MINISTRY OF FINANCE

Tiedonhallintalautakunta
Informationshanteringsnämnden

Recommendation on the handling of classified documents

Board

Publications of the Ministry of Finance – 2021:8

Publications of the Ministry of Finance 2021:8

Recommendation on the handling of classified documents

Information Management Board

Ministry of Finance Helsinki 2021

Publication sale

Online bookstore of the Finnish Government

vnjulkaisumyynti.fi

Publication distribution

Institutional Repository for the Government of Finland Valto

julkaisut.valtioneuvosto.fi

Ministry of Finance

ISBN pdf: 978-952-367-512-4
ISSN pdf: 1797-9714

Layout: Government Administration Department, Publications

Helsinki 2021 Finland

Description sheet

11 February 2021

Recommendation on the handling of classified documents

Publications of the Ministry of Finance 2021:8		**Subject**	Board
Publisher	Ministry of Finance		
Group Author	Information Management Board		
Language	English	**Pages**	77

Abstract

Under section 18 of the Act on Information Management in Public Administration, authorities operating in ministries, government agencies, public bodies and unincorporated state enterprises, along with courts of law and boards established to handle appeals shall security classify documents and mark them with a security classification to indicate the information security measures to be complied with when handling the documents. A security classification marking shall be applied if the document or information contained within it is secret on the basis of section 24, subsection 1, paragraphs 2, 5 or 7–11 of the Act on the Openness of Government Activities and the unauthorised disclosure or unauthorised use of the information contained in the document could prejudice national defence, preparedness for exceptional circumstances, international relations, combating of crime, public safety or the functioning of government finances and the national economy, or the safety of Finland in some other comparable manner.

The purpose of the recommendation is to support the work of authorities which use the security classifications.

The Information Management Board approved the recommendation on 11 February 2020, and this second, updated publication on 18 December 2020.

Keywords Information Management Unit, Information Management Act, advisory boards, information management, public administration, responsibilities, definitions

ISBN PDF	978-952-367-512-4	**ISSN PDF**	1797-9714
URN address	http://urn.fi/URN:ISBN:978-952-367-512-4		

Kuvailulehti

11.2.2021

Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä

Valtiovarainministeriön julkaisuja 2021:8		**Teema**	Lautakunnat
Julkaisija	Valtiovarainministeriö		
Yhteisötekijä	Tiedonhallintalautakunta		
Kieli	Englanti	**Sivumäärä**	77

Tiivistelmä

Julkisen hallinnon tiedonhallinnasta annetun lain 18 §:n mukaan valtion virastoissa, laitoksissa ja valtion liikelaitoksissa toimivien viranomaisten, tuomioistuimien ja valitusasioita käsittelemään perustettujen lautakuntien on turvallisuusluokiteltava asiakirjat ja tehtävä niihin turvallisuusluokkaa koskeva merkintä sen osoittamiseksi, minkälaisia tietoturvallisuustoimenpiteitä asiakirjaa käsiteltäessä noudatetaan. Turvallisuusluokkaa koskeva merkintä on tehtävä, jos asiakirja tai siihen sisältyvä tieto on salassa pidettävä viranomaisten toiminnan julkisuudesta annetun lain 24 §:n 1 momentin 2, 5 tai 7–11 kohdan perusteella ja asiakirjaan sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa maanpuolustukselle, poikkeusoloihin varautumiselle, kansainvälisille suhteille, rikosten torjunnalle, yleiselle turvallisuudelle tai valtion- ja kansantalouden toimivuudelle taikka muulla niihin rinnastettavalla tavalla Suomen turvallisuudelle.

Suosituksen tavoitteena on tukea turvallisuusluokitusta käyttäviä viranomaisia.

Tiedonhallintalautakunta hyväksyi suosituksen 11.2.2020, ja tämän toisen, päivitetyn julkaisun 18.12.2020.

Asiasanat	tiedonhallintalaki, tiedonhallintalautakunta, lautakunnat, tietoturva, julkinen hallinto, luokitukset, asiakirjat, tieto, suositus		
ISBN PDF	978-952-367-512-4	**ISSN PDF**	1797-9714
Julkaisun osoite	http://urn.fi/URN:ISBN:978-952-367-512-4		

Presentationsblad

11.2.2021

Rekommendation om behandling av säkerhetsklassificerade handlingar

Finansministeriets publikationer 2021:8		**Tema**	Nämnder
Utgivare	Finansministeriet		
Utarbetad av	Informationshanteringsnämden		
Språk	Engelska	**Sidantal**	77

