MINISTRY OF FINANCE
Finland

Information Security Instructions for Personnel

The Government Information Security Management Board

4/2009 VAHTI

MINISTRY OF FINANCE

Information Security Instructions for Personnel

The Government Information Security Management Board

4/2009 VAHTI

Printed matter

MINISTRY OF FINANCE
PO Box 28 (Snellmaninkatu 1 A) FI-00023 GOVERNMENT
FINLAND
Tel. +358 9 16001
Internet: www.financeministry.fi
Layout: Anitta Heiskanen

Edita Prima Plc
Helsinki 2009

Introducing the organisation – VAHTI's task

The Ministry of Finance is responsible for the steering and development of central government information security in Finland and has set up the Government Information Security Management Board (VAHTI) as the body responsible for cooperation, steering and development in the area of central government information security. In its work, VAHTI supports the Government and the Ministry of Finance in decision-making and in the preparation of decisions relating to central government's information security.

VAHTI's objective is, by developing information security, to improve the reliability, continuity, quality, risk management and contingency planning of central government functions and to promote information security so that it becomes an integral part of central government activity, steering and performance management.

VAHTI handles all the significant central government information security policies and the steering of information security measures. VAHTI also handles central government information security statutes, instructions, recommendations and targets. All areas of information security are subject to VAHTI's scrutiny.

VAHTI's work has improved central government information security, and the effectiveness of its work is evident not only in the central government but also in companies and internationally. The result is a very comprehensive set of general information security instructions (www.vm.fi/VAHTI). Led by the Ministry of Finance and VAHTI, a number of joint information security projects have been implemented with ministries and agencies. VAHTI has prepared, managed and implemented the central government information security development programme, in which significant development work has been achieved at a total of 26 development locations by 300 people appointed to the projects.

VAHTI promotes the development of networked operating practices in public administration information security work.

In addition to the central government, the results of VAHTI's work are also widely utilised in local government, the private sector, international cooperation and everyday life. For three years in succession, VAHTI has been recognised with an award for exemplary work in improving Finland's information security.

Contents

Introducing the organisation – VAHTI's task 3

1 Introduction 7
1.1 Basic instructions 7
1.2 What is meant by information security? 8
1.3 Why is information security important? 9
1.4 Legislation forms the basis of information security 9

2 Records management and information processing 11
2.1 Work-related information 11
2.2 Interviews, enquiries, research and disclosure of information 13
2.3 Own information and privacy 13

3 At the workplace 15
3.1 Use of computers 15
3.2 Access rights and passwords 16
3.3 Internet and e-mail 16
3.4 Security of premises 18

4 Mobile work, telework and working when travelling 21
4.1 Mobile work and mobile devices 21
4.2 Telework and remote access 22
4.3 On a home computer 23
4.4 Working when travelling 23

5 Problem situations 25
5.1 Duty to notify and how to act in problem situations 25
5.2. If you suspect an information security breach or malware infection 25
5.3 Consequences 25

6 Further information 27
Appendix 1: Key statutes relating to information security 29
Appendix 2: Valid VAHTI publications 31

1 Introduction

Information security is based on legislation and standards. Responsibility for information security and related expertise lies with everyone, including you. These information security instructions are intended for public administration personnel, those working on public administration assignments (e.g. service providers) and people regularly using its information systems or premises (e.g. students). These instructions can also be used where applicable in other public administration organisations.

These instructions summarise the basic issues of information security. They provide guidance on the implementation of information security in everyday work and in other practical situations. An effort has been to write these instructions so that they are suitable for as many organisations as possible. Each organisation may, however, owing to the special nature of its operations, have exceptions, additions and clarifications to these instructions, which naturally should be complied with. Moreover, should you think of a good idea to improve information security, take the initiative and propose it within your organisation.

