THE FINNISH PARLIAMENT´S INFORMATION SECURITY AND E-MAIL INSTRUCTIONS

PUBLICATION BY THE PARLIAMENTARY OFFICE 8/2005

THE FINNISH PARLIAMENT'S INFORMATION SECURITY AND E-MAIL INSTRUCTIONS

PUBLICATION 8/2005 BY THE PARLIAMENTARY OFFICE

ISBN 951-53-2714-8 (vol.)
ISBN 951-53-2715-6 (PDF)
ISSN 1239-1638

TO THE READER

The information security instructions begin by stating that, for the most part, Parliamentary work consist of information handling, and that Parliament is extremely dependent on information and on information technology. In future, this dependence will continue to increase, with information technology becoming more comprehensively integrated with Parliamentary work processes. Information security is included in everyone's daily work.

Information must be secured. This information security instruction provides instructions on how to protect information, systems, services and telecommunications. In addition to basic principles and legislative questions, the instruction also contains procedural instructions relating to information handling.

A corresponding instruction has been prepared for the use of e-mail. E-mail constitutes a very significant means of communication at present. However, shared rules of adequate accuracy concerning the use of e-mail have not been provided. In addition to mentioning the legislation concerning the use of e-mail, the instruction also contains practical advice and regulations for people's daily work.

It is advisable, and in the interest of everyone engaged in Parliamentary work, to become acquainted with both of these instructions.

Olli Mustajärvi, Head of IT Office

TABLE OF CONTENTS

THE FINNISH PARLIAMENT'S INFORMATION SECURITY INSTRUCTIONS

Approved by the Chancellery Commission 11th November 2004

PUBLICATION 8/2005 BY THE PARLIAMENTARY OFFICE

SUMMARY

Advisable to know and remember!

- ü All information users are personally responsible for information security.
- ü Information security is also a means of ensuring that public information is correct, up-to-date and available.
- ü Never give away your username and password.
- ü Never write your password down.
- ü Never use a password that is easy to guess, such as your spouse's or child's name.
- ü Always save any important information in your home directory on the H disk drive.
- ü Avoid unnecessary paper copies.
- ü Internet-provided information is not always correct – always ensure the correctness of information.
- ü Internet-provided information may be copyrighted – ensure that it is legal to use the information in question.
- ü Whenever users access a site on the Internet, they invariably generate an entry in the page log files.
- ü There is a separate instruction concerning the handling of e-mail, in addition to which, any other pertinent special instructions must be considered when handling information.

PREFACE

On 22nd April 2004, Parliament’s Administrative Director appointed a team to draw up a proposal for the Parliament’s information security instruction. The team invited Jarmo Vuorinen, Parliament’s Deputy Secretary General, to chair the team, with Committee Counsellor Kaisa Vuorisalo, Committee Counsellor Risto Eerola, Information Systems Manager Juha Suomalainen and ADP Manager Kari T. Sipilä acting as the members. Mr Sipilä was employed by Parliament until the end of May, and has subsequently participated in the team’s work. Mr Eerola and Mr Sipilä have served as the team secretaries. The team was assigned to produce its proposal by 30th June 2004.

To carry out its assignment, the team has examined information security issues both from the legislative work point of view and that of Parliamentary administration activities. On the one hand, this examination has focused on information systems management needs, and on the demands caused by the currently valid legislation, on the other.

When carrying out its assignment, the team has paid attention to the fact that applying the publicity legislation to the activities pursued by the Parliament’s Chancellery Commission is currently not based on a specific stipulation. Instead, it relies on the justifying reasons mentioned in the government proposal which led to the passing of the fundamental law in question. Consequently, the team’s opinion is that the current judicial status cannot be considered satisfactory. In addition to this, the team proposes that it should be considered whether Parliament’s communication activities require separate instructions, to supplement the instruction being proposed in this document.

The team that produced the Parliament’s information security instruction submitted its proposal to the Director-General for Administrative Affairs on 29th June 2004. Following this, the team has processed the statements and comments received and changed its proposal as necessary. However, it has not been possible to take all of the presented viewpoints into account. This is due to the fact that the basic norms and principles concerning the publicity of parliamentary activities and documents deviate, to a certain extent, from those applied to the Government and the public administration under it.

The team also states that Parliament should consider the drawing up of a separate instruction concerning good governance.

Helsinki, Finland, 5th November 2004

On the Team's behalf

Jarmo Vuorinen
Chairman

INTRODUCTION

For the most part, Parliamentary work consists of information handling. This means that Parliament is extremely dependent on information and information technology. It can be estimated that this dependence will continue to increase in the future. Information society development will continue to increase the amount of information to be dealt with. The central information security objective is to ensure disturbance-free information handling and information management at all times, and their uninterrupted operation under all circumstances.

Most of the information processed by Parliament is public by nature. Nevertheless, public information must also be secured. It is essential to guarantee that information is correct, up-to-date and available. Information security is the means of securing the good quality and applicability of information.

Regarding the handling of matters and the publicity of documents, Parliament is partly governed by regulations which differ from those applied to the Government and the public administration under it. This also means that public administration instructions cannot be applied to Parliament as such. Instead, it has been necessary to prepare a separate instruction for Parliamentary activities.

This instruction, its 3rd and 4th section in particular, confirms the procedures to abide by, on duty, when handling received information, documents and other recordings, irrespective of their technical presentation. This instruction concerns all Members of Parliament and their assistants, Parliamentary civil servants, Parliament employees, and any other people who work under Parliament and use Parliament’s information systems. This instruction includes six appendices. There is a separate instruction regarding the use of e-mail in Parliament.

1 INFORMATION SECURITY

1.1 Information security concept

Information security refers to the protection of information, systems, services and telecommunications through administrative and technical arrangements and personal measures taken by each individual user. Information is secured against threats that are caused by intentional, consequential, negligent and blameless action.

In this instruction, information refers to information that is handled, processed, recorded, transferred or transmitted in various ways. Information typically exists in the form of a document but voice and image recordings, databases and similar media are also covered by this instruction.

Information security is a must in all information handling phases, including its creation, use, editing, modifying, recording, transfer, transmission, distribution, copying, archiving and disposal.

Information security applies to both public and secret information. The purpose of information security is to guarantee the correctness and availability of information. From the Parliamentary point of view, the correctness and availability of information are crucial aspects, since Parliament deals with information that is largely dependent on legislation. Combined with the correctness and availability of information, the application of appropriate information security also guarantees the implementation of confidentiality and secrecy as necessary.

In this instruction, information security is considered to include the following basic aspects:

- Availability
- Integrity
- Verification
- Non-repudiation
- Confidentiality

Availability

Availability means that those who need the required information, and are entitled to it, can access it at all times, even under exceptional circumstances if necessary. Furthermore, it must be guaranteed that information will not be deleted due to any external operation. It is

important that all citizens have the opportunity to access and use public information if they so desire.

Integrity

Integrity means that the information content is always correct and up-to-date, and that it is protected against any irrelevant changes. The integrity requirement is central in the Parliamentary environment.

Verification and indisputableness

Verification means that it is possible to identify any party that produces or uses information, if necessary.

Indisputableness means that it is possible to prove, even afterwards as necessary, who has used or changed the information in question. This also applies to public information.

Confidentiality

Confidentiality means that the information in question is only at the disposal of those who are entitled to it. With regards to public information, confidentiality means that information is at everyone’s disposal if necessary.

1.2 Information ownership

The information ownership concept is essentially related to information security. Typically, information is owned by its producer or the producing organisation. The owner is responsible for the information in question, and makes any decisions concerning its use and exploitation. The information owner also defines the information handling category. No other party has the right to change this definition (however, see sections 2.2.2 and 3.4.). The definition typically involves information confidentiality but also other basic safety aspects as necessary. It is advisable to remember that each person is the owner of his or her own personal information and is ultimately responsible for it.

The information security procedures to be followed are based on valid regulations, this instruction and other internal instructions.

In addition to automatic data processing, information security includes other data processing and information handling methods, plus the security of office facilities. The office facilities’ security means that the facilities are kept in the appropriate condition to meet the information storage and usage requirements. In particular, this applies to information archives, computer rooms and data communication cross-connection facilities. The entire information security ultimately depends on the security of office facilities. These two support each other and must be of an adequate standard and mutually compatible.

1.3 Information security threats

A central threat to information security is the unauthorised use of information. Unauthorised use refers to a situation in which an unauthorised person gains access to information, or where an authorised person uses information in an unauthorised manner.

Careless protection of information or the wrong information security classification increases the risk of unauthorised use. It is especially important to protect information if the information is conveyed through or presented on the Internet. On the Internet, information may be exposed to unauthorised use, without the possibility of knowing who has abused it. This applies to Internet sites in particular. A typical threat caused by the Internet is the unauthorised changing of information.

The losing of a data medium (such as printouts, CDs, diskettes, memory cards) or a data processing device (such as portable devices or palmtop computers, mobile phones) always causes a threat to the information contained in them. The lost data medium or device can fall into the hands of those who could abuse their information content. However, it must be remembered that losing data media invariably means losing their information content, either for a limited period or permanently. In general, the information that has been recorded by the data medium or data processing device is significantly more valuable than the medium or device itself.

A stolen data medium or data processing device invariably causes a significant information security risk. In cases where the device value is the only motive for the theft committed, the loss the information contained is highly probable. Should a theft be committed because of the information, its abuse is extremely probable.

Information can also be changed or deleted indirectly. In this case, the various computer viruses are a central threat. As such, viruses may wreck havoc, or they can render the information system accessible to unauthorised use. The use of the Internet imposes a major risk for virus infections but viruses are also propagated through the data media and e-mail.

2 INFORMATION PUBLICITY AND SECRECY

2.1 Legislative work

2.1.1 Plenary sessions

The Parliament’s activities are governed by *section 50 of the Constitution of Finland.* According to it, *the Parliament’s plenary sessions* are open to the public unless the Parliament for a very weighty reason decides otherwise for a given matter. Parliament can also decide on the publicity of closed plenary session documents if necessary. The plenary session records and final protocols are governed by sections 69 and 70 of the Parliament’s standing orders. A record becomes public once it is undersigned by the Parliament’s General Secretary and checked by the Speakers. A final protocol, in turn, becomes public once it is undersigned by the Parliament’s General Secretary. The publication of Parliamentary documents is governed by section 71 of the Parliament’s standing orders.