Referat

Myndigheter vid statliga ämbetsverk och inrättningar, statliga affärsverk, domstolar och nämnder som har inrättats för att behandla besvärsärden ska enligt 18 § i lagen om informationshantering inom den offentliga förvaltningen säkerhetsklassificera handlingar och förse dem med anteckning om säkerhetsklass som visar vilket slag av informationssäkerhetsåtgärder som ska vidtas vid behandlingen av dem. Anteckning om säkerhetsklass ska göras, om en handling eller informationen i den är sekretessbelagd enligt 24 § 1 mom. 2, 5 eller 7–11 punkten i lagen om offentlighet i myndigheternas verksamhet och om obehörigt avslöjande eller obehörig användning av handlingen kan orsaka skada för försvaret, för förberedelser inför undantagsförhållanden, för internationella relationer, för brottsbekämpningen, för den allmänna säkerheten eller för stats- och samhällsekonomins funktion, eller på något annat jämförbart sätt för Finlands säkerhet.

Syftet med rekommendationen är att stödja myndigheter som använder säkerhetsklassificering.

Informationshanteringsnämnden godkände rekommendationen den 11 februari 2020 och denna uppdaterade publikation den 18 december 2020.

Nyckelord informationshanteringslagen, informationshanteringsnämnden, nämnder, informationssäkerhet, offentlig förvaltning, klassificeringar, handlingar, information, rekommendation

ISBN PDF	978-952-367-512-4	**ISSN PDF**	1797-9714
URN-adress	http://urn.fi/URN:ISBN:978-952-367-512-4		

Contents

1 Introduction

This Recommendation of the Information Management Board was prepared in the division of security classified documents appointed by the Board for a term running from 1 April 2020 to 31 December 2021. The division is chaired by Senior Ministerial Adviser Tuija Kuusisto of the Ministry of Finance and Chief Senior Specialist Tuula Seppo of the Digital and Population Data Services Agency served as secretary to the division. The Information Management Board appointed the members of the division from among experts in the various information management entities. In addition, at its meetings, workshops and seminars the division also widely consulted outside experts. The draft Recommendation was made available for comments via the Lausuntopalvelu public service for online consultation between 23 November and 4 December 2020.

The Act on Information Management in Public Administration (906/2019, Information Management Act) lays down provisions on the responsibilities relating to information security measures of public administration information management entities and authorities as well as private individuals and corporations or corporations subject to public law other than those serving as authorities insofar as they perform public administrative tasks. The Act also lays down provisions on the minimum standard of information security measures. Section 18 of the Information Management Act lays down provisions on the obligation of authorities operating in State agencies and institutions, the courts of law and committees established to handle appeals to security classify certain documents.

The Government Decree on Security Classification of Documents in Central Government (1101/2019, hereinafter Security Classification Decree) lays down provisions on the security classification of the documents referred to in section 18 of the Information Management Act, the markings to be made in documents to be classified and the information security measures related to the handling of classified documents in central government authorities.

This Recommendation serves as a guide to information management entities and authorities in the implementation of the information security requirements laid down in the Security Classification Decree. The Recommendation is intended to support the authorities using security classifications. It provides advice on how to assess the need for and degree of security classification and the risks relating to the information to be classified as well as how to pay attention to the protection of information at all stages

of its handling in different areas and throughout the lifecycle of the information. The Recommendation contains relevant practical examples and means of implementation. In addition, it provides advice to recipients of classified information on the appropriate handling of the information. When making use of the Recommendation, it must be noted that the requirements of the Decree may be fulfilled in many different ways and the authority's risk management plays a key role when choosing among them.

Under the Information Management Act, information security measures shall be assessed on a risk basis. When assessing the implementation of information security measures for *secret* information, utilisation of the recommendations concerning documents at security classification level IV described in this Recommendation is recommended. The aim of this approach is for the requirements on the handling of secret documents to be consistent with those concerning documents at security classification level IV. This approach avoids needing separate information systems for a single purpose so as to handle secret documents and documents at security classification level IV, for example multiple case management systems for use by all personnel at an agency. On the other hand, it also avoids the accidental handling of documents at security classification level IV in information systems that do not fulfil the requirements for such documents. When assessing information security measures in respect of secret information, the recommendations concerning documents at security classification levels I–III may also be utilised on a case-by-case basis. Unless otherwise provided, documents that are secret on the basis of section 24 of the Act on the Openness of Government Activities and the information contained in such documents shall constitute secret official documents. A security classification shall be performed when a document or the information contained therein is secret on the basis of section 24, subsection 1, paragraphs 2, 5 or 7–11 of the Act on the Openness of Government Activities. The additional requirement applies that the unauthorised disclosure or unauthorised use of the information contained in the document can cause prejudice to national defence, preparedness for exceptional circumstances, international relations, combating of crime, public safety or the functioning of government finances and the national economy or to the safety of Finland in another comparable manner.