1.1 Basic instructions

1. Follow information security bulletins, familiarise yourself with information security instructions and participate in training offered to you. Act according to the instructions you receive.
2. Support your organisation's access control and display your photo ID card (if such is supplied) on the organisation's premises.
3. Do not leave visitors alone or unsupervised in your office or in other organisation premises.
4. Do not allow a visitor to use your computer.
5. Adhere to the 'clean desk' principle. Do not keep confidential material on your desk.Handle information carefully irrespective of the medium, whether it is conveyed by person, computer, paper, telephone or telefax.
6. Do not disclose your personal user IDs and passwords to another person – not even to information management personnel, because they do not need them.

7. Do not allow anyone to look at your computer display or keyboard- when you are processing sensitive information or when you are typ- ing inuser IDs and passwords.
8. Change your passwords sufficiently often and immediately when you suspect they may have been disclosed.
9. Use information materials and tools only for handling your tasks.
10. Don't install software or make changes to its settings if this is not part of your job description.
11. Save your work on a network server, where the data will be backed up centrally.
12. Fetch your printouts from the network printer immediately after- printing.
13. Remember that when you are using your organisation's equipment, network or e-mail you are always viewed on the information network – even unintentionally – as a representative of the organisation.
14. Always use appropriate encryption, if you have to transfer confidential information via the internet.
15. If you transfer information using a memory stick or other information storage medium, always supervise the transfer personally.
16. Prevent unauthorised access to information systems by always locking your workstation when you leave your room.
17. At the end of each working day, log out of the information system and switch off your workstation in accordance with organisation-specific instructions.
18. Always report information security problems as well as perceived threats and security shortcomings immediately to the person re- sponsible for information security, the Information Management organisation and your own supervisor. It is their duty to initiate the required measures.
19. Ask, if necessary, the advice of your organisation's experts.

1.2 What is meant by information security?

The purpose of information security is to ensure that information, information systems, and services receive appropriate protection, so that risks related to their confidentiality, integrity and availability are appropriately managed. Information security is an element of an organisation's operational quality.

In practice this means, among other things, that some of the information and information systems are accessible only to those authorised to use them.

Accordingly, third parties are given no opportunity to process, modify or delete information. Those authorised to process information can only use information and systems appropriately in their tasks. Information, systems and services must be reliable, correct and up-to-date. They should not be disclosed, modified or destroyed in an uncontrolled way as a result of unauthorised activity, malware, hardware or software faults, or other damage or incidents. Information, systems and services must also remain active and be accessible when they are needed. The increasingly widespread use of electronic services has additionally highlighted the requirement that users of electronic services be identified reliably and that the existence and content of electronic services events can also be substantiated later.

1.3 Why is information security important?

Information security measures safeguard the interests of the individual, the organisation and society. Information security is a fundamental prerequisite of the functions, services, applications and information technology infrastructure of society. Indeed, the functions are nowadays to a large extent dependent on the processing and transfer of information. In a networked operating environment, few organisations still have sole responsibility for their own information security.

Attending to information security is the duty of everyone working in an organisation. The major information security problems are generally related to haste, carelessness, lack of expertise and other qualitative factors connected with the implementation and use of information systems. Information security is only as good as its weakest link. It therefore depends not only on technology but also on our everyday operating practices and attitudes. Inadequate information security jeopardises the interests of the government, citizens, organisations and customers, and also generates extra work and costs. By enhancing information security, the reliability and continuity of functions are improved.

1.4 Legislation forms the basis of information security

The public administration processes a vast amount of both public and confidential information. Finnish legislation contains many information security obligations; a fundamental premise of legislation is that information security must be appropriately arranged. Information security is based on the Act and Decree on the Openness of Government Activities as well as a number of other acts. The protection of privacy and the principle of openness are basic rights enshrined in the Constitution. According to the openness legislation, information is public unless it is to be kept secret on the basis of the Openness Act

or other statutes. The authorities must always ensure that information is processed according to the law.

