



MINISTRY OF FINANCE  
FINLAND

# USER'S INFORMATION SECURITY INSTRUCTION

5/2003



THE GOVERNMENT INFORMATION SECURITY MANAGEMENT BOARD

VAHTI

# USER'S INFORMATION SECURITY INSTRUCTION

5/2003

*THE GOVERNMENT INFORMATION SECURITY  
MANAGEMENT BOARD*

VAHTI

**MINISTRY OF FINANCE,  
FINLAND**

Snellmaninkatu 1 A, Helsinki  
P.O. Box 28  
FI-00023 GOVERNMENT  
FINLAND

**Telephone**

+358 9 160 01 (Switchboard)

**Fax**

+358 9 160 33123

**Internet**

[www.vm.fi](http://www.vm.fi)

**Inquiries**

Telephone +358 9 160 33 222

E-mail:

[vahtijulkaisut@vm.fi](mailto:vahtijulkaisut@vm.fi)

ISSN 1455-2566

ISBN 951-804-405-8

Edita Prima Ltd  
HELSINKI 2004

## FOREWORD

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 information security instructions and guidelines as well other information security publications.

In winter 2003 VAHTI set up a task force to draw information security instruction for end users as well as other necessary material to develop end user information security. This document presents one of the key results of the task force.



## INDEX

INTRODUCTION .....	7
Check list of information security .....	7
What is meant by information security? .....	8
Why is information security important? .....	9
Legislation forms the foundation of information security .....	9
Processing of data .....	11
USE OF THE COMPUTER .....	13
Access rights and passwords .....	14
Internet and email .....	15
Remote access and remote work .....	17
Security of premises .....	18
YOUR OWN INFORMATION AND PRIVACY .....	19
Duty to notify .....	19
What to do in problem situations? .....	20
Consequences .....	20
For additional information, see .....	21
Information Security Instructions of the Ministry of Finance and the Government Information Security Management Board VAHTI .....	23

---

# INTRODUCTION

This Information Security Instruction is meant for all users in public administration. The Instruction summarises the most central basic issues of information security and gives practical advice for the implementation of information security in one's own work.

## *Check list of information security*

---

1. Information security is based on legislation and normative guidance.
2. Attendance to information security belongs to everyone, including you.
3. Identify the targets to be protected in your organisation (information, documents, premises and information systems).
4. Identify the nature of documents and information (confidential information, personal data, etc.).
5. Familiarise yourself with the Information Security Instructions of your organisation and comply with them.
6. The use of information systems always requires a personal access right.
7. Remember that in the data network you represent public administration.
8. The security of unprotected email can be compared to the security of a postcard.
9. You may distribute malicious programmes, such as viruses, worms and Trojans, simply by browsing Internet sites.
10. Where necessary, request the experts of your organisation for assistance.

## *What is meant by information security?*

---

Information security means the appropriate protection of information, systems, services and data communications by administrative, technical and other measures both in ordinary and exceptional circumstances. The confidentiality, integrity and availability of information is protected against threats and damage caused by faults in hardware and software, natural events and both wilful, negligent or accidental events.

The central concepts of information security have the following meanings:

**Confidentiality:** information and systems are accessible only to those authorised to use them. Third parties are not given a possibility to alter or destroy information nor to process it otherwise.

**Integrity:** information and systems are reliable, correct and up-to-date and they have not been altered nor can they be altered in an uncontrolled way as a result of hardware or software faults, natural events or human activities.

**Availability:** information and services in the systems are accessible to those entitled to use them within a response time determined in advance. The information has not been destroyed nor can it be destroyed as a result of faults, events or other operations.

Other general requirements of information security include the verification of the parties and the nonrepudiation of a transaction, which are especially important when it must be possible to identify the users of the system for example for interactive electronic communications or remote work.

**Authentication** means reliable identification of the parties (person or system).

**Nonrepudiation** means subsequent legally binding proof of what has happened. Nonrepudiation ensures that the other party cannot deny its actions afterwards.

## *Why is information security important?*

---

The operations of public administration are extremely dependent on data and information technology. Information society development, internationalisation, networking and the transfer of operations and services to data networks further enhance their significance. Information security is the means to ensure the management of important information and the continuity of operations.