In the application of the Security Classification Decree, the other key statutes relating to security classification and secrecy shall also be taken into account. Provisions on matters including the publicity of official documents, grounds for secrecy and obligations relating to the provision of documents are laid down in section 12 of the Constitution of Finland (731/1999) and in the Act on the Openness of Government Activities (621/1999).

Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation) and the Data Protection Act (1050/2018) that supplements it contain provisions on the processing of personal data and on non-disclosure obligations.

The Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018) contains provisions on matters including the processing of personal data in the context of preventing, detecting or investigating criminal offences or referring them for consideration of charges and safeguarding against, and preventing threats to, public security. In addition to the recommendations appearing in this Recommendation, a central government authority shall also take into account all other specific regulation relating to its activities and the processing of personal data. The Office of the Data Protection Ombudsman is a national supervisory authority which supervises the compliance with data protection legislation (tietosuoja.fi).

Provisions on the secrecy obligation of a document classified in accordance with international information security obligations and on the implementation of international information security obligations are laid down in the Act on International Information Security Obligations (588/2004). The National Security Authority (NSA) has issued guidelines on the processing of international classified information [in Finnish] (Ministry for Foreign Affairs NSA 2020).

This current document is the second version of the Recommendation initially issued by the Information Management Board in 2020.

2 Points of departure for security classification

In this Recommendation, classified document means the documents referred to in section 18, subsection 1 of the Information Management Act. The obligation to security classify documents applies to the authorities operating in State agencies and institutions, the courts of law and committees established to handle appeals.[1]

2.1 Basis for security classification

While a classified document is always secret, a secret document is not always classified. A security classification shall be performed when a document or the information contained therein is secret on the basis of section 24, subsection 1, paragraphs 2, 5 or 7–11 of the Act on the Openness of Government Activities. The additional requirement applies that the unauthorised disclosure or unauthorised use of the information contained in the document can cause prejudice to national defence, preparedness for exceptional circumstances, international relations, combating of crime, public safety or the functioning of government finances and the national economy or to the safety of Finland in another comparable manner.[2]

A security classification marking may not be used in cases other than those referred to in subsection 1 unless the making of the marking is necessary to implement an international information security obligation or unless the document is otherwise connected to international cooperation. Documents referred to in the Act on International Information Security Obligations (588/2004) shall be marked with a security classification as provided in said Act.

1 See Information Management Act, section 18, subsection 1.

2 Section 3 of the Security Classification Degree describes the kinds of harm that the unauthorised disclosure or unauthorised use of a document or information contained in it may cause at each security classification level.

2.2 Assessment of security classification level

The security classification level of a document is based on assessment of the harm arising from its unauthorised disclosure. In assessing the harm required for security classification, account shall be taken of factors including the following:

- which protected interest mentioned in law is subject to the harm
- what is the extent, magnitude and duration of the estimated harm
- what are the impacts of the estimated harm
- whether risks arise from the aggregation of documents ('aggregate effect')
- what kinds of threat factors affect the potential materialisation of the harm.

Section 3, subsection 1, paragraphs 1–4 of the Security Classification Decree describes how documents that are to be classified are divided into the different classification levels:

1. documents at security classification level I, where the unauthorised disclosure or unauthorised use of the secret information contained in the document can cause exceptionally grave prejudice to the interests to be protected that are referred to in section 18, subsection 1 of the Information Management Act.
2. documents at security classification level II, where the unauthorised disclosure or unauthorised use of the secret information contained in the document can cause significant prejudice to the interests to be protected that are referred to in section 18, subsection 1 of the Information Management Act.
3. documents at security classification level III, where the unauthorised disclosure or unauthorised use of the secret information contained in the document can cause prejudice to the interests to be protected that are referred to in section 18, subsection 1 of the Information Management Act.
4. documents at security classification level IV, where the unauthorised disclosure or unauthorised use of the secret information contained in the document can be disadvantageous to the interests to be protected that are referred to in section 18, subsection 1 of the Information Management Act.

It is recommended that authorities assess the requirement of harm in advance on a risk basis so as to accomplish consistency in classification. The risk assessment shall take into account the harm possibly arising to the interests to be protected from the unauthorised disclosure or unauthorised use of the information. Every attempt should be made to estimate the consequences in concrete terms, taking into account the interest to be protected as a whole.

In individual cases, it may be possible that while the information is secret on the basis of section 24, subsection 1, paragraphs 2, 5 or 7–11 of the Act on the Openness of Government Activities, its unauthorised disclosure or unauthorised use is not capable of harming the safety of Finland in the manner described in section 18 of the Information Management Act or in a comparable manner. In such an event, the marking **SALASSA PIDETTÄVÄ** shall be used. Although this may apply in individual cases, as a rule, when the requirement of harm clause in section 24, subsection 1, paragraphs 2, 5 or 7–11 concerning secrecy is fulfilled, the requirement of harm under section 18 of the Information Management Act may also be deemed to be fulfilled.