"In order to create and implement good information management practice, the authorities shall see to the appropriate availability, usability, protection and integrity of documents and information systems and the information contained in them as well as other factors affecting the quality of information." (Act on the Openness of Government Activities, Section 18 Good Information Management Practice)

"The data controller shall carry out the technical and organisational measures necessary for securing personal data against unauthorised access, accidental or unlawful destruction, manipulation, disclosure and transfer, or other unlawful processing." (Personal Data Act, Section 32 Data Protection)

A list of statutes mainly relating to information security is appended to these instructions.

2 Records management and information processing

Records management means controlling the processing of information and documents within an organisation's operating processes throughout their entire life cycle. Records management aims to improve the efficiency of records preparation, processing, decision-making, publication and archiving as well as the management of information in document form (documentary information).

Documentary information is part of an organisation's capital, and accordingly quality requirements pertaining to documentary information must be safeguarded, handling practices carefully planned and protection ensured. The quality requirements for documentary information include ensuring its authenticity, integrity, reliability and availability.

Information, on the other hand, means information that can be saved, processed or transferred in different forms. The information can be, for example, in a single document, speech, e-mail or text message, database, computer or mobile phone memory, audio or video recording, or even in the memory of a single person. The entire life cycle of the information must be considered, and accordingly significant processing stages from the perspective of information security include the creation of the information as well as its use, modification, saving, transfer, distribution, copying, archiving and destruction. When information is processed, due attention must be paid to the fact that the information being processed is often significantly more valuable than the technical device used to process the information.

2.1 Work-related information

- Ascertain the classification of the information or documents as well as the associated rules and restrictions relating to their use, disclosure and restrictions. (VAHTI 5/2006 Records Management Information Security Instructions, VAHTI 2/2000 Information Security Instructions for the Processing of Government Data, VAHTI 4/2002 Instructions for

Processing Sensitive International Data [These publications available in Finnish only]).

- If you prepare a confidential document, you are also responsible in accordance with your duties for its classification and labelling. Some confidential material is covered by the security classification.
- Handle information carefully, irrespective of the processing or storage medium.
- Remember that you may use and process confidential and sensitive information you receive only in carrying out your tasks. For example, using information in a personal data file contrary to its intended use is illegal. Remember also that use of information systems is monitored.
- When processing confidential information, make sure that no one else can see the information in your documents or on your computer display. Also take care when inputting passwords that no one can "see" a password from the movements of your fingers.
- Save the work you do as far as possible on a server from which the Information Management organisation makes back-up copies. Avoid situations in which a document or other material is only on a device or storage medium of which back-up copies are made only irregularly.
- If information is transferred using a memory stick or other information storage medium, always supervise the transfer personally. Take care to avoid situations in which other, unencrypted information is present on the storage medium in addition to the file to be transferred.
- Take care to remove concealed data (meta, residual and hidden data) in files made by office system applications (e.g. word processing, presentation graphics, spreadsheets), particularly when sending files outside your organisation or transferring information on a storage medium. Files may contain older data or other information from the system, even though it does not appear on the screen.
- Check with a virus protection program before use, according to organisation-specific instructions, any memory stick, CD/DVD disk or other storage medium brought from outside your organisation.
- If you have to send confidential information, send it in encrypted form. Make sure that the recipient is authorised to receive it and that the information reaches its destination. A telefax may be used to send confidential information only in exceptional circumstances. In such cases, make sure that the recipient is in place to receive it.
- Avoid unnecessary printing and copying, because extra copies, interim versions and inferior items (alongside the cost and environmental effects) increase the danger of information falling into the wrong hands and thus

also increase security tasks, particularly in terms of storage and destruction.

- Check which printer you are using and where it is located. Fetch your printouts from the network printer immediately after printing.
- When destroying confidential information, use shredders complying with the required protection classification or destruction service collection containers.

2.2 Interviews, enquiries, research and disclosure of information

- Direct all enquiries and requests for interviews to the person responsible for the records in question and act in accordance with the organisation's communication policy.
- Take care not to give out confidential information or information covered by the protection of privacy even in connection with conversations and forms that appear innocent enough.
- Forward requests for research and the disclosure of information to the person responsible for the information in question, whose task it is to confirm the justifications for the disclosure of information and to decide on its disclosure. If information is disclosed using a storage medium in electronic form, the storage medium used absolutely must be new and not one that has been used before.