2.1.2 Publicity of Committee meetings and matters dealt with

The meetings of Committees are not open to the public as a rule. However, a Committee may open its meeting to the public during the time when it is gathering information for the preparation of a matter. These regulations apply both to the Committee which deals with the preparing of a matter and to any Committee giving a statement. *A matter* becomes public in the Committee in question when its handling is concluded there, unless otherwise prescribed by the confidentiality decision concerning the matter, for example. According to subsection 3 of the Constitution’s section 50, the members of a Committee shall observe the level of confidentiality considered necessary by the Committee for a compelling reason. When considering matters relating to Finland’s international relations or European Union affairs, however, the members of a Committee shall observe the level of confidentiality considered necessary by the Grand Committee or the Foreign Affairs Committee after having heard the opinion of the Government.

2.1.3 Publicity and secrecy of documents

The publicity of Committee documents is governed by the Parliament’s standing orders. Minutes shall be drawn up of each Committee meeting, with the members present and any experts heard mentioned, in addition to any proposals and decisions made with their voting results. The minutes of a Committee meeting become public when confirmed by the secretary through his or her signature. The handling documents of a matter, that is those prepared and received by a Committee for handling the matter, such as any expert statements in writing, become public once the Committee has concluded the handling of the matter in question. Any Parliamentary group that is not represented in a Committee or a subcommittee thereof is entitled to

receive a copy of any document pertaining to a matter being processed, provided that these are not secret.

The grounds for the secrecy of documents are governed by the Parliament’s standing orders. A document is to be kept secret in cases where:

- releasing information on it would cause significant damage to Finland’s international relations or capital and financial markets, or if
- the document contains information about a business secret, a trade secret, a person’s health or his or her economic status.

The last-mentioned grounds for secrecy involve a so-called conditional damage clause, according to which secrecy shall only be applied in cases where releasing information about a document would cause a significant impediment or damage. Nevertheless, an impediment or damage of this type can be disregarded, provided that there is a considerable societal need for the document to be public.

For reasons comparable to the above, a Committee may also decide a document to be secret. Because of the public nature of Parliamentary work, this type of concealment, which is based on a single decision, can be only secondary and exceptional, however.

Documents that are to be kept confidential in accordance with section 50, subsection 3, of the Constitution, form a separate group of their own.

As for Committee documents’ *secrecy duration*, the stipulations set out in the Act on the Openness of Government Activities are to be abided by as applicable. As a rule, the secrecy period is 25 years, unless otherwise ruled or prescribed. However, a Committee can also decide that the secrecy period be shorter. In accordance with the Act on the Openness of Government Activities, the secrecy period may be extended, in cases where a document’s becoming public would significantly impede those benefits that are originally protected by the statutory secrecy liability.

Committee civil servants engaged in legislative work are governed by Committee regulations on publicity, secrecy and confidentiality of documents and document-contained information.

According to the justifications mentioned in the constitution proposal, other Parliamentary organs shall follow Committee regulations in their activities as applicable. This also applies to the Speakers’ Council, for example.

2.2 Administration activities

2.2.1 The public sector

According to the Act on the Openness of Government Activities, any offices operating under Parliament, that is the Parliamentary Office, the Office of the Parliamentary State Auditors, the Ombudsman's Office, and the State Audit Office, are all regarded as *authorities*. This means that Parliamentary administration follows, as applicable, the same publicity regulations as in the nation's Government in general. Even though the Act on the Openness of Government Activities cannot be directly applied to the activities pursued by the Parliament's Chancellery Commission, it has been considered, in the justifications for the constitution proposal, that the Commission shall be governed, as applicable, by the same publicity principles as public administration in general.

For example, Parliamentary administration is governed by the general regulations set out in the Act on the Openness of Government Activities on documents becoming public, on people's right to obtain information about authorities' public documents, the authorities' secrecy and confidentiality obligations, and their obligation to promote the implementation of the said law's purpose in practice.

The Act on the Openness of Government Activities refers to *authorities' documents* that are seen as documents in the possession of authorities, which have been drawn up by authorities or their employees, or which have been delivered to authorities for the handling of a matter, or otherwise in connection of a matter belonging to their line of activities or tasks. The Act on the Openness of Government Activities also covers the use of outsourced services. Consequently, the following are also regarded as documents drawn up by authorities: any assignment-based documents produced for and submitted to authorities. A document submitted to authorities is one that is handed over to an authority due to an assignment, or delivered otherwise to an authority-assigned party for the performance of their duties.

Documents that have been drawn up for the authorities' internal operations, *are not, as a rule, considered to be authorities' documents*, which are referred to in the Act on the Openness of Government Activities. These documents are only covered by the law in question in cases where they contain the type of information that must be archived in accordance with the Archives Act.

Furthermore, any notes and memorandums made by authorities' employees or by people working on authorities' assignments, which have not been submitted by them for presentation or other handling of a matter, *shall not be regarded* as authorities' documents in accordance with the Act on the Openness of Government Activities. This means that a document is not governed by the Act on the Openness of Government Activities before a civil servant has considered the document to be complete and has

submitted it to a party who decides upon the matter or processes it otherwise. As such, a transfer of this type does not mean that the document will be presented to a superior or another party for guidance or comments.

See section 6 of the Act on the Openness of Government Activities for *the time of publishing for documents drawn up by authorities.* However, this regulation is only secondary when compared to the secrecy regulations. In other words, a document will become public *only in so far as it is not to be kept secret in accordance with the regulations below*. For the most common document types, the publishing times are as follows:

- Any entry made to a public record or a public list will become public once it is made.
- Any invitations to tender, reports, clarification requests, statement requests, proposals, suggestions, initiatives and applications with their appendices, which are made by authorities, will become public once they have been undersigned or verified in a similar fashion. However, any requests to supplement a submitted quotation, plus any reports drawn up to clarify a quotation document, for example, will not become public before the agreement in question has been entered into.
- Research reports and statistics produced by authorities, and any other comparable reports that constitute a solution or a plan of general importance, or a description of their alternatives, justifications or subsequent effects, including matters that are otherwise unfinished, will become public once they are ready for their intended application.
- Minutes of authorities' meetings will become public once they are inspected and undersigned, or verified in a similar fashion, provided that they have not been drawn up in order to prepare a specific matter (such as Commission meeting records).
- As a rule, any decisions, statements, and documents made by authorities in the capacity of a contracting party to resolve a matter, plus any documents drawn up by authorities for the processing thereof, will become public once they have been undersigned or otherwise verified in a similar fashion.

Contrary to the above, any Committee reports, clarifications and any other similar documents that are intended for public distribution will become public once they are in the possession of authorities for distribution, in other words, in a printed or otherwise duplicated form.

As a rule, any document that has been *submitted to an authority* to process a matter or any other matter belonging to its jurisdiction or responsibility will become public once the authority in question has received it. Travel declaration forms submitted by authorities' employees, and job application documents, are examples of such documents. Documents of this type can also contain sections that are to be kept secret. In addition, section 7 of the

Act on the Openness of Government Activities contains special regulations on the publicity of competitive biddings.

2.2.2 Secrecy

Secrecy entails two separate dimensions: the obligation to keep a document secret, and professional secrecy concerning the information which is to be kept secret.

The document secrecy obligation prohibits anyone from disclosing a secret document or a copy thereof. The grounds, according to which authorities' documents must be kept secret, are set out in section 24 of the Act on the Openness of Government Activities.

The professional secrecy obligation applies to civil servants. It prohibits anyone from disclosing secret information, regardless of whether the information has been recorded or not. Information governed by professional secrecy can be derived from a document or obtained orally. This means that the scope of application of professional secrecy is wider than that of document secrecy.

According to the Act on the Openness of Government Activities, authorities' employees are not allowed to disclose the secret content of any document, nor any information which should be kept secret in cases where it is recorded in a document. The same applies to any information that comes to their knowledge when employed by authorities, the secrecy of which has been prescribed by the law. The law specifically stipulates that any information covered by professional secrecy shall not be disclosed by people employed by authorities, and that the secrecy obligation extends to the individuals' post-employment and post-assignment periods. Consequently, professional secrecy is not determined by the employment duration in question.

Professional secrecy is not restricted to permanent appointments but applies to all employments. According to the Act on the Openness of Government Activities, professional secrecy also applies to all trainees and any other people actually working for the authority in question.

Assignment relations, purchased service agreements, among others, also constitute grounds to extend professional secrecy to people acting outside the sphere of authorities.

In these cases, professional secrecy applies to secret information that the authority has given to the contractor in question. On the same grounds, professional secrecy applies to the contractor's employees.

Professional secrecy also entails *prohibition of utilisation.* Prohibition of utilisation means that a person bound by professional secrecy must not use secret information for his or her own benefit, or to anyone else's disadvantage. This prohibition will extend to the person's post-employment or post-assignment period.

According to section 25 of the Act on the Openness of Government Activities, a document must be invariably provided with a *secrecy marking*, in cases where it is handed over to the party in question, provided that it is to be kept secret due to the benefit of another party or public interest. A secrecy marking can also be made on other documents which are kept secret. The marking is to indicate which sections of the document are secret, and what the secrecy in question is based on. However, in cases where secrecy is based on a stipulation including a so-called conditional damage clause, the marking may be made so as to only indicate the regulation forming the basis for the secrecy in question. Nevertheless, secrecy markings have *no independent legal effects of their own.* This means that information requests cannot be denied for the mere fact that the document in question has been marked as secret. *Concealment must be resolved separately in each individual case, in compliance with the Act on the Openness of Government Activities.*

According to the Act on the Openness of Government Activities, information may be provided concerning a secret official document, or its content, on the grounds prescribed by the law in question. Should only a part of the document be kept secret, information provision must be restricted to the public section of the document, without releasing any secret information.

Consequently, releasing information concerning a document that is to be kept secret is an exception which needs to be legally justified. According to section 26 of the Act on the Openness of Government Activities, special statutory stipulations and consent given by a party that is originally protected by the statutory secrecy obligation, constitute *general grounds for exceptions* of this type. Furthermore, information may be provided about a business secret or a trade secret, for example concerning the financial status of another party. This is based on section 24, paragraph 1, subparagraph 32 of the Act on the Openness of Government Activities and may be done in cases where the information in question is required to implement another authority's statutory information obligation regarding a person's private life, or to execute an authority's statutory compensation or any other claim. An authority may also release secret information, for example, concerning any tasks or assignments being carried out on its account, provided that this is necessary so as to perform the task or assignment in question.