In the interests of avoiding over- and under-classification, an organisation shall be familiar with the special regulation related to its particular field and attend to the strengthening of the secrecy and security classification regulation capacities of its personnel. The organisation shall ensure that documents are duly security classified. The management of an information management entity shall attend to the determination of information management responsibilities, guidance and instructions, training, proper tools and supervision (Information Management Act, section 4). The recommendation of the Information Management Board addresses in more detail the implementation of management responsibilities in information management [in Finnish] (Ministry of Finance 2020:18).

The information shall be classified by the person who gives the commission relating to the matter or first generates the information, or by the person who in the capacity of decision-maker on the matter decides on the classification of the document. The person who classifies the information assesses the potential secrecy of the information and the provision on which the secrecy is based. When the information is secret on the basis of section 24, subsection 1, paragraphs 2, 5 or 7–11 of the Act on the Openness of Government Activities and the unauthorised disclosure or unauthorised use of the information can cause prejudice to national defence, preparedness for exceptional circumstances, international relations, combating of crime, public safety or the functioning of government finances and the national economy or to the safety of Finland in another comparable manner, the information constitutes information that is to be classified. With regard to a document that contains information that is to be classified, the degree of potential harm shall be assessed and the security classification level marking shall be made according to the degree of harm. Annex 1 describes the secrecy and security classification assessment process relating to this assessment (the Act on International Information Security Obligations is not taken into account in the flow chart). The table appearing as Annex 2 provides examples for assessing the harm required for security classification from the viewpoint of the interest to be protected.

The classification shall always be performed on a case-by-case basis on the basis of the risk assessment. The effect of combining information and the aggregate effect shall be taken into account in risk assessment and in the dimensioning of information security measures in the handling of the information, as these may heighten the risks and necessitate information security measures on the basis of the risk assessment. For example, when two pieces of information at security classification level TL IV are combined, the end result may fall at levels TL I–IV depending on the outcome of the combination. The aggregate effect is discussed in more detail in chapter 5.3.

In the performance of a commissioned task, the documents prepared in consequence of the commission shall be considered, as a rule, official documents of the commissioning authority as provided in section 5 of the Act on the Openness of Government Activities. The provisions of the Act on the Openness of Government Activities (or other provisions) shall apply to the secrecy of such documents and, under section 14 of the said Act, the decision on granting access to such documents shall, as a rule, be made by the commissioning authority. With regard to documents that are to be classified, it is recommended that security classification be separately agreed in commissioning situations when the handling of documents that are to be classified is anticipated. For example, when a private enterprise performs a task, such as the design and production of software or a piece of equipment, on commission from a central government authority subject to an obligation to security classify and information and documents that are to be classified arise during the performance of the task, the commission agreement should provide that the commissioned party classifies the documents arising in the commission relationship in the manner agreed with the commissioning party. Security classification in general and the level of security classification in respect of certain types of information should be agreed at least broadly. In such a case, it may also be held that the authority subject to an obligation to security classify made the original decision on classification of information relating to the matter and then instructs the commissioned party to comply with the decision.

2.3 International equivalence of security classification levels

The documents referred to in the Act on International Information Security Obligations constitute datasets subject to special protection and shall be classified in the manner determined in the said Act. The information referred to in the Act means classified information of other States or international organisations. Section 4 of the Security Classification Decree lays down provisions on the equivalents of Finnish security classifications in fulfilling international information security obligations. Unless otherwise

provided in the international information security obligation, the provision shall be complied with. The National Security Authority (NSA) has issued separate guidelines on the processing of international classified information. The national and EU security classification levels and their abbreviations are given side by side in the table below. The rules of handling are different for the different levels and the security rules for protecting EU classified information (EUCI) shall be complied with when handling documents at the EU security classification levels. [3]

Table 1. Security classification levels and their abbreviations and EU equivalents

National security classification level				EU classification	
Security classification level I	TL I	ERITTÄIN SALAINEN	(E)	TRÈS SECRET UE/ EU TOP SECRET	TS-UE/ EU-TS
Security classification level II	TL II	SALAINEN	(S)	SECRET UE/ EU SECRET	S-UE/ EU-S
Security classification level III	TL III	LUOTTAMUKSELLINEN	(L)	CONFIDENTIEL UE/ EU CONFIDENTIAL	C-UE/ EU-C
Security classification level IV	TL IV	KÄYTTÖ RAJOITETTU	(R)	RESTREINT UE/ EU RESTRICTED	R-UE/ EU-R

3 See European Council security rules (2013/488/EU)

3 Marking the security classification level

3.1 Marking methods

The security classification level marking indicates the information security measures that are to be complied with in handling the document. When there are no grounds for classifying the document, the security classification marking may not be used. The basis for secrecy shall be recorded on the marking.