2.3 Own information and privacy

- Use your private e-mail address (self-acquired, independent of the employer) for your personal communications.
- Your own personal files should not unnecessarily by saved on your workplace mobile phone, workstation or server.
- Everyone has the obligation to maintain secrecy about messages that they have inadvertently gained knowledge of in their tasks.
- Kill all gossip.
- Detailed log information on the use of systems as well as e-mail traffic and internet browsing is saved in the information systems and network. This information is used in maintenance, fault diagnostics and information security monitoring. Cases of misuse may be investigated. Consult the detailed organisation-specific instructions.

3 At the workplace

3.1 Use of computers

Computer use includes both use of your own workstation and of services accessed via a network.

- As the user, you are responsible for your own computer. So be careful.
- Only Information Management can install computing equipment on the network and install or update software on computers.
- Always log in to a computer with your own user ID and password.
- Prevent unauthorised access to information systems by always locking your workstation (on a Windows workstation press Ctrl+Alt+Del and select Lock Computer) when you leave the room. For extra security you can also use a password-protected screensaver. Act in accordance with organisation-specific instructions.
- While working, save your work frequently. Don't leave work unsaved when you leave your workstation.
- Save all important data on a network server disk from which the Information Management organisation regularly makes back-up copies.
- If a workstation hard drive or other storage medium, such as a memory stick or CD/DVD disk, breaks or is otherwise withdrawn from use, it must not be disposed of in a waste bin; ensure that it is destroyed in accordance with the organisation's instructions or send the storage medium to Information Management for destruction.
- At the end of the working day, log out of software and your computer and also switch off your computer in accordance with the organisation's instructions.

3.2 Access rights and passwords

Access rights are required for information systems. Your access right is personal and it is connected specifically to your identity and your job. Treat your user ID and password just as you would your own bank card and PIN code.

- Do not disclose your personal user IDs, passwords, smart cards or PIN codes to another person – not even to Information Management. Respond sceptically to all enquiries relating to your passwords or system access rights.
- Change your passwords sufficiently often and immediately when you suspect that they may have been disclosed.
- Ensure that passwords are sufficiently complex and avoid using familiar everyday words as passwords. A good password may have small and capital letters, numbers and even special characters. Not all systems accept special characters, however. A good password is easy to remember but difficult for another person to guess.
- Do not write passwords down – at least in a place where they can be easily found.
- Do not use a user ID or password given by your organisation when registering for internet services.
- If, in certain situations or systems, shared accounts have to be used, this will be decided by the system or information owner. The use of shared accounts is permitted only with the owner's permission. A shared account password must always be changed when some user's access right ends or it is suspected that someone not belonging to the group has gained knowledge of it. Passwords should in any case be changed sufficiently often.

3.3 Internet and e-mail

The internet and e-mail are good tools both for searching for information and for communication. You must remember, however, that e-mail or the internet have no protection in themselves; the information moves unencrypted on the public network. E-mail and the internet should be used with care.

- The internet and e-mail at the workplace are intended for official use only. Use your private e-mail address for your personal communications.
- Use only those services which you know to be appropriate.