In addition, the Act on the Openness of Government Activities separately prescribes on providing *another authority* with secret information, and about providing *a foreign authority or an international organ* with such information.

Moreover, it is to be noted that *a party involved*, for example an applicant, shall have the right to receive information on the content of a document, from an authority that is handling or has handled his or her case. This right also extends to other than public documents, provided that the document content in question may affect or may have affected the handling of his case. However, the Act on the Openness of Government Activities prescribes several exceptions to this primary rule.

3 HANDLING OF INFORMATION MATERIALS

3.1 Basic norms for handling

The regulations concerning the handling of information materials by the Parliament is mainly based on its standing orders concerning legislative work, and on the Act on the Openness of Government Activities regarding administration activities. In addition to this, there is a number of special regulations valid pertaining to the handling of information materials of specific types. In particular, such regulations are included *in the Personal Data Act* (523/1999). Chapter 2 of this Act sets out the general principles concerning the handling of personal data, and chapter 3 of the regulations concerning the handling of sensitive data and personal identity numbers.

According to the *Act on the Protection of Privacy in Electric Communications* (516/2004), any identification information and geographic location information that is generated in conjunction with telephone calls and e-mail messages, for example, shall primarily be regarded as confidential. This means that they are protected by professional secrecy and the prohibition of utilisation. Chapters 3 and 4 of the said Act contain separate regulations concerning the handling of information of this type. The Act on the Protection of Privacy in Electric Communications also contains regulations as to when and how a community subscriber, such as the Parliament, has the right to intervene in communication between individuals within the subscriber-owned communication networks, in order to maintain information security.

In addition to the statutory handling rules, document processing may be regulated through *information materials' handling classifications*. A handling classification is connected to the promotion of good administration practice, and cannot, as such, constitute a secrecy obligation or any impediment to publicity. However, the classification must be taken into consideration when documents are processed, stored and disposed of.

3.2 Parliamentary handling classification for documents

All the information and documents that are processed by the Parliament *are classified* by their content as follows:

- Public,
- For internal use,
- Secret.

If a document is not public, it must be provided with a classification marking. This means that public documents are not classified as per handling category. When processing *recordings meant for internal use,* the

number of which is high, and for which the classification practice has been established and is generally known (such as Committees' preparatory documents), their handling classification, or distribution, need not be separately marked on the document in question. When processing documents of this type, any given regulations and instructions are to be obeyed in all pertinent respects.

Regardless of the aforesaid exceptions, the official who classifies the information in question shall also be responsible for verifying that the documents and any other recordings are provided with the information handling classification marking, and that the document distribution scope is defined.

The *preparation material* accumulated from the drawing up of a document or any other recording shall be processed and stored as required by its handling classification. In cases where secret preparation material is processed by more than two people, the material must also be marked with a stamp or through using another suitable method. Any unnecessary preparation material must be disposed of immediately.

For information classification examples, refer to *Appendix 1*. The head of the office or unit responsible for information and documents will provide additional instructions as necessary, to specify the procedures set out in Appendices 1-6.

Public information

Most of the information processed by Parliament is classified as public. According to the law, this information is not to be kept secret, and outsiders may be allowed access to it.

Parliament's Information Unit is responsible for the active publication of information.

Information that is meant for internal use

Information may be classified for internal use in cases where:

- the document in question has been drawn up for an authority's internal work and does not contain any information necessitating the document to be archived due to the information quality or its character, or

- the document in question is unfinished, in other words notes which have not been submitted by the author for introduction or any other further processing of the matter in question.

Regardless of the fact that information which has been classified for internal use is not to be kept secret, it shall only be discussed by and communicated between people who are necessary from the point of view of the handling of the matter in question.

With respect to its contents, the information that is classified for internal use corresponds to the markings used by a number of official institutions: *"Not to be divulged to outsiders"* and *"For official use only"*.

Information to be kept secret

Information is to be classified as secret only when so prescribed by the law.

Since any documents relating to *legislative work* are public as a rule, it is especially important to mark secret all the documents which are secret on the aforesaid grounds, based on the Parliament's standing orders, section 43, paragraph 3, or which contain information that belongs to the sphere of professional secrecy, based on section 50, paragraph 3 of the Constitution. The latter professional secrecy obligation is normally connected to matters processed by the Grand Committee or the Foreign Affairs Committee that also bindingly decide upon the professional secrecy obligation on behalf of any other Committees.

Any regulations which are central from the point of view of *administration activities* concerning concealment are combined in the Act on the Openness of Government Activities. Individual secrecy regulations are set out in section 24, paragraph 1, of this law, which includes an itemised 32-point list of documents which are to be kept secret. Among other things, the purpose of these regulations is to protect:

- the country's foreign-policy interests and international relations,
- the country's safety and civil defence,
- the public interest in crime investigations and other police activities,
- safety arrangements for people, buildings, institutions, constructions, information and communication systems, and their implementation,
- the pursuance of the national incomes policy, financial policy, monetary policy, and foreign exchange policy,
- the reliability and functioning of financial systems and insurance systems,
- the citizens' confidence in capital markets and financial markets,
- the preservation of the authorities' preconditions for inspections,
- the conservation of nature values,
- the benefits related to research activities and statistics production,
- economic benefits,

- professional research and development benefits that are comparable to business secrets or trade secrets,
- the functionality of the experiments and tests, and
- the people's privacy.

In the majority of cases, the Act on the Openness of Government Activities defines the document-related secrecy obligation with the aid of the document-contained information. When regulating the secrecy of such documents, which are secret because of their content, the main attention is paid to the type of their information content. The non-disclosure of a document is partly based on the absolute secrecy obligation set out in the Act on the Openness of Government Activities. In such a case, the document shall be kept secret without any additional preconditions. However, most secrecy regulations prescribed by the Act on the Openness of Government Activities include a so-called *conditional damage clause*. The purpose of this clause is to restrict secrecy to the crucial elements in each situation, from the point of view of the interest being protected. *The effect of the clause on the secrecy in question will vary, depending on whether the document in question should be public or secret according to the law.* In the cases above, a document is prescribed to be kept secret, provided that releasing information on it will cause the regulation-intended type of disadvantage to the benefit being protected. On the other hand, if secrecy is presupposed, the releasing of information is determined by the fact that disclosure will not cause the prescribed type of damage to the benefits being protected. Irrespective of which one of the two alternatives is presupposed in the regulation, *an estimate of any probable damage must be made as per case.*

Outsiders must not be given any information which is to be kept secret unless they have a legitimate right to it. Any discussions and other exchange of information must be exclusively restricted to duly authorised persons. In general, the persons in question are indicated by the document distribution information.

The "secret category" corresponds to "*For authorised personnel only*", which is a category used in some institutions.

3.3 Handling information material requests

The Act on the Openness of Government Activities prescribes that information concerning a public document must be provided as soon as possible. However, this must be done *within two weeks* from the date on which the authority has received the request concerning the document, at the latest. In exceptional cases, the period may be extended to a maximum of thirty (30) days, however, counting from the receipt of the request in question. The following are among such cases:

- there is a large number of requested documents,
- parts which are to be kept secret are included in the documents, or
- if there is another reason, comparable to the above, which delays the matter handling process and requires special measures for the matter to be resolved.

In normal cases, the maximum deadline is two weeks, during which a document request must be responded to. *In general, the response time for a document request is considerably shorter.* Parliament's Ombudsman has estimated that, in practice, a document's publicity decision must be made on the same date as the request has been made.

It is to be noted, in particular, that after the documents produced or received by Committees have been transferred for filing, any document requests relating to them will be processed by the Parliament Library.

3.4 Responsibility for information security

Information users have the primary responsibility for information security. At the same time, a user may be the information owner, information producer or the document author, for example. Anyone involved with information is personally responsible for information security. In cases where information is secret or meant for internal use only, each user shall be responsible for keeping it secret, and for disclosing it to authorised parties only. The owner of the information has a duty to perform the handling classification of the document (information), if necessary.

The information owner is obliged to classify the document (information) for handling as necessary. The appendix of this instruction contains a table with examples of information handling classification categories. Information provided by another authority or community or an international partner, shall primarily be handled as presupposed by the information owner, unless otherwise prescribed by the special regulations pertaining to Parliament work. Should information be classified, Parliament and any similar actor shall process it through the use of an identical or closely similar classification category.

4 SECURITY ISSUES RELATING TO THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES

4.1 Basic security issues relating to the use of information technology

ADP system users are identified with the aid of a username and a password. These are used as necessary to verify who has used the information system in question. User names authorise users to use the information systems and information that they need in their work, and which they are allowed to access. Information system user authorisations are granted by the information system owner. Only the owner or a party duly authorised by the owner may grant information system authorisations.

A username is always personal and must not be given away to another user under any circumstances. The username owner is invariably the sole party responsible for anything done with the username. A user does not have the right to provide another user access to an information system, without the information system owner’s permission.

Parliament’s information systems, and the information contained therein shall primarily be used for duty-related or assignment-related tasks only. Unnecessary printing or copying of information intended for internal use or secret information must be avoided since extra paper copies increase the risk of information falling into the wrong hands.

It is advisable to save your data onto a net-based disk (for example, save any personal data onto the H disk drive) because any data items contained therein will subsequently be backed up at regular intervals, thus ensuring that data may be successfully restored as necessary. If data is merely saved onto the workstation hard disk (C disk drive), it may be lost in its entirety if the computer crashes or breaks down.

In cases where the information to be dealt with has been classified for internal use only, or as secret, and if it must be distributed further, then it is the user’s responsibility to make sure that the information in question is conveyed to authorised parties only.

4.2 Use of the Internet

The Internet is a very good source of information, and a practical information transfer system between various parties. In addition, it is an excellent tool for the publication of information. The Internet is not a single, uniform network but consists of a huge number of inter-linked networks through a standard procedure (the TCP/IP protocol family). The

Internet does not have a responsible operator, and its functionality and operation are not regulated by international agreements.

It is always possible to copy, record and change any information conveyed on the Internet, without any indication of this action remaining in the information itself. On the Internet, information frequently passes through several networks. It is often impossible to clarify afterwards the route travelled by the information in question on the web. At separate user sessions, even during a single session, information can be passed through separate routes on the web.