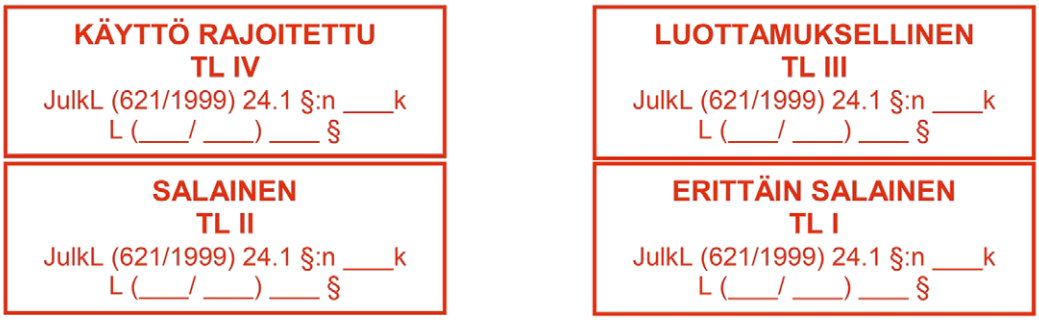
The provisions on security classification markings are laid down in section 3, subsections 2–5 of the Security Classification Decree. There are four security classification levels and corresponding markings:

- documents at security classification level I are marked ERITTÄIN SALAINEN,
- documents at security classification level II are marked SALAINEN,
- documents at security classification level III are marked LUOTTAMUKSELLINEN, and
- documents at security classification level IV are marked KÄYTTÖ RAJOITETTU.

In addition to the said markings, the markings TL I; TL II; TL III; and TL IV may be used.

Documents at security classification levels I–IV shall be marked according to the model in Figure 1 with the stamp of the relevant security classification level and, when necessary, they shall also be also stamped *salassa pidettävä* to indicate secrecy. The legislative basis for secrecy shall be recorded on the document and in the metadata. Secrecy markings are based on the Act on the Openness of Government Activities and are therefore beyond this Recommendation's scope of guidance.

Figure 1. Model stamps for security classification markings



The security classification level shall be marked in Swedish in documents prepared in the Swedish language or translated into Swedish. The marking may also be made in other cases when the authority deems it necessary. In Swedish, documents at security classification level I are marked YTTERST HEMLIG; documents at security classification level II are marked HEMLIG; documents at security classification level III are marked KONFIDENTIELL; and documents at security classification level IV are marked BEGRÄNSAD TILLGÅNG.

The security classification level of a document shall also be indicated in the information on the document in the case register referred to in section 25 of the Information Management Act and in another information pool generally used by an authority for information management.[4] The marking may be made on a separate document to be attached to the document if it is not technically feasible to make markings on a document or to modify the marking or if the handling requirements corresponding to the security classification level are needed only for a certain short period.[5]

The document shall clearly indicate the parts of the document which contain classified information. Individual paragraphs, chapters or annexes may be marked e.g. by using the security classification level abbreviations (E), (S), (L) or (R) before the paragraph, chapter or annex. When the same security classification level applies to all parts of the document, these parts may be marked with brackets, in which case the text *hakasulkeilla merkitty teksti on salassa pidettävää ja turvallisuusluokan X tietoa* shall appear at the beginning of the document to indicate that all text within brackets is secret and at security classification level X.

4 See Security Classification Decree, section 3, subsection 4.

5 See Security Classification Decree, section 3, subsection 5.

The security classification level of information may also be stated orally when classified information is addressed at e.g. meetings. In common international practice, the security classification level, page number and date is clearly recorded on each page. For documents at security classification levels III–I, the number of the copy is also often recorded on each page when the document is to be distributed in more than one copy. These practices are recommended for nationally classified documents as well.

3.2 Removal and modification of marking

If there are no longer legal grounds for the security classification of a document or if it is necessary to modify the security classification level, an appropriate marking of the removal or modification of the marking shall be made on the document on which the original marking was made and in the information on the document referred to in section 3, subsection 4 of the Security Classification Decree. The appropriateness of the marking shall be checked at the latest when providing a third party access to the document (Security Classification Decree, section 5, subsection 1).

The following steps shall be taken when modifying the classification of a document:

- Where the document is in paper format, the stamp indicating security classification level or secrecy shall be crossed out.
- The text salassapito päättynyt shall be written below the stamp to indicate that secrecy has expired, and the text shall be accompanied by the date and the signature of a competent public official.
- The changed status of the document to public shall also be recorded in the document register.
- Where the document is in electronic format, the marking is accomplished by modifying the metadata, and e.g. documents subject to request for information shall be accompanied by a separate cover message indicating the date of expiration of secrecy.
- The metadata modification shall be recorded in the document log data.