- It is not permitted to send confidential information via the internet without appropriately strong encryption. Such messages and attachments must be encrypted using products approved by Information Management.
- Learn to use encryption products correctly, so that you do not inadvertently send information unencrypted.
- Downloading programs via the internet may be completely forbidden in your organisation. In such cases, Information Management will install all necessary programs. If, based on organisation-specific instructions and your tasks, you download programs, always try to confirm the reliability of the software and its source.
- If you use public terminals or temporarily a computer in the possession of another person, remember to empty the internet browser's cache and cookies. Ask Information Management for assistance, if necessary.
- Remember that an authority has an obligation to process official e-mail.
- Official e-mail can be processed only using hardware owned by one's own organisation or possibly by some other public administration organisation.
- Work-related e-mail is received and directed to the e-mail system of one's own organisation. It must not be directed or forwarded outside the organisation's e-mail system.
- Instruct customers conducting business electronically to send matters for consideration to the e-mail address specified by the organisation.
- Remember that you are responsible, in accordance with your official duties, for any work-related e-mail that may be sent to your personal e-mail.
- The use of e-mail other than official e-mail (for example free internet e-mail programs or your home e-mail) is permitted only with your own organisation's consent.
- Make sure that obligations relating to the processing of your e-mail in accordance with your official duties are fulfilled also during your absence.
- E-mail attachments may contain malware (virus, worms or Trojan horses). Regard all atypical e-mail messages, particularly attachments, with suspicion. Do not open suspect messages; act only in accordance with instructions. If necessary, contact Information Management.
- Junk mail may include unsolicited advertisements that arrive in your e-mail. Junk mail should not be answered; it should be destroyed immediately. If you answer an e-mail message, the sender will know that your e-mail address is valid and will continue sending junk mail and, moreover, forward your address to other senders of junk mail.

- Do not give your work e-mail address to third parties other than in work-related contexts.
- Apply a healthy suspicious about the reliability of e-mail. An e-mail message may also come from somewhere other than the party shown in the sender field. Viruses can also send e-mail without the user taking any action. Beware "phishing messages" that ask you to input user IDs and passwords for services that look authentic.
- Do not forward chain letters.
- If you receive an e-mail message belonging to someone else, direct the message to the correct recipient and inform the sender of the recipient's correct e-mail address. If you do not know the correct address, notify the sender of the incorrect transmission. Remember that you have a duty to keep confidential any message you receive.
- A distribution list is a list of people disclosed to every recipient and it may be personal data information or confidential information governed by specific provisions on disclosure. You can use the e-mail hidden copy function if you wish to prevent the addresses on a distribution list being seen by the recipients.
- Take care to ensure that any e-mail message you send is directed to the correct people and the correct addresses, also when you are using prepared distribution lists. Avoid sending unnecessary e-mail messages. Sending Christmas greetings, for example, loads both the e-mail system and the recipient's e-mail box.
- When an employment relationship ends, the corresponding e-mail address and e-mail box are deleted. Make your official mail available to your employer and delete any personal messages.

3.4 Security of premises

Security of premises ensures that information, documents and computing equipment are kept and handled appropriately and securely. Security of premises includes, among other things, access control, technical surveillance and guarding, prevention of fire, water, electrical, ventilation and break-in damage as well as security of courier services and dispatches containing information.

- At a customer-service point or other customer-service situation orient your computer display with discretion – should the display information be visible to the customer or not?

- Comply with access control instructions. Use and display your photo ID card (if such is supplied) on the organisation's premises.
- When arriving at your workstation, check that nothing inappropriate has happened during your absence.
- Every visitor must be accompanied by a chaperone. The chaperone is responsible for the visitor's conduct and movements on the premises.
- Try to use meeting rooms for visits.
- Take care that no irrelevant material is displayed in meeting rooms. Correspondingly, when your meeting is completed, ensure that no confidential material or notes remain on tables, boards, waste bins or elsewhere.
- Keep information and equipment safe, as far as possible in a locked cabinet and room.
- Never leave a laptop computer or mobile phone unsupervised. Keep equipment in a locked room. Also ensure that memory sticks, CD/DVD disks and paper printouts etc. are appropriately stored.
- Adhere to the 'clean desk' principle. Do not keep confidential information on your desk.
- Do not leave a visitor alone or without supervision in your office or other premises.
- Photography may be prohibited on an organisation's premises – comply with organisation-specific instructions. Be aware of your visitors' actions, for example their use of camera-equipped mobile phones.
- Lock your office door at the end of the working day or when you will be away from your workstation for extended periods.
- Direct visitors or people who have "lost their way" to their correct destinations. Do not let unauthorised people into premises e.g. when you are leaving work.
- Do not leave access control doors, or doors otherwise intended to be kept closed, open.