On the Internet, Parliamentary users can be identified by the organisation level. Whenever a user visits an Internet site or service, the service administrator can see whether the user comes from the Parliament.

Information that is generally available on the Internet is not always authentic and correct. Each user must personally verify the information correctness and authenticity, plus his or her right to use the information in question. Copyright protection must be remembered, in particular. Copyrighted material must not be downloaded onto the Parliament's computers, unless separately so authorised.

4.3 Remote usage

Remote usage includes any use of the Parliament's computers outside the Parliament's premises. Remote usage can take place while being connected to the Parliament's information network, or without this connection.

When remote usage takes place through the Parliament's information network, that is from a *remote workstation*, the connection between the Parliament's computers and the portable workstation in question is protected by means of a special program. In any other remote usage, the data communication connection is not protected.

Remote access to secret information is prohibited without this protection. When using remote access without the said protected connection, the user must verify that the information to be dealt with has not been classified as secret. In cases where information is processed through an unprotected connection, while being connected to the Internet, the user must ensure, in advance, that any data items being processed are checked for viruses before they are returned to the Parliament's information network.

In connection with remote usage, users must take good care of the equipment and data media available, and are not allowed to lend these to outsiders. *Never leave a portable workstation, a mobile phone, or any other data medium in an open place without surveillance.* Especially avoid leaving them on view in cars and other vehicles.

4.4 Outsiders working in the Parliament

In terms of information security, identical principles are applied to all parties working in the Parliament – Parliamentary and non-Parliamentary employees, and any other actors alike. The said external actors must be made familiar with their statutory obligations and liabilities. In cases where such an external actor must be provided with information that has been classified as secret, their secrecy-related duties must be set out in the purchase agreement, service agreement, or another similar document. In cases where an individual person is to be provided with secret information, whom a separate agreement will not be made, his or her secrecy-related duties must be clarified in a separate letter of commitment. The head of the unit in question is responsible for concluding and storing the said agreements and commitment documents.

4.5 Consequences for information security breaches

The slightest sanction for breaching statutory regulations, these instructions, or any other information security regulations, will be the cancelling of the information system user authorisation for the person or party in question.

5 HANDLING INFORMATION SECURITY ISSUES

Parliament’s information security arrangements are co-ordinated by its *IT Office* that supports the decision-makers and is responsible for the information security arrangements’ functionality. The IT Office can be contacted in ICT-related matters, and, for example, for any information security problems concerning document classifications.

The responsibility for information security control arrangements rests with the head of each unit that produces, processes or otherwise deals with information. He or she must personally see to it that information is dealt with and processed according to the procedures presented in this document and its appendices, and that the unit personnel are made familiar with any relevant information security issues and aspects.

APPENDICES 1 - 6

Appendix 1 Examples of information handling categories

Public	For internal use	Secret
Purpose and main tasks in Parliamentary work	Matters being prepared by various Committees	
Operating strategies for Parliamentary units Operating plans and budgets for departments and units		
Organisation charts Registers		
Bulletins and announcements		
Publicised speeches, lectures and research reports	Internal and unfinished reports	
Use of Parliamentary funds		
		Companies' and private persons' credit information, etc.
		Private persons' health information
Publicised EU Notices		The Grand Committee's secret EU materials
Information security principles and information security instructions		Information security solutions (controls and their details)
		Parliament's recovery plans for catastrophes
		Parliament's contingency plans and other preparatory arrangements
Undersigned acquisition and contract agreements Invitations to tender are public once they have been undersigned or otherwise verified	Quotations prior to the acquisition decision	Acquisitions and contracts relating to safety and security
General computer types Number of microcomputers General office software		Detailed computer hardware configurations, security equipment

Public	For internal use	Secret
Information system entities	Documents and properties of individual systems	Security systems
	Physical access control and work time monitoring arrangements	Parliament's safety and security arrangements for special cases

Appendix 2 Classification markings

Public	For internal use	Secret
No marking	If necessary, write on or stamp the front page as "For internal use", close to the document name	Write on or mark the front page as "Secret"

Appendix 3 Oral communication

Handling technique	For internal use	Secret
Telephone conversations	Permitted	Use covert speech as necessary
DECT telephones and other radiophones (without encryption devices)	Permitted	Prohibited
GSM phones	Permitted	Use covert speech as necessary
Answering machines, voice mail	Permitted	Prohibited
Conversations on public vehicles and public premises	To be avoided, make sure that outsiders cannot hear the conversation	Prohibited

Appendix 4 Handling information through electronic communication systems

Handling technique	For internal use	Secret
Telefax (including Internet-based fax)	Permitted	Make sure that you have typed the correct recipient number. Verify reception with a test transmission. Send the message. (The named recipient or their representative must be present at the receiving device.)
Telefax devices with encryption	Permitted	Permitted
Internal e-mails	Permitted	Permitted for those who need the information for their work
External e-mails and electronic letters	Permitted	Prohibited, unless the encryption technique has been approved by the Parliament IT Office
Parliament Intranet (Fakta and other systems)	Permitted	Permitted, provided that viewing is restricted to authorised document users
Other Internet services	Permitted	Prohibited

Appendix 5 Handling paper documents, drawings, microfilms, etc.

Handling method	For internal use	Secret
Distribution markings (in general, at the end of the document)	To the personnel required by the work in question	To the personnel required by the work in question, list the persons or personnel groups for distribution
Monitoring the use of information (The owner = the information producer or the recipient of externally-provided information)	The owner gives instructions, if necessary	The owner or someone authorised by the owner (a secretary, for example) controls and keeps a list of information recipients that is then attached to the original document
Copying	Additional copies may be made in accordance with the work requirement	Recipients mentioned for distribution; or people authorised by them, a secretary, for example, must keep a list of those who have received additional copies
Delivery by internal post	Similar to ordinary mail, if necessary, in a closed envelope	Courier delivery in a closed envelope, with the marking "Personal" positioned below the recipient's name

Handling method	For internal use	Secret
Delivery by post	Similar to ordinary mail, if necessary, in a closed envelope	Not to be used. By courier only
Opening received mail	By the recipient or those authorised by him or her	By the recipient, or those separately authorised by him or her to open secret mail (a secretary, for example)
Keeping diaries	In accordance with the diary instructions	The diary publicity is to be assessed as per message. A totally secret diary marking is permitted in cases where any information concerning the matter under discussion is considered secret
Archiving	In accordance with the archiving instructions	To be archived alongside other secret documents
Lending	May be lent in accordance with the work requirement	No to be lent
Preservation in Parliament	If necessary, in a locked room or cabinet	In a locked room, box, cabinet, safe, vault or similar space
External preservation (at home, in a hotel, etc.).	In locked rooms	In a locked room, box, cabinet, safe, vault or similar space
Preservation during travel	In a locked briefcase, if possible	Invariably in a locked briefcase under constant surveillance
Disposal: documents - by whom? - how?	Those mentioned in the distribution list, or people authorised by them, for example, a secretary or an office master, disposes of the documents using a document shredder, or deposits them in a locked collection container	Those mentioned in the distribution list, or people authorised by them, for example a secretary disposes of the documents using a document shredder, the maximum shred size being 0.8 x 20 mm, or deposits them in a locked collection container
Disposal: OHP transparencies, protective paper jackets, ink ribbons - by whom? - how?	The holder deposits the material in a locked collection container	The holder deposits the material in a locked collection container, or disposes of them using a document shredder, the maximum shred size being 0.8 x 20 mm

Appendix 6 Handling of information in the electronic form

Handling method	For internal use	Secret
Processing on workstations located on controlled Parliamentary premises	The use of password-protected screen savers is recommended	Permitted only for the handling duration, after which the information must be saved onto a data medium that is stored in a locked metal cabinet or a safe
Processing on workstations located on controlled Parliamentary premises, with a data communication connection to network-based classified information	A personal network username and a password must be used	A personal network username and a password must be used
Processing on portable microcomputers containing classified information and which are carried outside the Parliament	Password-protected screen savers must be used	Device-specific passwords and security software must be used The use of a password-protected screen saver is compulsory Personal responsibility for surveillance
Processing on remote workstations, with a data communication connection to classified information located on Parliamentary premises	A personal network username and a password must be used The data communication connection technology must be approved by the Parliament IT Office	A personal network username and a password must be used The data communication connection technology must be approved by the Parliament IT Office
Processing in information systems	User authorisation based on personal usernames and passwords	User authorisation based on personal usernames and passwords The information system protection arrangements must be approved by the Parliament IT Office
Copying and forwarding	In accordance with the user authorisation Forwarding in accordance with the work requirement	Prohibited
Printing on shared Parliamentary printers	Permitted	Those mentioned in the distribution list or people authorised by them must control the printing process
Data media[1)] preservation in Parliament	If necessary, in a locked room or cabinet	In a locked room, box, cabinet, safe, vault or similar space
Data media[1)] preservation outside parliament: at home, in a hotel etc.	In locked rooms	In a locked room, box, cabinet, safe, vault or similar space
Preservation of data media[1)] during travel	In a locked briefcase, if possible	Invariably in a locked briefcase under constant surveillance

Handling method	For internal use	Secret
Data media[1] shipments	In a closed package to those mentioned in the distribution list, by post, for example	As courier delivery only, into the hands of the named recipient
Reuse of data media[1] by other MPs	Requires - the media-contained files to be deleted (using the DEL-command) or - formatting of the data medium in question (using the FORMAT-command)	Prohibited The data medium must be disposed of, provided that the information owner will no longer use the medium in question
Data media[1] disposal	Through breaking, folding or rendering useless by a similar method	Through using a document shredder
Deleting information from the hard disk in conjunction with computer replacements	The Parliament's ADP support deletes the existing information and initialises the computer hard disk	The user deletes the files The Parliament's ADP support deletes the information and initialises the computer hard disk
Delivering microcomputers to an external maintenance service	Removal of the hard disk from the microcomputer is recommended Information recovery onto the hard disk invariably requires a case-specific agreement and a reliable partner	The Parliament's ADP support removes the hard disk from the computer before maintenance Information recovery onto the hard disk invariably requires a case-specific agreement and a reliable partner

1) The term data media refers to diskettes, ZIP disks, CD-ROM disks, magnetic tapes and other similar portable recording devices.