If the document has been received from another authority, the marking related to a security classification level may be removed or modified only by permission of the authority that prepared the document or by permission of the authority in charge of the handling of the matter in its entirety unless it is clear that there are no longer grounds for the use of a security classification level (Security Classification Decree, section 5). The need for a marking related to security classification with regard to filed documents

or documents stored in a central government authority shall be assessed if the central government authority takes up a document for other handling (Security Classification Decree, section 16).

3.3 Earlier classifications and markings

Documents handled in 2010–2019 during the period when the Government Decree on Information Security in Central Government, issued pursuant to the Act on the Openness of Government Activities and preceding the Security Classification Decree, was in force, shall retain their original marking until a need to re-take the document up for handling arises. In such a case, the secrecy and security classification level of the document shall be re-assessed on a case-by-case basis in accordance with the current provisions. In such a case, information classified at protection levels I–IV may be classified as secret and also given a security classification if the conditions for security classification are fulfilled. The table below is provided as an aide to re-assessment.

Table 2. Secrecy and security classification level shall be reconsidered in respect of each document.

Classifications in 2010–2019	Classification as of 2020
ERITTÄIN SALAINEN, protection level I (ST I)	ERITTÄIN SALAINEN TL I
SALAINEN, protection level II (ST II)	SALAINEN TL II
LUOTTAMUKSELLINEN, protection level III (ST III)	LUOTTAMUKSELLINEN TL III
KÄYTTÖ RAJOITETTU, Protection level III (ST III), Protection level IV (ST IV)	KÄYTTÖ RAJOITETTU TL IV
SALASSA PIDETTÄVÄ, Protection level III (ST III), Protection level IV (ST IV)	SALASSA PIDETTÄVÄ

When re-assessing the classification of information, in respect of information classified earlier at different protection levels and re-assessed to be classified as secret but not as security classified, regard shall be had to the fact that under the Information Management Act, information security measures shall be assessed on a risk basis. When assessing the implementation of information security measures in respect of secret information,

utilisation of the recommendations described in this Recommendation concerning documents at security classification level IV is recommended. When assessing information security measures in respect of secret information, the recommendations concerning documents at security classification levels I–III may also be utilised on a case-by-case basis.

4 Document handling requirements

4.1 Registration and monitoring of document handling

Under section 25 of the Information Management Act, an information management entity shall maintain a case register of matters that are being and have been considered by the authorities, into which information on the matter, its consideration and the documents shall be registered. An authority shall, without delay, register a document it has received or drafted in the case register. The case register is maintained to implement document publicity, to specify requests for information, to structure the details of documents and other corresponding details, to organise the measures relating to document handling, to monitor case processing times, and to guide processes. In addition to the provisions laid down in section 26 of the Information Management Act concerning the mandatory details to be recorded in the case register, the registration of a document shall also indicate the date of its receipt.

Provisions on the measures to be implemented for the purpose of monitoring document handling, such as registration for security purposes, are laid down in section 14 of the Security Classification Decree. When granting handling rights, regard shall be had to the requirements under section 8 of the Security Classification Decree concerning handling rights and lists thereof.

In registration, for example, the details described in section 26 of the Information Management Act shall be taken into account, subject to the clarifications described in the following.

The following shall be registered in respect of handling:

- handler (person or organisation – when not an authority) and
- date.

The following shall be registered in respect of receipt:

- original sender (organisation or person),
- recipient,
- other handler when the document is received by another (e.g. registry),
- date of receipt,
- date of registration, and
- manner of receipt (analogue/electronic).

The following shall be registered in respect of dispatch:

- original dispatcher,
- other handler when the document is dispatched by another (e.g. registry),
- recipient of dispatch,
- external recipient of dispatch (organisation or person),
- date of dispatch,
- date of registration, and
- manner of dispatch (analogue/electronic).

The action-oriented case management division under the Information Management Board is currently drafting a recommendation on the implementation of case management at information management entities and on document registration.

4.1.1 Document registration and monitoring, security classification level IV (TL IV)

Documents at security classification level IV (TL IV) shall be prepared and registered primarily with the case management system in use when this system fulfils the requirements of TL IV. The recipient organisations or persons shall be recorded in the document, cover note or in connection with the document. A document at security classification level IV shall be marked with the stamp for security classification level IV and also with the stamp *salassa pidettävä* to indicate secrecy when necessary. The legislative basis for secrecy shall be recorded on the document and in the metadata. The case management system for documents at security classification level IV is typically the same as the general case management system.