Information security is also important because public administration processes a lot of important information, such as personal data, financial information and documents of various organisations. Some of the information has to be kept secret or it is sensitive or otherwise confidential. Information to be kept secret means documents and information provided secret by the law. Secrecy is governed i.a. by the Act on the Openness of Government Activities, the Personal Data Act and other special Acts. Certain documents of the authorities to be kept secret are governed by a security classification. Therefore it is important that the information does not, wilfully or otherwise, end up in the hands of unauthorised parties.

In addition, public administration involves a lot of information that is not to be kept secret but which is public in nature, but we must ensure that also this information is correct, unaltered and accessible and processed according to the law.

## *Legislation forms the foundation of information security*

---

*“In order to create and realise good practice on information management, the authorities shall see to the appropriate availability, usability, protection, integrity and other matters of quality pertaining to documents and information management systems.”* (Act on the Openness of Government Activities 18 §, Good practice on Information Management)

*“The registrar shall carry out the technical and organisational measures necessary for securing personal data against unauthorised access, against accidental or unlawful destruction, manipulation, disclosure and transfer and against other unlawful processing.”* (Personal Data Act 32 §, Data security)

In addition to the Act and Decree on the Openness of Government Activities, information security is governed by numerous other Acts. The protection of privacy and the principle of openness are basic rights governed by the Constitution. In addition to provisions on secrecy contained in various Acts, the most important of these Acts are

- The Constitution (731/1999), Chapter 2 § 10 (The right to privacy and the secrecy of confidential communications)
- The Constitution (731/1999), Chapter 2 § 12 (Right of access to documents and recordings in the possession of the authorities)
- Act on the Openness of Government Activities (621/1999)
- Personal Data Act (523/1999) (General rules on the processing of personal data)
- The Archives Act (831/1994) (Drafting, saving and use of documents)
- Act on State Civil Servants (750/1994) §17 (Provision on State civil-service relationship)
- Act on a Municipal Civil Servants (304/2003)
- The Employment Contracts Act (55/2001)
- The Penal Code (39/1889), Chapter 34 § 9a (Criminal computer mischief)
- The Penal Code (39/1889), Chapter 38 § 8 (Computer break-in)
- The Penal Code (39/1889), Chapter 38 § 9 (1) (Personal data offence)
- Personal Data Act (523/1999) § 48 (Personal data offence)
- Tort Liability Act (41/1974)
- Act on the Protection of Privacy in Working Life (477/2001)
- Act on the Protection of Privacy in Telecommunications and the Data Security of Teleoperations (565/1999)

## *Processing of data*

---

Here data refers to information stored, processed or transferred in different modes. The data may consist of a single document, a file, a voice or picture recording, speech, database, software to be executed, a sample or some other form. The data has to be looked at from the viewpoint of its total lifecycle. The stages of data processing are its creation, use, alteration, storage, transfer, distribution, copying, filing and destruction.

When processing information it must be taken into consideration that the data being processed is often significantly more valuable than the medium used in the processing. This means that data have to be protected at all stages of processing.

- Identify the classification of material and any restrictions relating to its use, disclosure and processing. (e.g. the Information Security Instruction on the Processing of Government Data Material VAHTI 2/2000)
- If you are drafting a document to be kept secret, you are, in accordance with your tasks, also responsible for its classification and marking. Some material to be kept secret is governed by security classification.
- Handle information carefully irrespective of the medium – no matter whether the information is transmitted by computer, paper, telephone, tape, laboratory sample or telefax.
- Information in data storage regarding which you have access rights may be used only for work assignments.
- Where possible, store what you have created on a server, from where Information Management will verify the information. Avoid a situation in which a document or other material exists only in your own personal computer, because if the hard disk is destroyed, all data may be lost.
- Always check a diskette, CD ROM or other storage medium brought from outside the office with a virus programme before using it.
- When processing secret information or typing in a password, make sure that no one can see the display or keyboard of your computer.
- Avoid unnecessary printouts and copies, because extra copies increase the danger of the material falling into the wrong hands.
- Ensure the printer to which you are printing and its location.