THE FINNISH PARLIAMENT’S E-MAIL INSTRUCTIONS

Approved by the Chancellery Commission 11th November 2004

PUBLICATION 8/2005 BY THE PARLIAMENTARY OFFICE

SUMMARY

Advisable to know and remember!

- Remember to use good manners when using e-mail.
- E-mail is a written document which can be dealt with and duplicated by others at a later stage.
- There is no cancel function available in external e-mail transmissions.
- Respect the recipient’s mailbox. Do not send chain letters, Christmas greetings or joke messages in internal e-mail.
- E-mail is like an open note on the Internet – anybody can read it.
- Always write the e-mail address exactly right, otherwise the message can go to the wrong person, or it may disappear.
- On the Internet, it is possible to send an e-mail in anybody’s name.
- E-mail is intended for the transmission of messages and for their short-term storage. Computer programs and large information materials are to be conveyed by other methods.
- The arrival or response times of e-mail cannot be guaranteed. To ensure the arrival of e-mail, ask the recipient to acknowledge receipt.

PREFACE

In Parliamentary use, e-mail has become a very significant medium, in internal and external communication alike. With the increasing significance of e-mail, the need to specify joint rules for e-mail users has increased simultaneously, to facilitate the undisturbed operation of the existing e-mail system. The purpose of this set of instructions is to meet that need.

It was primarily drawn up for the Parliament's needs, and for those of any offices operating under it. The instructions lean on the existing legislation and on good information management practice. When preparing these instructions, use was made of the Government's existing instructions for public administration. Furthermore, the ethical principles created by Internet users were also taken into account.

The instructions have been prepared as an assignment commissioned by the Parliament's Information Systems Group. The document was produced by the following team:

Kari T. Sipilä, ADP Manager (until 30th May 2004), Administrative Department (Chairman)
Ritva Bäckström, Committee Counsellor, Committee Secretariat
Jorma Kuopus, Deputy Chief Secretary, Parliamentary Ombudsman's Office
Kaj Laine, Director of Internal Audit, State Audit Office
Marja Wallin, Parliament Secretary, Central Office
Outi Juntura, System Analyst, Administrative Department (Secretary)

The team carried out its assignment in a good, constructive spirit. Discussions on the instructions' content were very versatile, with the exchange of thoughts illuminating the issue from several points of view. The team's objective was to write good, clear, easy-to-read instructions, explaining the grounds and operating rules for the users of e-mail in our Parliament.

Helsinki, Finland, 24th May 2004

Kari T. Sipilä

INTRODUCTION

Background

These are the Parliament’s e-mail instructions containing general procedural instructions for the use of e-mail inside Parliament, between Parliament and citizens/clients, and between various authorities.

At the same time the instructions reflect the Parliamentary e-mail policy.

Premises for the use of e-mail

Originally, e-mail was intended for the transmission of short messages and their short-term storage. E-mail functions best in internal communication. Subsequently, its use has expanded to the transfer of information materials. There are no international agreements in force concerning the conveyance of e-mail messages, nor any single responsible operator. Instead, the transmission of messages is based on the use of a uniform data communication protocol. Regardless of the fact that the e-mail protocol contains a few shortcomings regarding the encryption and integrity of the messages being conveyed, e-mail has become the general practice in global electronic communication.

In external e-mail communication, the transmitting of sensitive information is to be avoided, and secret information must not be passed on via e-mail without encryption.

Terminology

Internal e-mail refers to communication between users through the Parliament’s e-mail system.

External e-mail refers to outgoing communication from the Parliament’s e-mail system to the Internet, or to incoming communication from the Internet to the Parliament’s e-mail system.

An electronic message refers to information that is sent using electronic data transfer, in accordance with the law, in e-Business with authorities. Consequently, the distinction between a message and a document is open to interpretation in some cases. Depending on the context, a message may also be a document.

An electronic document, in turn, refers to an electronic message that is connected to the institution of proceedings in a case, to the handling of the matter in question, or to the publication of the pertinent decision.

1 COMMUNICATION INSIDE THE PARLIAMENT

The Parliament's e-mail system is reliable, with regards to the arrival, functional dependability, security, and information confidentiality preservation of any internally transferred e-mail. The internal e-mail system uses ready-made address lists to ensure that the message is received by the right person. Internal communication may consist of document transmission, discussions or information provision with the aid of distribution lists.

2 EXTERNAL COMMUNICATION

External communication passes through the Internet from the Parliament to the recipient, or through the Internet from the sender to the Parliament. An essential aspect is that the messages in question are transmitted through the Internet. The Parliament IT Office is not in the position to guarantee the message-specific information security or the conveyance of messages on the Internet. In malfunction situations, it is mostly difficult, and frequently impossible, to clarify the delay or disappearance of the message transmission. The Internet does not have a single responsible operator, and there is no international agreement to appeal to, so as to safeguard its functionality. The only issue that has been jointly agreed upon is the use of and adherence to joint data communication standards.

2.1 Official business with Ministries

The Ministries follow their own instructions on the use of e-mail. The e-mail communication between the Ministries and Parliament is directed to the closed network of the Prime Minister's Office, instead of the Internet. The Prime Minister's Office is a physically separate and secure network between the Ministries. Even in cases where connection to the Prime Minister's Office network is lost, e-mail messages will not be routed via the Internet to the Ministries. This means that confidential and official materials can be transmitted via e-mail to the following quarters (the list was updated on 20th May 2004):

- vn.fi and vnk.fi – Prime Minister's Office
- vm.fi – Ministry of Finance
- tpk.fi – Office of the President of the Republic
- mmm.fi – Ministry of Agriculture and Forestry
- vyh.fi or ymparisto.fi – Ministry of the Environment
- formin.fi – Ministry of Foreign Affairs
- mintc.fi – Ministry of Transport and Communications
- intermin.fi – Ministry of the Interior
- mol.fi – Ministry of Labour
- bof.fi – Bank of Finland

- rata.bof.fi or rahoitustarkastus.fi – Financial Supervision Authority
- stm.fi – Ministry of Social Affairs and Health
- minedu.fi – Ministry of Education
- om.fi – Ministry of Justice
- okv.fi – Office of the Chancellor of Justice
- ktm.fi – Ministry of Trade and Industry

2.2 Citizens’ e-mail based business with Parliament

If necessary, citizens may conduct any of their e-mail based business between authorities and various organisations through using the official e-mail addresses. The Parliament’s official e-mail addresses are as follows:

- eduskunta@eduskunta.fi (Parliament)
- kirjaamo@eduskunta.fi (Registry)
- eoa-kirjaamo@eduskunta.fi (Ombudsman’s Registry)
- valtiontilintarkastajat@eduskunta.fi (State Auditors)
- kirjaamo@vtv.fi (State Auditors’ Office)
- riksdagen@riksdagen.fi (Parliament, service in Swedish)
- kirjaamo@riksdagen.fi (Registry, service in Swedish)
- eoa-kirjaamo@riksdagen.fi (Ombudsman’s Registry, service in Swedish)
- statsrevisorerna@riksdagen.fi (State Auditors, service in Swedish)

The above official addresses are not filtered for their content or junk e-mail. Instead, any virus-infected e-mail messages are deleted automatically. The e-mailbox administrator of each official address is obliged to check any e-mail received.

3 E-MAIL HANDLING PRINCIPLES

3.1 E-mail addresses and their publication

Parliament's e-mail addresses can be personal (firstname.surname@eduskunta.fi), official (kirjaamo@eduskunta.fi) or internal, general e-mail addresses that are related to customer services (for example, office assistants, security). E-mail cannot be sent from general e-mail addresses to the Internet. For each personal e-mail address (firstname.surname@eduskunta.fi), there is also a Swedish (riksdagen.fi), English (parliament.fi) and French (parlement.fi) version available.

All the e-mail addresses of Parliament and its office are found in the JULHA directory service (http://www.julha.fi).

3.2 Usernames and passwords

In addition to Members of Parliament, all people employed by the Parliament and its offices, are provided with an e-mail username and a password, provided that their employment duration is at least 30 days. The appropriate use of this user authorisation is always the user's personal responsibility. This means that you must never give away your username password to anybody. During holidays, each employee is obliged to ensure that his or her substitute has the required user authorisation for the e-mail box in question.

The e-mail system passwords must be renewed every six months, and at any time if the situation so requires. A password must be difficult to guess, and at least eight characters in length. Passwords are meant for personal use only.

3.3 Handling of official e-mail

The primary purpose of e-mail is to convey messages and to store them for short periods. In e-Business, electronic messages are separated from electronic documents. An electronic message refers to information that has been sent using an electronic data transfer method. An electronic document refers to an electronic message that is connected to the institution of proceedings in a case, to the handling of the matter in question, or to the publication of the pertinent question. Consequently, the distinction between a message and a document is open to interpretation in some cases. Depending on its content and context, a message may also be a document in accordance with the Act on the Openness of Government Activities.

Any e-mail received at official addresses (eduskunta@eduskunta.fi, kirjaamo@eduskunta.fi, eoa-kirjaamo@eduskunta.fi, valtiontilintarkastajat@eduskunta.fi,

kirjaamo@vtv.fi) must be directed to all those responsible for the matters in question. As far as possible, any message should be responded to via the official e-mail address in question.

The e-mail sender is responsible for the message and its arrival, and for any delay from a deadline that has possibly been agreed upon. This responsibility also applies to the correctness of the address in question. On the Internet, even a single misspelled character will take the e-mail to the wrong address (provided that the misspelled address exists somewhere). To clarify the division of responsibilities, the official e-mail box administrator must immediately notify the sender of the message/ document receipt, provided that this is not a case of junk e-mail or spam referred to in 6.2. Following the said notification, the responsibility for the message and its handling will transfer to the recipient. In cases where you receive official e-mail via your own e-mail box, direct it to an official e-mail address.

It is prohibited to send an official e-mail or direct it automatically to a private e-mail address (to external e-mail systems, such as hotmail, yahoo, etc.), for information communication safety reasons.

3.4 Handling of private e-mail

The use of e-mail at work, even in the Parliamentary environment, involves the protection of privacy for employees, officials and civil servants. In private e-mail communication, it is advisable to mark the e-mail message header field as “Personal/Private”. Furthermore, it is a good idea to define the message confidentiality level (private, internal, general) for internal e-mail transmissions. For example, if an internal e-mail message has been marked as private, it may not be forwarded automatically, nor can it be viewed by persons with the so-called secretarial rights to read the recipient’s mail box.