4.1.2 Document registration and monitoring, security classification level III (TL III)

Documents at security classification level III (TL III) shall be prepared with a case management system or other system that fulfils the requirements of TL III. The dispatch and receipt of a document shall be registered (Security Classification Decree, section 14). In addition, the handling of a document at security classification level III shall be monitored in an electronic log, an information system, a case register or the document itself (Security Classification Decree, section 14).

The document shall be registered and its dispatch and receipt shall be monitored in a separate electronic case register that is subject to secrecy and security classification or manually when no case register that fulfils the requirements of TL III is available. Case registers at security classification levels III–I are typically case registers separate from the security classification level IV case register and case management systems. However, case number management may be accomplished in a single case register intended for public, secret and classified case numbers. In such an event, care shall be taken not to record any secret or classified information in the metadata of this public case register or case management system.

Documents at security classification level III shall be marked with the stamp for security classification level III and also with the stamp *salassa pidettävä* to indicate secrecy when necessary. The legislative basis for secrecy shall be recorded on the document and in the metadata.

The recipient organisations or persons shall be recorded in the document, cover note or in connection with the document. A list of persons handling documents at security classification levels III shall be maintained (Security Classification Decree, section 14, subsection 1, paragraph 4). This list may, for example, be maintained on a separate cover page on which the names of the recipient of the document and the persons who have gained access to the information are recorded. When the document is returned to the registry (registration point), the details of the persons who have gained access to the information have accrued on the cover page. When a system that fulfils the requirements of security classification level III and allows electronic monitoring of handling is in use, the monitoring of persons who handled a document may be accomplished through logging or other system data.

The registration obligation only applies to information in document format. The exchange of an individual piece of information at security classification level III (e.g. conversation or brief note) which may at a later date be verified from those party to the exchange need not be registered separately. For example, the persons who have gained access to information at an event may be verified at a later date from the list of event participants.

Documents at security classification level III should primarily be handled electronically, in which case the logging performed by the case management system is often sufficient. The primary tool for manual registration of handling, dispatch and receipt shall be the case management system in which the matter in question is being considered. Handling may also be registered e.g. on a paper document or in connection with it, in which case every attempt should be made to enter the details in an electronic case register or case management system.

Since the dispatch and receipt of documents shall be registered separately for each document, no unnecessary printouts or copies of a document at security classification level III may be made to widen its distribution when the document can be handled electronically in the manner required by the matter.

Responsibility for registering any handling resides with the person handling a document at security classification level III. For example, the person who grants access to a document shall, when dispatching or copying the document, manually record the person to whom access to the document has been granted. Responsibility for the dispatch (to an external actor) and receipt (from an external actor) of a document at security classification level III resides with the dispatching party or the party entered as the recipient.

4.1.3 Document registration and monitoring, security classification level II (TL II)

Documents at security classification level II (TL II) shall be prepared with a case management system or other system that fulfils the requirements of TL II. The dispatch and receipt of such documents shall also be registered (Security Classification Decree, section 14). In addition, the handling of a document at security classification level II shall be monitored in an electronic log, an information system, a case register or the document itself (Security Classification Decree, section 14). The recipient organisations or persons shall be recorded in the document, cover note or in connection with the document.

A document at security classification level II shall be marked with the stamp for security classification level II and also with the stamp *salassa pidettävä* to indicate secrecy when necessary. The legislative basis for secrecy shall be recorded on the document and in the metadata. The registration shall indicate the persons to whom the document has been distributed.

Documents at security classification level II (TL II) shall be prepared with a case management system or other system that fulfils the requirements of TL II. The document shall be registered and its dispatch and receipt shall be monitored in a separate electronic

case register that is subject to secrecy and security classification or manually when no case register that fulfils the requirements of TL II is available.

A list of persons handling documents at security classification levels II shall be maintained (Security Classification Decree, section 14, subsection 1, paragraph 4). This list may, for example, be maintained on a separate cover page on which the names of the recipient of the document and the persons who have gained access to the information are recorded. When the document is returned to the registry (registration point), the details of the persons who have gained access to the information have accrued on the cover page. When a system that fulfils the requirements of security classification level II and allows electronic monitoring of handling is in use, the monitoring of persons who handled a document may be accomplished through logging or other system data.

4.1.4 Document registration and monitoring, security classification level I (TL I)

Documents at security classification level I shall be prepared on a separate workstation that fulfils the requirements, or manually. The dispatch and receipt of a document shall be registered (Security Classification Decree, section 14). The handling of a document at security classification level I shall be recorded in an electronic log, an information system, a case register or the document itself (Security Classification Decree, section 14, subsection 1, paragraph 1). The document shall be registered and its dispatch and receipt shall be monitored in a separate electronic case register that is subject to secrecy and security classification and fulfils the requirements of security classification level I, or manually in such a way that the requirements of security classification level I are fulfilled.