- When using a network printer, fetch your printout right after printing it.
- Use thrashers and information security material collection boxes complying with the protection requirements to destroy information to be kept secret.
- If you have to send confidential information, ensure that the recipient is entitled to it and that he receives the material.
- Remember that you may use and process information only when attending to your own tasks. The use of information in a personal data file violating its purpose of use is against the law. Remember that the browsing and other use of information is subject to supervision.
- Make sure that you do not disclose confidential information in a public place. Take care for example when talking in a public vehicle or in the street.
- Kill all gossip.

---

## USE OF THE COMPUTER

The use of the computer means the use of services available both through one's own workstation and through the network.

- As a user you are responsible for your own computer. Remember to be careful.
- Always log in with your own user identifier and password.
- Prevent unauthorised use of information systems by logging off your computer whenever you leave your room. You may also use a password-protected display saver. In order to spare electricity, you can turn off your display for the night.
- Remember to log off both from software and your computer.
- If you use public terminals or a computer temporarily in the possession of another person, always remember to log off both from the software and the computer at the end of your work.
- The installation and updating of hardware and software may only be carried out by Information Management.
- Should a hard disk or other storage medium, such as a diskette, be broken or otherwise removed from use, it must not be thrown in the waste bin; instead, submit the storage medium to Information Management, which will attend to its proper destruction and ensure that the data material is not disclosed to third parties.

## *Access rights and passwords*

---

Access rights are always required for an information system. The access right is personal and it always relates to you personally and to your task. Always treat your user identifier and password in the same way as you treat your bank card and identification code.

- Never give your personal user identifiers or passwords or smart card or PIN code to be used by another person, not even by ADP personnel, because they do not need them. Be suspicious of any inquiries relating to your passwords or access rights to information systems.
- Change your passwords sufficiently often and as soon as you suspect that they have been revealed.
- Ensure that the passwords are sufficiently complicated and avoid using familiar everyday names as passwords. A good password may include both lower and upper key letters, numbers and even special characters. However, special characters cannot be used with all systems. A good password is one which you can easily remember but which an outsider cannot easily guess.
- Do not write your passwords down.
- Do not use the personal user identifier and password of the organisation when you register in the Internet.
- In certain situations or systems one has to use common identifiers. The use of common identifiers is decided by the owner of the system or information. The use of common identifiers is allowed only by permission of the owner.
- The password of common identifiers available to more than one person has to be changed whenever the access right of a user terminates or when it is suspected that someone outside the group has learned the password. Also otherwise, the password has to be changed often enough.

## *Internet and email*

---

The Internet and email are good tools both for information retrieval and contacts. However, it must be remembered that email or the Internet themselves have no protection, but that the information moves unencrypted in a public network. Therefore the use of email and the Internet require that the user be careful.

- The Internet and email at the workplace are meant for official use.
- The Internet may not be used to transmit confidential information without proper encryption. The information has to be encrypted by means approved by Information Management before it is sent through a public data network.
- Learn the correct use of encryption products so that you do not, by mistake, send information unencrypted.
- Do not use or install software available through the Internet.
- If you use public terminals or a computer temporarily in the possession of another person, remember to delete the cache memory of your Internet browser and to delete any cookies. Where necessary, ask Information Management for assistance.
- Remember that an authority has an obligation to process official email.
- Official email may be processed only with hardware owned by one's own organisation or another organisation of public administration.
- Work-related email is received and directed to the email system of one's own organisation. It may not be directed outside the email system of one's own organisation.
- Instruct all customers using electronic communications to send any matters to be handled and pending to the email address determined by the organisation.
- Remember that you are – in accordance with your official duties – responsible for any work-related mail that may come to your personal email.
- The use of other than official email is allowed at work only with the permission of one's own organisation. This includes for example free email software from the Internet or your email at home.