It is advisable to remember *that e-mail communication between the Parliament and external e-mail systems is not encrypted.* This means that confidential or sensitive personal information, for example relating to people’s health, must not be transmitted to external e-mail systems. This applies to public and private e-mail communication alike.

Employees are entitled to acquire private e-mail addresses (for charge-free browser-operated e-mail services, for example) and use them on Parliament’s workstations.

3.5 E-mail arriving at the wrong address

Should a user receive an e-mail message that has been intended for another person, he or she will be subject to professional secrecy and utilisation prohibition concerning the message.

If an authority or a civil servant receives an e-mail message that has been intended for another authority, the message must be forwarded to the correct authority in accordance with the Administrative Procedure Act.

Any e-mail messages intended for another person (such as namesakes) must be forwarded to the correct address, provided that this is known. If the address information is not available, then the sender must be informed of the transmission failure, in accordance with good manners, and the message received must be deleted.

Should an e-mail address be changed (when changing the surname, for example), any mail arriving at the old e-mail address will be directed to the new address for a period of 30 days. The person in question is to notify his or her communication partners of the new e-mail address during the said period.

3.6 Procedure to be used during an e-mail user's temporary/periodic absence

A person's e-mail will be closed in conjunction with his or her pre-planned, periodic absence, such as leave of absence. If the person in question has the remote user authorisation, they may use their usernames and passwords during their temporary absence. When a permanent appointment or service relation comes to an end, the related e-mail user authorisation will be revoked. The person in question is to notify his or her communication partners of a possible new e-mail address.

The Act on the Protection of Privacy in Working Life prescribes that the opening and clarification of any messages sent to an employee, or that of any duty-related messages transmitted by him or her, during his or her temporary or periodic absence, must be based on the employee's consent. The last resort shall be the opening of the messages addressed to the employee in question, without his or her consent, as prescribed by the law (see chapter 6, sections 18-20 of the Act on the Protection of Privacy in Working Life).

3.7 Procedure after a person's death

After a person's death, the IT Office will close the dead person's e-mail account and delete its e-mail content.

3.8 Forwarding of e-mail

Automatic forwarding of e-mail from the Parliament's e-mail system is invariably prohibited for information protection and communication reasons. This applies to:

- any transmissions to private e-mail addresses during holidays;
- other e-mail addresses during leave of absence; and

- the forwarding of message transmissions to private e-mail addresses outside Parliament.

Parliamentary employees may safely access e-mail remotely from any Internet-based workstation that is provided with a sufficient protection level, in other words, from those allowing an encrypted HTTPS connection. Furthermore, the person in question must possess the medium for identification granted by the Administrative Director to verify his or her remote user authorisation.

3.9 Clearing of e-mail boxes

The size of the Parliament's e-mail boxes is 70 megabytes (20th May 2004). To secure the fast functioning of the e-mail system, any new e-mail messages received should be read or marked as having been read. In addition, the number of messages in the Received Folder should be kept to a minimum (under 500 messages is recommended). Therefore, any messages that are over 6 months old will be cleared from the Received Folders and Outgoing Folders on Saturdays. Should anyone want to retain messages which are older than 6 months, they must transfer the messages to their own folders. The filing of messages in folders is a good e-mail management method in many additional respects.

3.10 Use of distribution lists

The transmission of general notices and bulletins through wide distribution lists (in Parliament) should be scheduled for quiet times by using the e-mail timing function. The transmission of general personal announcements (Buy/Sell/Rent addressed to the entire personnel) through e-mail is prohibited. There are advertising pages for these purposes on the Intranet (Fakta, Inner Circle) and the VTV forum. It is not desirable to send Christmas greetings to the entire personnel.

3.11 Undersigning of e-mail messages

The Parliament's e-mail system supports the S/MIME standard that enables the encryption and undersigning of messages. A signature guarantees the message integrity (=unchangeability) and verifies the sender. Up until now, however, Parliament has not adopted the practice of encrypting and undersigning of e-mail messages, with the aid of an HST card, for example. Consequently, secret material is not to be sent through e-mail on the Internet.

4 E-MAIL AND INFORMATION SECURITY

It is impossible to provide e-mail messages and their appendices with any basic safety warranty features for their passage through the Internet. Any required information security features must be built in separately. The basic security features are as follows:

- Confidentiality – the information is accessible to only those who are entitled to it.
- Integrity – the information remains unchanged under all circumstances.
- Verification – the parties can be reliably identified.
- Indisputability – the parties can be identified, even afterwards, to prove that they have personally written the message in its existing form.
- Availability – the services are available at all times as necessary.

In addition, there are other information security problems with e-mail:

- viruses
- junk e-mail or spam
- message disappearance
- delayed arrival of messages

The existing system technology is incapable of eliminating all these information security shortcomings. Instead, we must accept them as basic impediments relating to the use e-mail; and whenever e-mail is used, these risks must be borne in mind. They can be partly reduced through good e-Business practice and appropriate e-mail system administration. Each user is personally responsible for the promotion of e-mail information security.

5 MAINTENANCE REQUIREMENTS AND METHODS

E-mail maintenance is required to ensure the undisturbed functioning of e-mail. For this purpose, the reception of malicious programs, junk e-mail or spam and unnecessary file attachments is restricted as per need.

5.1 Restrictions for e-mail messages and file attachments

The IT Office has a right to set restrictions on e-mail messages and their file attachments. Restrictions can be implemented, for example, by filtering off any messages and files of excessive size (more than 20 megabytes, more than 50 file attachments), or those imposing a threat to the Parliament’s information security, such as executable programs (.exe, .bat, .com, Java Scripts, and the like). Users are informed of these restrictions.

Parliament observes good information management practice, based on which the IT Office uses computer programs to check the messages and their file attachments for possible viruses and malicious programs. The IT Office is obliged to delete any messages that contain viruses or other malicious programmes, plus any file attachments from all incoming and outgoing e-mail transmissions.

Parliament’s virus control has been arranged on a very comprehensive basis. The e-mail servers and user workstations are provided with antivirus software. The IT Office endeavours to stay abreast of any viruses being propagated. However, should a virus, worm or any other malicious programme manage to pass through Parliament’s virus control, then the IT Office will inform users of the incident and take immediate action for its elimination. In general, virus warning e-mails are false alarms and comparable to junk e-mail or spam. They are not to be forwarded. Should a user suspect that his or her computer is contaminated by a virus or another malicious program, they must inform the ADP support service accordingly.

5.2 Junk e-mail

Junk e-mail or spam refers to all unnecessary e-mails – generally advertising e-mail, which is sent to large groups of users without their consent. With the increasing use of the Internet, spamming has become a serious problem. Currently, ready-made spam programs are being propagated to enable massive disturbance to existing e-mail systems. Ordinary users experience spam-related disturbances in the form of increasing incoming e-mail which slows down or even prevents the e-mail

function in its entirety. Other forms of disturbance include sending e-mail in other people’s names, and filling up their e-mail boxes.

Never respond to junk e-mail. If a message is responded to, your address will be indicated as operational, which will further increase the risk of being entered onto additional junk e-mailing lists.

The IT Office makes efforts to reduce the junk e-mail problem technically, by using inhibit lists that prevent the arrival of junk e-mail from well-known spam propagating servers. Junk e-mail inhibition applies to Parliament’s e-mail system in its entirety. Furthermore, users may create their own personal inhibit function, for example, with the aid of the Tiimiagentti (Team Agent) software.

It is prohibited to use the Parliament e-mail system to propagate any junk e-mail, illegal material, or any other material that is contrary to good manners (abusive, blasphemous, racist or insulting materials, among others).

5.3 Supervision of e-mail and data communication network use

The IT Office controls Parliament’s e-mail communication to guarantee information security and the IT system’s disturbance-free functioning. This supervision does not violate communication secrecy or users’ privacy. Neither do other forms of network usage supervision groundlessly violate people’s privacy. Under certain circumstances, however, a detailed investigation may be necessary.

5.4 Collection and storage of log data from e-mail and information communication network usage

Parliament uses log data only for technical tasks by maintenance personnel bound to professional secrecy. Among others, these tasks include safeguarding the required service level, the clarification of fault situations, and the compilation of statistics.

To analyse information security violations or acute attack situations which threaten the information network security, the IT Office may disclose routing information, for example, to the Finnish Communications Regulatory Authority (www.ficora.fi), or to other Finnish system administrators. Among other items, this routing information includes precise log data concerning each attack’s network connections. In these cases, it may also be necessary to disclose information relating to an individual username. The disclosing information invariably restricts those usernames that can justifiably be presumed to have fallen into the wrong hands, or to cases where there is reason to believe that the username holder may be guilty of the breach or crime being processed. Any disclosing of the said information will be recorded.

5.5 Responsibility of the maintenance personnel

Parliament’s ADP support service always requests permission of the user being provided with instructions, before they assume remote control of his or her computer screen. The ADP support’s professional secrecy extends to any operations carried out in remote control on a user’s workstation.

The IT Office appoints the persons responsible for the Parliament e-mail system. The e-mail system refers to the server system which comprises the equipment with its system software, the dedicated e-mail server software, data transfer connections and any e-mail messages processed by the server, and their processing rules.

The maintenance personnel consists of those who deal with log data and other people’s messages in their work. They are bound by professional secrecy and have committed themselves to observe the rules prescribed for the maintenance personnel.

6 LEGISLATION

This set of instructions includes an appended survey of the legislation pertaining to the use of e-mail in working life in various ways. The legislation is briefly summarised providing an account of the content of various regulations and their significance for the use of e-mail. The intention has been to make the basic regulations available in a combined form to those interested. On the other hand, the team that prepared these instructions found it appropriate to analyse the regulations’ background, so as to provide a basis for its own work and for these instructions. However, the e-mail user instructions apply as such, and can be used separately, without reading the appended legislation appendix.

7 INTERNET BEHAVIOUR OR NETIQUETTE

The Internet and e-mail are excellent tools for information retrieval and communication. It should be borne in mind that there is no protection in e-mail and the Internet. Instead, information flows through public networks without encryption. E-mail is like an open note on the Internet – anybody can read it.

Since e-mail is unencrypted and unsigned it is easy to falsify. Anybody can send e-mail in anybody’s name, so maintain a healthy suspicion towards any incoming e-mail.