4 Mobile work, telework and working when travelling

4.1 Mobile work and mobile devices

Many mobile work devices may be similar in terms of features and content to the workstations used in the workplace. Such devices are no longer mere telephones. Threats similar to those affecting more permanent, installed equipment are associated with mobile work equipment and its use, so the same security instructions, where applicable, are involved. Special care should be taken, moreover, when equipment is taken and used outside the security measures offered by workplace premises.

- Attend to the security of laptop computers, mobile phones, communicators and PDAs used by you in your work. Do not store more information on them than is absolutely necessary.
- Familiarise yourself with the user instructions and security features of equipment and its software (e.g. PIN requests, Bluetooth settings, application downloading).
- Ensure that your mobile phone is protected by the PIN request feature. Change the PIN codes provided by the equipment manufacturer or service provider.
- Do not download and install on your equipment anything unrelated to work.
- Use data encryption as far as possible.
- Attend to back-up copying and/or, if necessary, synchronisation of data with other information systems in accordance with organisation-specific instructions.

4.2 Telework and remote access

Telework means work performed elsewhere than in the organisation's permanent operating location. Typical telework is office work done from home. Telework may also be done from some other permanent location (e.g. a teleworking point arranged by an organisation) or when travelling (e.g. hotel or another organisation's premises), in which case the operating environment will vary and it may not be possible to influence the security of the environment. The teleworker's own measures and procedures will, accordingly, be highly significant. A remote connection is a communications link from outside an organisation's internal network, and remote access is the use of information technology services using a remote connection. As wireless network connections become commonplace, the teleworker must increasingly be able to make independent assessments of teleworking environment security.

- Observe secure procedures in everything you do. This is particularly important when operating outside permanent office premises. In telework you should, where applicable, adhere to all of the same security principles as if you were in the organisation's usual premises.
- Telework is permitted only on the basis of a separate agreement to do so. Check the organisation-specific instructions on telework .
- Remember that all of the work done in an organisation cannot be done securely as telework. Identify this type of work. Remote access to some systems may be prohibited or blocked.
- As a rule, the employer will arrange the acquisition and installation of the equipment, software and communications links required for remote access.
- Ensure that the hardware, software, communication links and paper material used by you are, and can be, used only by you.
- Ensure that user IDs, passwords, any smart cards and other authentication tools used by you are in your possession only and known only to you.
- Use agreed encryption programs and check that they are up to date.
- Carry with you only the amount of information material that is absolutely necessary and always ensure that the information is appropriately protected.
- When handling documents, adhere to the same principles as normal, taking the special risks of telework into account. Telework should be restricted to material whose disclosure will not jeopardise information security. In telework, you must take into account the classification of material and the rules relating to its use as well as restrictions on its disclosure, use and handling.

- Attend to the back-up copying of your information material as well as its secure storage and destruction procedure.

4.3 On a home computer

If you have a home computer and an internet connection, it is also important to attend to their information security.

- Now and then, ask a reliable information technology expert to check that your workstation environment is secure.
- For every user of the computer, make personal user IDs and passwords, which only have normal user's rights.
- Use the administrator ID and password for maintenance tasks only.
- Install only official, up-to-date software.
- Ensure that your operating system and other system software are automatically updated.
- Use a well-known information program package with a good reputation (incl. e.g. virus protection, firewall, spyware protection, junk mail filer) and ensure that is automatically updated.
- Do not open suspicious e-mail messages and attachments.
- Make regular back-up copies and practise using them.
- When you register for internet services and make purchases, for example, use only reliable services and suppliers. Do not give more personal information than is necessary – do not give any information at all relating to your employer.
- Switch off your computer and close your internet connection when you are not using them.

4.4 Working when travelling

- Avoid speaking about confidential work matters in public places and on means of transport.
- If you are working on a public means of transport, ensure that your fellow passengers cannot view the information and documents you are working with. Take care not to activate unnecessary wireless connections on your computer.