- Ensure that your email will be processed in accordance with your official tasks during your absence.
- Appended files may contain malicious programmes (viruses, worms or Trojans). Be suspicious of any unusual email and especially appended documents. Do not open any suspicious messages, but inform Information Management thereof.
- Junk mail includes i.a. any advertisements coming to your email without your order. Junk mail should not be answered; instead, it should be destroyed right away. If you answer a message, the sender of junk mail will know that your email address is functioning and he will continue sending you junk mail and also transmit your address to other senders of junk mail. You can avoid junk mail by not giving your email address on inappropriate www sites. You should also avoid giving any other personal information.
- Have a healthily suspicious attitude towards the security of email. Anyone can send email in the name of someone else. Also viruses are able to send email without any measures by a user.
- Ensure that all the email that you send is directed at the correct persons and the correct addresses.
- Avoid sending unnecessary email. For example the sending of Christmas greetings means an extra load both for the email system and the email box of the recipient.
- Do not transmit chain letters onwards.
- If you receive email belonging to someone else, direct the message to the correct recipient and inform the sender of the correct email address of the recipient. If you do not know the correct address, notify the sender of the erroneous transmission. Remember that you have to keep the message that you have received confidential.
- A distribution list is a list of persons sent to each recipient and it may constitute personal data information or confidential information governed by specific provisions on disclosure. You may use the hidden copy function if you do not want the recipients to see each other's names.
- Upon the termination of an employment relationship, your email address and box will be removed. Make your official mail available to your employer and delete any personal messages.

## *Remote access and remote work*

---

We talk about remote access when you use the data network of the organisation or part thereof from outside the organisation by means of a data communications connection. Remote work means work done elsewhere than at the permanent premises of the office.

- Remote access and remote work is allowed only subject to separate agreement.
- Remember that all work done at the office cannot be done in the form of remote work with full information protection. Identify this type of work.
- The employer will attend to the acquisition and installation of hardware, software and data transfer connections required for remote work.
- When you use a remote connection, you are part of the data network of the organisation and therefore you have to take into consideration the same issues in the processing of information as when you are in the actual premises of the organisation.
- Make sure that any hardware, software, data communications connections and paper material that you use in remote work are only accessible to you.
- Make sure that all user identifiers, passwords, smart cards and other verification media are only in your possession and known only to you.
- Carry with you only the necessary amount of data material and always ensure the appropriate protection of the material.
- Remote work has to be limited to material whose disclosure does not endanger the information security of the office. In the same way as in the office, also in remote work you must always take into account the classification of the material and the related use as well as any restrictions on disclosure, use and processing.

## *Security of premises*

---

The security of premises ensures that information, documents and computer equipment are kept and handled appropriately in secure premises. The security of premises includes i.a. access control, technical supervision and control, the prevention of fire, water, electricity, ventilation and burglary damage as well as the security of couriers and dispatches containing data material.

- Comply with instructions on access control. Direct guests or “lost” persons to the right places. Do not let inappropriate persons into the premises for example when leaving work.
- Do not leave doors subject to access control open.
- You are responsible for your own guests and their movements in the premises either personally or with the help of a secretary or another person belonging to the staff of the organisation.
- Keep all information and equipment secured, where possible, in a locked desk or room.
- Never leave a laptop or mobile phone without supervision. Keep the equipment in a locked space. Remember also the appropriate safekeeping of diskettes, paper printouts, etc.
- Be especially careful when travelling. Laptops or mobile phones may not be left visible in a car nor may they be left in the car overnight.
- Comply with the “Clean Desk Principle”. No confidential information may be kept on the desk.
- Do not leave a guest in your own room or in other premises alone or without supervision.
- In a point visited by clients, the computer display may not be visible to the client.

---

## YOUR OWN INFORMATION AND PRIVACY

- You must not unnecessarily store your own personal files on your workstation or on the server.
- You are yourself responsible for the processing of personal messages you have received.
- Detailed log information on the use of the systems is stored in the systems and in the data network. This information is used for maintenance, fault detection and the supervision of information security.
- All employees are liable to keep confidential any private messages they have learned of.
- Email traffic and Internet browsing as well as the use of the inquiry systems are supervised e.g. for reasons of sufficiency of capacity, and any abuse may be interfered with.