The arrival or response times of e-mail cannot be guaranteed. The sender is always responsible for the arrival of e-mail. A good practice to secure the arrival of e-mail is to include a separate receipt/confirmation request in the transmission.

E-mails are written documents which may be stored for long periods. The message in question must endure various types of further processing. In general, sound advice is not to write something in e-mail that you would not otherwise say face to face with the person in question.

It is easy to duplicate and forward e-mail to third parties without the original author knowing anything about it. This risk should also be observed when writing e-mails. On the other hand, each and every one should consider whether any message received was originally intended only for the recipient, before forwarding, printing/distributing it.

Respect the recipient’s mailbox. Do not forward chain letters. For example, the transmission of large message files, such as Christmas greetings, overloads the e-mail system and the recipient’s e-mail box.

The e-mail address is valuable to its owner. Its replacement is not easy and usually causes a great deal of trouble. Junk e-mail may damage your e-

mail address or render it useless. Take good care of your e-mail address. It is advisable to carefully consider to whom to give your personal e-mail address. In general, when registering for Internet-based services, only disclose the minimum of information.

Netiquette, an example:

- http://edu.tokem.fi/IT/Netiketti/netiketti.html

Information security guides, an example:

- http://www.tieke.fi/tietoturvaopas/opas.html

8 SOURCES

- The State Administration's Information Management Instructions for Internet Information Security, the State's Executive Team for Information Security 1/2003.
- The State Administration's Procedural Instructions for E-mail and Log Data. The State Administration's Management Team for Information Security 5/2001.
- Valid regulations, instructions and recommendations for the National Archives and Records Administration/Archives of the State/National Archives. On the Internet:

  http://www.narc.fi/ohjeet.html, and

  http://www.narc.fi/johto-/hyvatiedon-hallinta2.pdf
- JHS 132 E-mail in e-Business 132/2003.
- The handling of electronic information systems and materials. Regulation and instruction 126/40/01 22.5.2001 (National Archives and Records Administration, the validity period is from 1st July 2001 to 30th June 2005).
- The archiving requirements in the handling of e-mail. Regulation and instruction by the National Archives and Records Administration 5/06/97, 19.11.1997.

Laws, decrees and decisions in principle:

- Constitution of Finland
- Administrative Procedure Act (434/2003)
- Personal Data Act (523/1999)
- Language Act (423/2003)
- Act on Electronic Services and Communication in the Public Sector (13/2003)
- Act on Electronic Signatures (14/2003)
- Act the Protection of Privacy in Electronic Communications (516/2004)
- Act on the Protection of Privacy in Working Life (477/2001)
- Archives Act (831/1994)

- Act on Parliament Civil Servants (1197/2003)
- Council of State Decision-in-Principle on Electronic Business, the Development of Services, and the Reduction of Data Collection 5th February 1998

LEGISLATION CONCERNING THE USE OF E-MAIL

This set of instructions includes a brief appendix containing a concise survey on relevant legislation from the point of view of e-mail users and service administrators. The regulations extend from the protection of message confidentiality at the constitutional level, to authorities' duties to implement good governance. The protection of privacy in working life has been prescribed separately. With regards to the use of e-mail, the Act on the Protection of Privacy in Electronic Communications constitutes the central regulation. Similar relevance is seen in the regulations concerning authorities' documents, good governance and archiving. Electronic business with authorities may be arranged in various ways and this regulation also applies to the use of e-mail.

The Constitution of Finland

The secrecy of private messages is protected as a civil right. In accordance with section 10 of the Constitution, everyone's private life, honour and sanctity of the home are guaranteed. The secrecy of correspondence, telephony and other confidential communications is also inviolable. In accordance with the draft law in question (HE 309/1993 vp), the purpose of this regulation is to protect the content of confidential messages against access by outsiders. The regulation also secures other types of information relating to the confidential messages, such as their identification data, for example. The regulation concerning the protection of confidential messages was formulated to be comprehensive, so as to also cover the continuously developing new forms of communication with maximum effect. The regulation also applies to communication in various information networks, such as e-mail. Consequently, the content of any messages transmitted or received through e-mail also belong to the sphere of this protection.

The said regulation protects confidential communication against illegal interference. This means that an employer does not have the right to access an employee's messages in information networks, due to the fact that the communication in question may include confidential items, in addition to distinctly work-related messages. The Act on the Protection of Privacy in Working Life (759/2004) prescribes preconditions under which an employer has the right, in specific situations, to access and open a message that has been transmitted/received by an employee.

Furthermore, additional laws may be passed to prescribe restrictions that safeguard citizens' fundamental rights, or any other necessary restrictions pertaining to the investigations, trials and safety inspections of crimes which endanger the security or domestic peace of an individual or society, including the loss of freedom.

Section 21, subsection 2, of the Constitution prescribes the preconditions for good administration. Among other things, the requirement for good administration means that authorities shall act according to the service principle in all communication with their clients, including an electronic business. The guarantees for good administration are prescribed in more detail in the Administrative Procedure Act (434/2003) and in the Act on Electronic Services and Communications in the Public Sector (13/2003).

Administrative Procedure Act

The new Administrative Procedure Act (434/2003) entered into force in early 2004. The Act confirmed the existing practices of good administration and introduced a number of new aspects. Among other things, the Administrative Procedure Act prescribes the procedure to be observed when submitting documents to authorities, and when returning documents to clients, respectively.

Section 7 of the Act obliges authorities to observe the service principle, and appropriateness in their service provision. Section 8 of the Act prescribes authorities' obligation, within the limits of their power, to provide their clients with the required guidance in administrative matters, to provide answers to pertinent questions, and to respond to clients' inquiries. This consultation shall be free of charge. In cases where the matter in question is outside the authority's jurisdiction, the client shall be instructed to contact the competent authority. The practice of good administration includes appropriate responding to inquires, which must be itemised to a sufficient degree, within a reasonable period of time, and to additional contacts of other types. In addition to conventional forms of business, the obligations apply to e-mail and any other contacts made using other electronic data transfer methods.

According to section 17 of the Act, documents are delivered to authorities' business addresses at the sender's own risk. The sender must also make sure that the document in question arrives within the time limit possibly set by the authority. According to section 23 of the Act, authorities shall also present the party in question, if they so request, an estimated decision date. Furthermore, authorities must respond to any inquiries concerning the progress of the proceedings in question. In cases where a document is delivered by mistake to an authority that has no jurisdiction in the matter, the document shall be delivered to the competent authority without delay, as prescribed by section 21 of the Act. This applies to ordinary paper documents and electronic documents alike.

Language Act

The purpose of the Language Act is to guarantee every citizen's right to a just trial and to good administration, irrespective of his or her language, and that the individual's linguistic rights are implemented without having to appeal to them separately. This requirement applies to conventional

communication methods and electronic business alike. According to section 27 of the Act, correspondence between the state authorities shall take place in the Finnish language, unless the sending or receiving authority is exclusively Swedish-speaking, or if it is not otherwise more appropriate to use Swedish or any other language. However, the Act prescribes certain situations where the recipient's language shall be used.

Act on Electronic Services and Communications in the Public Sector

The purpose of the Act on Electronic Services and Communications in the Public Sector (13/2003) is to increase the fluency and speed of business by promoting the use of electronic data transfer methods. In addition, the Act contains several special regulations concerning electronic business.

As a term, electronic data transfer methods refers to electronic forms, e-mail and licences that have been granted for the use of electronic information systems, in other words, technology-based fixed line connections to information systems. The Act prescribes the rights, duties and responsibilities of authorities and their clients in electronic business. The law in question is applied to the institution of proceedings for matters, to their handling, and to the publication of related decisions.

The law implies that e-mail messages are equivalent to letters delivered to authorities, and to other contacts made on paper. The judicial status of a message depends on its content. The crucial aspect is whether the matter in question belongs to the jurisdiction and tasks of the addressed authority or not.

In accordance with the law, an authority that possess the required technical, financial or other pertinent capacity, shall, within the limits thereof, provide everyone with the opportunity to send a message to an electronic address, or to a defined device, to institute and conclude proceedings in his or her case. Furthermore, all people shall be provided with the opportunity to electronically send prescribed notices and required announcements to authorities. The same applies to any reports and similar documents requested by authorities, and to any pertinent messages in general.

In accordance with the law, authorities shall endeavour to use such hardware and software that is technically as compatible and easy-to-use as possible from the client's point of view. Authorities are obliged to ensure sufficient information security in electronic business and in mutual information exchange between authorities.

In accordance with the law, the sender is responsible for the arrival of a document in electronic business (section 8). The sender's legal status is secured here by the fact that the law prescribes the authority in question to acknowledge the receipt of an electronic document and to inform the sender without delay accordingly (section 12). The announcement can be

delivered through an information system as an automatic receipt, or by using other methods. According to section 21 of the Act, an electronic document must be filed in such a manner that its originality and content are retained unchanged as can be verified at a later stage.

Section 9 of the Act sets out the signature requirements. According to this section, an electronic document, which has been received by an authority, does not need to be supplemented by a signature, provided that the sender information is included in the document, and that there is no doubt regarding the document originality or integrity. In cases where a separate signature is not required in accordance with the law, the requirement will be fulfilled by an electronic signature referred to in section 18 of the Act on Electronic Signatures (14/2003).

In accordance with the Act, electronic business may be arranged in the best possible manner from the point of view of the authorities. The use of e-mail is an option. The problem with the e-mail system is the increasing number of disturbing messages. The elimination of this problem has not been possible through statutory regulations. Due to information security problems and message filtering requirements, the use of e-mail in electronic business is not problem-free. According to the principle of good administration, the accessibility of authorities must be secured.

Act on the Openness of Government Activities

The Act on the Openness of Government Activities (621/1999) prescribes the publicity of authorities' documents, everyone's right to access information, and authorities' responsibilities to implement openness and good information management in their activities. The Act also includes regulations on the grounds for information secrecy, plus the general grounds and preconditions for disclosing secret information.

In the use of e-mail, it should be borne in mind that a message written or received through e-mail may also be a document of an authority, as referred to in the law, provided that the information in question belongs to the authority's activities and jurisdiction. According to the law, authorities' documents are those in the possession of an authority, those drawn up by authorities or their employees, or those submitted to an authority for processing a matter, or submitted otherwise to an authority on a matter under their jurisdiction. In addition, any documents which have been drawn up on an assignment given by an authority are also regarded as documents drawn up by authorities. A document submitted to an authority is one that is submitted to an authority as an assignment, or to a party working for the authority for the execution of the assignment in question.