- Keep your information and equipment safe. Never leave a laptop computer or mobile phone unsupervised. Keep equipment under lock and key. Remember to store data media, paper print-outs etc. appropriately. Laptop computers and mobile phones should not be left in vehicles in a visible place, nor should they be kept in vehicles overnight.
- Avoid using public terminals (e.g. net cafés, libraries) for work matters. In such places you cannot influence what information is being collected about you or what will be done with this information. Generally, moreover, you are not offered the opportunity to delete this information from the device.

5 Problem situations

5.1 Duty to notify and how to act in problem situations

- If a device, access card, identifier etc. disappears or is stolen, notify the person responsible for this field immediately in order to limit your own responsibility.
- Always report malware (e.g. viruses, worms or Trojans) and other information security problems immediately to the person responsible for information security, the Information Management organisation or your own supervisor.
- In addition, also report other security suspicions, protection shortcomings or problems to those responsible for security or your own supervisor.

5.2 If you suspect an information security breach or malware infection…

- Don't panic.
- You don't need to close your computer, but disconnect the local area network cable from your workstation.
- Write down the contents of any report or warning. Make a note of your actions and record any lost working time for a possible compensation claim.
- Contact Information Management and/or the person responsible for information security. Assist the investigation. Report what you were doing when the computer began to function in an unexpected way. Act according to the instructions you receive.

5.3 Consequences

- The violation of laws, regulations and instructions may result in access rights to information systems being revoked. Supervisors are always informed of any violations.

- In serious cases, misuse may also lead to a claim for damages and criminal proceedings. Another possible consequences may be dismissal and the termination of your employment relationship.

6 Further information

Further information on information security can be obtained from the following sources:

- Head of Information Security, Information Management, Head of Security and your supervisor
- Your organisation's own information security instructions
- Legislation – FINLEX, the government legislation database (www.finlex.fi)
- Organisations issuing instructions and provisions on information security, for example
    - The Ministry of Finance VAHTI instructions (*www.vm.fi/vahti*)
    - The National Archive Service (*www.narc.fi*)
    - The Data Protection Ombudsman (*www.tietosuoja.fi*)
    - The Finnish Information Society Development Centre (*www.tieke.fi*)
    - The Finnish Communications Regulatory Authority (*www.ficora.fi*)
    - The Information Security Guide for the public administration and business (www.tietoturvaopas.fi)

Appendix 1: Key statutes relating to information security

In addition to the confidentiality provisions contained in various acts, the most important acts are as follows (majority available in Finnish):

- The Finnish Constitution (731/1999), Chapter 2 Section 10: Protection of privacy and secrecy of confidential correspondence
- The Finnish Constitution (731/1999), Chapter 2 Section 12: Public accessibility of documents and records in the possession of authorities
- The Act on the Openness of Government Activities (621/1999)
- The Decree on the Openness of Government Activities and on Good Practice in Information (1030/1999)
- The State Civil Servants Act (750/1994), Section 17: Statute on the state public service relationship
- The Act on Municipal Civil Servants (304/2003)
- The Employment Contracts Act (55/2001)
- The Government resolution on state administration information security (VM0024:00/02/99/1998)
- The Archives Act (831/1994): Drafting, storage and use of documents
- The Act on International Security Obligations (588/2004): Sensitive international documents
- The Personal Data Act (523/1999): General principles relating to the processing of personal data
- The Act on Background Checks (177/2002)
- The Act on the Protection of Privacy in Working Life (759/2004): Processing of personal data on employees
- The Act on Electronic Services and Communication in the Public Sector (13/2003) Information security in electronic services and transfer of information between authorities
- The Act on Electronic Signatures (14/2003)
- The Act on the Protection of Privacy in Electronic Communications (516/2004) Confidentiality of electronic communications and protection of privacy
- The Penal Code (39/1889) Chapter 34 Section 9a: Causing harm to data processing

- The Penal Code (39/1889) Chapter 38 Section 8: Data trespass, hacking
- The Penal Code (39/1889) Chapter 38 Section 9 Paragraph 1: Personal data offence
- The Personal Data Act (523/1999) Section 48: Personal data file violation
- The Tort Liability Act (41/1974)

Up-to-date statute texts can be found on FINLEX, the government legislation database (*www.finlex.fi*).