### *Duty to notify*

---

- Always notify the person in charge of information security, Information Management or your own superior without delay of malicious programmes (viruses, worms and Trojans) as well as of other issues relating to information security.
- Likewise, always notify the person in charge of security, office managers or your own superior without delay of other suspicions or problems relating to security.

## *What to do in problem situations?*

---

Violation of information security may be suspected when your computer for example suddenly slows down even if you have not performed any specific function or if unexpected notices or warnings appear on the display.

- Do not panic.
- You need not close your computer.
- Write down the contents of any notice or warning.
- Contact Information Management and/or the person in charge of information security.
- Act according to instructions.
- Assist in the investigation; tell the investigators what you were doing when the computer started to function in an unexpected way.
- Write down what you have done and report lost working hours for a possible claim for damages.

## *Consequences*

---

- A violation of the laws, regulations and instructions may result in a revocation of access rights to information systems. The superior is always notified of any violations.
- If a violation results in financial losses, this may lead to a claim for damages.
- An abuse of information or wilful or negligent operations in violation of the laws, regulations and instructions may result in disciplinary measures, such as a notice to terminate your employment relationship and/or criminal-law sanctions.

## *For additional information, see*

---

- The instructions of the organisation
- Legislation
- The instructions of the Ministry of Finance and VAHTI ([www.financeministry.fi/security](http://www.financeministry.fi/security))
- Other organisations issuing instructions and provisions on information security (e.g. the Finnish Communications Regulatory Authority, the Office of the Data Protection Ombudsman and the National Archive Service)
- Chief of Information Security, Information Management, superior, Chief of Security



## ***Information Security Instructions of the Ministry of Finance and the Government Information Security Management Board VAHTI***

- Risk Assessment Instruction to Promote Government Information Security, VAHTI 7/2003
- General Instruction on Information Security Education in Public Administration, VAHTI 6/2003
- User's Information Security Instruction, VAHTI 5/2003
- Glossary of Government Information Security, VAHTI 4/2003
- Assessment of Information Security Management, VAHTI 3/2003
- Secure IT Architecture for Remote Access, VAHTI 2/2003
- Authentication in Government Electronic Services, Ministry of Finance, 2003
- Secure Use of the Internet, VAHTI 1/2003
- Instructions for Processing Sensitive International Material, VAHTI 4/2002
- Information Security Instruction for Remote Work, VAHTI 3/2002
- Information Security Recommendation for ICT Rooms, VAHTI 1/2002
- IT Security and Ensuring Operations, Ministry of Finance and National Board of Economic Defence, 2002
- Actions and Response in Attack Situations, VAHTI 7/2001
- Information Security Checklist for ICT Procurements, VAHTI 6/2001
- Secure eMail and Log Data Policy, VAHTI 5/2001
- General Instruction on Information Security of Electronic Services, VAHTI 4/2001
- Methods and Recommendations for Cryptography, VAHTI 3/2001
- Information Security Recommendation for Government LANs, VAHTI 2/2001
- General Instruction for Government Information Security Work, VAHTI 1/2001
- General Instruction on Protection against Viruses and Other Malware, VAHTI 4/2000

- Information Security Recommendation on Information System Development, VAHTI 3/2000
- Information Security Instruction on Processing Government Data Material, VAHTI 2/2000
- Instruction on Destroying Unnecessary Data Material, Ministry of Finance 19.4.2000
- Recommendation for Drafting an Information System Report, Ministry of Finance 17.2.2000
- Instruction on Security Classification and Marking of Secret Information and Documents, 2000
- Information Security Recommendation for Outsourcing, VAHTI 2/1999
- Recommendation for Security of Premises, Ministry of Finance 31.12.1998
- Information Security in Management by Results and Development Tools, VAHTI 2/1997

# VAHTI



MINISTRY OF FINANCE, FINLAND  
Snellmaninkatu 1 A, Helsinki  
P.O. Box 28  
FI-00023 GOVERNMENT  
Telephone: +358 9 160 01  
Fax: +358 9 160 33123  
[www.vm.fi](http://www.vm.fi)

5/2003  
USER'S INFORMATION  
SECURITY INSTRUCTION

ISSN 1455-2566  
ISBN 951-804-405-8