On the other hand, letters or other documents that are submitted, for example, to people employed by an authority, or to other people in a position of trust, because of their other tasks, or due to their position, are not regarded as authorities' documents. The same applies to any

documents acquired for authorities' internal training, information retrieval or any other comparable internal use.

From the point of view of information contained in e-mail, the application of the law implies the obligation to consider the viewpoints that are related to the publicity, storing and secrecy of the information/document in question.

Section 18 of the Act contains regulations on authorities' responsibilities to guarantee good information management. Authorities shall ensure the appropriate accessibility, availability, protection, integrity and any other quality-related factors pertaining to documents and information systems, and to the information contained therein. Among other things, this includes the obligation to clarify the effect of measures being carried out on the publicity, secrecy, protection and quality of documents, when introducing new information systems and preparing administrative and legislative reforms. Authorities must design their document management, information and knowledge management, information systems, information handling and data processing procedures in a fashion that enables and secures the publicity of documents, the filing of information system contained information, and their appropriate disposal.

Good information management also includes several other duties relating to document administration. The Decree on the Openness of Government Activities and on Good Practice in Information Management (1030/1999) contains detailed regulations on the publicity of authorities' activities and on good practice in information management. According to the Act, authorities are obliged to assess and clarify the significance of their documents and information systems, and that of the information stored therein. In addition to paper documents, this obligation applies to any information existing in an electronic form.

Archives Act

The Archives Act (831/1994) applies to Parliament, the State Auditors' Office, the Parliamentary Ombudsman's Office, and to the State Audit Office, only in terms of the regulations set out in its sections 6 and 7, plus section 8, subsections 2 and 1. Section 6 of the Act specifies the archive materials. In this Act, any presentations, which are created through the use of electronic or other comparable means in a form that can be read, heard, or otherwise understood with the aid of technical devices, are referred to as documents, in addition to conventional paper documents.

Act on the Protection of Privacy in Working Life

The Act on the Protection of Privacy in Working Life (759/2004; entered into force on 1st October 2004) contains regulations on retrieving and opening an employee's e-mail. The regulations set out in section 6 of the Act ensure, on the one hand, the secrecy of an employee's confidential

messages, and, on the other hand, the employer's access to any messages which belong to the employer and which are necessary from the point of view of uninterrupted operations, during the employee's absence.

When passing this law, Parliament pointed out that it is necessary to inform users of the problems relating to the e-mail system reliability, when organising the required forthcoming training. The acceptance of the regulations concerning the retrieval and opening of e-mail must not lead to a situation where functions which are central from the point of view of the employer's activities are increasingly based on e-mail, such as the transmission and reception of invitations to tender and quotations. In general, any messages that are intended for the employer shall primarily be directed to official or joint e-mail addresses of the workplace or unit in question. This means that any messages that are essential for the employer's activities will always be read by more than one person. This also eliminates the need for retrieving and opening of an employee's e-mail messages during his or her absence.

The purpose of this regulation is to steer the existing practice towards a situation where the opening of any messages, which are sent to or by an employee, and which belong to the employer, would be based on the employee's consent. The last resort is the opening of messages which belong to the employee in accordance with the statutory procedures.

Under the preconditions prescribed in the law, an employer may retrieve or open e-mail messages that are sent to or by an employee, only provided that the necessary measures have been carried out to protect the messages in question. The protection obligation also presupposes that the employee has an automatic e-mail response function available during his or her absence, and a substitute, or that the employee can direct the messages to a person approved by the employer, or to an alternative address. Alternatively, an employee may consent that a person accepted by him or her, and by the employer, receives the messages in question in order to clarify whether any of them are required in terms of work arrangements and clearly belong to the employer.

In cases where the employer's protection obligations are fulfilled, the person in question may retrieve and open an electronic message that belongs to the employer, provided that the statutory procedure is observed. The information concerning the message sender, recipient or the message header is to be used to clarify whether any messages have been sent to the employee during his or her absence, and whether he or she transmitted or received any messages, immediately prior to his or her absence, which belong to the employer. The requirement is that the employee in question handles work-related tasks independently on the employer's account and that the transmitting or receiving of messages of this type is, undisputedly, part of his or her work. Furthermore, it is required that the employee is temporarily incapacitated from carrying out his or her tasks, and that the

employer cannot otherwise obtain the message-contained information. In addition, it is required that contacting the sender has not been possible to clarify the message content, so as to forward it to an employer-provided address.

In cases where the employee has died or has been otherwise permanently prevented from carrying out his or her work-related duties, the employer shall have the right, under similar preconditions, and on the basis of corresponding information, to clarify whether any message belongs to the employer, provided that clarifying the employee's work-related tasks, or safeguarding the employer's activities is not possible by any other means.

The employer may open a retrieved message, provided that the message sent to or by the employee obviously belongs to the employer. Clarification of the message content has to be necessary for the employer, so as to conclude business-related negotiations, to serve customers, or to secure on-going operations. A message must be opened by a person with the information system administrator's authorisation in the presence of another person.

In accordance with the law, a report must be drawn up pertaining to the opening or retrieval of a message. The report is to include the names of the persons who participated in the event, their signatures, why the message was retrieved/opened, the event date and time, plus the names of persons informed of the opened message content. The report must be delivered to the employee without delay. The handling of the information must be restricted to the minimum required. In addition, those who have dealt with the information in question must not disclose it to outsiders during their employment or their post-employment period.

Act on the Protection of Privacy in Electronic Communications

The purpose of the Act on the Protection of Privacy in Electronic Communications (516/2004) is to safeguard confidentiality and implement the protection of the privacy. The intention is to promote information security in electronic communication, the well-balanced development of versatile electronic communication services. The Act uses the "message" concept in reference to telephone calls, e-mail messages, SMS messages, voice mail and other similar messages that are transmitted between information network parties, or sent to freely selectable recipients. Information security has been defined to consist of those administrative and technical measures that secure that information is available to only those who are entitled to it, and that information cannot be changed by those who are not entitled to it, and that information and information systems are available to and exploited by authorised parties.

In accordance with the law, any messages, including their identification data and geographic information, are confidential. If a message has been made to be received by the public at large, the information in question is

not considered confidential, however. The protection of confidentiality also extends to the identification information accumulating from the browsing of Internet pages.

The statutory regulations on professional secrecy and utilisation prohibition imply that a person who has received information concerning a confidential message, or its identification data, is not allowed to disclose or exploit the message content, its identification data, or the information concerning the existence of the message in question without the communicating party's consent, or without the justification prescribed in the law. The same also applies to geographic information. Professional secrecy and the utilisation prohibition also apply to those who are or have been employed by telecommunications companies, providers of value added services, community subscribers or telecommunications contractors, and to any other parties who work or have worked for them.

In accordance with the law, the protection of messages and their identification data is permitted by using available technical means and methods. However, protection implementation must not disturb the implementation or use of network-based services or communication services. To protect this procedure, the law prohibits the import, manufacture and distribution of systems which may be used to eliminate the technical protection of electronic communication. The possession of such a system is also illegal.

The law separately allows the handling of messages and their identification data in specific situations, for example, for service implementation and development purposes, to develop the processing technology, and for fault detection and troubleshooting purposes. However, this does not provide any right to access and clarification of the message content.

The law prescribes the obligation of telecommunications companies and providers of value added services to arrange information security for their services. Community subscribers must arrange information security for their users' identification data and geographic information. In this connection, the arrangements' technical level, costs, and any serious threats must be taken into account.

Responsibility for the statutory general control and development rests with the Ministry of Transport and Communications, in addition to which the Finnish Communication Regulatory Authority's supervision tasks have been prescribed. The Act on the Protection of Privacy in Electronic Communications also contains regulations on coercive measures, a reference provision to the Penal Code and a penal provision for the breach of information security in electronic communication.

Penal code

The punishments for the breach of communication secrecy are prescribed in chapter 38 of the Penal Code (39/1889). According to section 3 of this chapter, a person who unlawfully opens a letter or any other closed message addressed to another person, or hacks into the contents of an electronic or other technically recorded message which is protected from outsiders, shall be punished. In addition, anyone who obtains information on the contents of a call, telegram, transmission of text, images or data, or another comparable telemessage or the transmission or reception of such a message, may be condemned for message interception. The chapter also contains regulations on aggravated message interceptions.

Section 8 of the chapter contains regulations on computer break-ins. A person who by using an unauthorised access code or by otherwise breaking a protection unlawfully hacks into a computer system where data is processed, stored or transmitted electronically or in a corresponding technical manner, or into a separately protected part of such a system, shall be sentenced for a crime. A person shall also be sentenced for a computer break-in if he without hacking into the computer system or a part thereof, by using a special technical device unlawfully obtains information contained in a computer system.

Advisable to know and remember concerning information security!

- ü All information users are personally responsible for information security.
- ü Information security is also a means of ensuring that public information is correct, up-to-date and available.
- ü Never away your username and password.
- ü Never write your password down.
- ü Never use a password that is easy to guess, such as your spouse's or child's name.
- ü Always save any important information in your home directory on the H disk drive.
- ü Avoid unnecessary paper copies.
- ü Internet-provided information is not always correct – always ensure the correctness of information.
- ü Internet-provided information may be copyrighted – ensure that it is legal to use the information in question.
- ü Whenever users access a site on the Internet, they invariably generate an entry in the page log files.
- ü There is a separate instruction concerning the handling of e-mail, in addition to which, any other pertinent special instructions must be considered when handling information.

Advisable to know and remember concerning e-mail!

- ü Remember to use good manners when using e-mail.
- ü E-mail is a written document which can be dealt with and duplicated by others at later stage.
- ü There is no cancel function available in external e-mail transmissions.
- ü Respect the recipient's mailbox. Do not send chain letters, Christmas greetings or joke messages in internal e-mail.
- ü E-mail is like an open note on the Internet – anybody can read it.
- ü Always write the e-mail address exactly right, otherwise the message can go to the wrong person or it may disappear.
- ü On the Internet, it is possible to send an e-mail in anybody's name.
- ü E-mail is intended for the transmission of messages and for their short-term storage. Computer programs and large information materials are to be conveyed by other methods.
- ü The arrival or response times of e-mail cannot be guaranteed. To ensure the arrival of e-mail, ask the recipient to acknowledge receipt.