness to invest in Finland. Care must be also taken to make sure that differences in the national implementation of EU directives concerning information security do not unreasonably impede Finnish companies that operate in several Member States. It is crucial for a competitive information society that its most important information and knowledge capital, such as industrial property rights and business secrets, is protected. These measures can safeguard business activities in Finland and the operation of Finnish companies abroad and make Finland more attractive as a corporate location.

Finland is part of the global information network economy, and most information security threats and attacks come from outside the country's borders. Prevention of these threats requires not only comprehensive preparedness and efficient networks of international cooperation but also a forward-looking approach and the identification of signs and signals of threats, however weak. Finland must be active in international cooperation between national authorities to prevent information security threats and minimise any possible damage. Globalisation is not just a threat but also an opportunity. To act effectively in international forums, Finland must be able to prioritise its international activities and allocate resources to key information security issues. Effectiveness can only be achieved through good national cooperation and exerting an influence on decisions before they are made.

- **Increasing Finland’s attractiveness and competitiveness through better predictability**
    - Promotion of the adoption of international standards and active participation in international development work.
    - Active involvement in EU cooperation to ensure that information security directives are implemented in as uniform a way as possible and so also promote the activities of Finnish companies operating in several countries.

- **Intensifying forward-looking and influential international cooperation**
    - The creation of a national network for the purpose of exchanging information and experiences of international working groups will be considered.
    - The need to establish a National Communications Security Authority (NCSA) in Finland will be examined.

Implementation of the Strategy

The overall responsibility for the National Information Security Strategy lies with the Government, which supervises the Strategy’s implementation and updates it when necessary. The Information Security Group of the Ubiquitous Information Society Advisory Board appointed by the Ministry of Transport and Communications supports the coordination of the Strategy’s implementation and monitors the implementation process. The Information Security Group submits an annual report to the Government on the implementation of the Strategy and on the need to update it, and reports to the Ubiquitous Information Society Advisory Board on the progress of the work.

In order to attain the Strategy’s goals, an action plan will be drawn up based on the priorities set out in this Resolution. The measures, indicators, monitoring and follow-up necessary for the implementation of the Strategy will be included in the action plan, which will be completed by spring 2009.