Appendix 2: Valid VAHTI publications

VAHTI 4/2009	Information Security Instructions for Personnel
VAHTI 3/2009	Logging instructions *
VAHTI 2/2009	General instructions on ICT contingency planning *
VAHTI 1/2009	VAHTI annual report 2008 *
VAHTI 9/2008	General instructions on information security in projects *
VAHTI 8/2008	Information security terms *
VAHTI 7/2008	Informationssäkerhetsanvisningar för personalen **
VAHTI 6/2008	Report by IS training in the central government *
VAHTI 5/2008	24/7 information security services in the central government *
VAHTI 4/2008	General instructions on information security auditing in the central government *
VAHTI 3/2008	Encryption technologies in the central government *
VAHTI 2/2008	Personnel security as a part of information security *
VAHTI 1/2008	VAHTI annual report 2007 *
VAHTI 3/2007	Summary of general instructions on information security management *
VAHTI 2/2007	Information security in modern mobile phones *
VAHTI 1/2007	Challenges in international information security work *
VAHTI 12/2006	Electronic identification in the central government services *
VAHTI 11/2006	Instructions for information security trainers *
VAHTI 10/2006	Security instructions for the personnel *
VAHTI 9/2006	Best practises in access control and management *
VAHTI 8/2006	Assessment of information security in the central government *
VAHTI 7/2006	Change and information security, from regionalisation to outsourcing – a controlled process *
VAHTI 6/2006	Setting and measuring information security targets *
VAHTI 5/2006	Records management information security instructions *
VAHTI 4/2006	Review of the arrangement of round-the-clock information security in the central government *
VAHTI 3/2006	Review of the distribution of central government information security resources *
VAHTI 2/2006	Electronic-Mail Handling Instruction for State Government
VAHTI 1/2006	VAHTI annual report 2005 *

VAHTI 3/2005	Management of information security anomalies *
VAHTI 2/2005	Electronic mail handling instructions for central government *
VAHTI 1/2005	Information Security and Management by Results
VAHTI 5/2004	Securing the state administration's key information systems *
VAHTI 4/2004	Datasäkerhet och resultatstyrning **
VAHTI 3/2004	General instructions on protection against malware *
VAHTI 2/2004	Information Security and Management by Results
VAHTI 1/2004	Government Information Security Development Program 2004-2006
VAHTI 7/2003	Risk assessment instruction to promote government information security *
VAHTI 3/2003	Assessment of information security management systems *
VAHTI 2/2003	Secure remote access from insecure networks *
VAHTI 1/2003	Secure use of the Internet *
VAHTI 4/2002	Instructions for processing sensitive international data *
VAHTI 3/2002	Information security instructions for telework *
VAHTI 1/2002	Information security recommendation for ICT rooms *
VAHTI 6/2001	Information security checklist for ICT procurement *
VAHTI 4/2001	General instructions on the information security of electronic services *
VAHTI 2/2001	Information security recommendation on government local area networks *
VAHTI 3/2000	General recommendation on information system development *
VAHTI 2/2000	Information security instructions for processing government data material (revised) *

* (only available in Finnish)
** (Swedish publication)

Revised and supplementary instructions can be found on the VAHTI website (www.vm.fi/vahti) and instructions can also be ordered from the printing house Edita.

MINISTRY OF FINANCE
Snellmaninkatu 1 A
P.O. BOX 28, 00023 GOVERNMENT
Tel. (09) 160 01
Fax (09) 160 33123
www.vm.fi

4/2009
VAHTI
June 2009

ISSN 1455-2566 (print)
ISBN 978- 951-804-979-4 (print)
ISSN 1798-0860 (pdf)
ISBN 978-951-804-980-0 (pdf)