A document at security classification level I shall be marked with the stamp for security classification level I and also with the stamp *salassa pidettävä* to indicate secrecy when necessary. The legislative basis for secrecy shall be recorded on the document and in the metadata.

A list of persons handling documents at security classification level I shall be maintained (Security Classification Decree, section 14, subsection 1, paragraph 4). This list may, for example, be maintained on a separate classified cover page on which the names of the recipient of the document and the persons who have gained access to the information are recorded. When the document is returned to the registry (registration point), the details of the persons who have gained access to the information have accrued on the cover page. When a system that fulfils the requirements of security classification level II and allows the

electronic monitoring of handling in a way that no information at security classification level I is covered by the monitoring of handling, the monitoring of persons who handled a document may be done through logging or other data in this system.

4.2 Access to and receipt of documents

The requirements imposed on the processing of datasets apply throughout the lifecycle of the information. The person handling the information occupies a special role in the implementation of these requirements. Under all situations of working with the information, that person is responsible for the correct personal handling of the information with the tools indicated and approved by the employer and in compliance with the employer's instructions. Official information is characterised by the fact that a competent authority or a representative of that authority shall be identified or determined for the information. This competent authority has key responsibility for information within its competence. The provisions on the obligation of the authorities to attend to the secrecy and protection of information when disclosing secret information for the performance of a commissioned task are laid down in section 26, subsection 3 of the Act on the Openness of Government Activities. Information may only be disclosed to a party entitled to gain access to the information. Provisions on the obligation of secrecy and non-disclosure and on prohibition of use are laid down in sections 22 and 23 of the Act on the Openness of Government Activities.

4.2.1 Access to documents

A central government authority shall ensure in advance that the protection of a classified document is duly organised if the authority grants access to a classified document to a party other than a central government authority. The requirement does not apply to disclosing information on the contents of a document based on a party's right of access to information (Security Classification Decree, section 6). With regard to granting access to documents, at least the following access situations may be identified: the general grounds for granting access to secret information, granting access to another central government authority, granting access to e.g. an enterprise on the basis of a commission, and granting access to another party on the basis of a request for information.

An authority shall maintain secure procedures that allow only persons with right of access to handle classified information. The authority shall employ a verification procedure of sufficient strength, for example by requiring strong identification of persons or parties requesting service, when offering the opportunity to handle classified information.

The Act on the Openness of Government Activities governs granting access to a document that is in the possession of an authority. The classification marking of a document has no impact on the obligation of an authority to assess the publicity of the document on a case-by-case basis and individually for each document whenever someone requests access to the document on the basis of the Act on the Openness of Government Activities. Unlike classification under the Act on the Openness of Government Activities, classification under the Act on International Information Security Obligations leaves no room for discretion with regard to secrecy.

Under section 14 of the Act on the Openness of Government Activities, the decision to grant access to an official document shall be made by the authority in possession of the document unless otherwise provided in law. If access is requested to a document prepared by another authority or pertaining to a matter under consideration by another authority, the request may be forwarded to be dealt with by the authority that has prepared the document and is responsible for the consideration of the matter as a whole (Act on the Openness of Government Activities, section 15, subsection 1). If access is requested to a document which, in accordance with the Information Management Act, is required to bear a security classification marking and which has been drafted by another authority, the request shall be transferred for the consideration of the authority that had drafted the document. (Act on the Openness of Government Activities, section 15, subsection 3).

In considering a request for access, it shall be determined whether the grounds for secrecy and security classification remain in existence. The secrecy of a document depends on the point in time from which the matter is examined. A secrecy or security classification marking reflects the situation at the time of the preparation of the dataset. The possible consequences of the disclosure of the information contained in a document may change over time.

Under section 5, subsection 1 of the Security Classification Decree: If there are no longer legal grounds for the security classification of a document or if it is necessary to modify the security classification level, an appropriate marking of the removal or modification of the marking referred to in section 3 shall be made on the document on which the original marking was made and in the information on the document referred to in section 3, subsection 4. Typically, the decision to modify the security classification level is made by the official who presents the document or by the person who decides the matter. The appropriateness of the marking shall be checked at the latest when providing a third party access to the document.

4.2.2 Measures on the part of a recipient (other than central government)

The obligation to security classify applies to authorities operating in State agencies and institutions, the courts of law and committees established to handle appeals (Information Management Act, section 18). Classified materials may also be received by parties to which security classification does not apply, such as municipalities, joint municipal authorities and rescue departments, and by private parties in the performance of commissioned tasks. Chapter 2.2 contains recommendations on security classification and making security classification markings when documents that are to be classified are prepared in consequence of a commission given by an authority subject to the obligation to classify.

The recipient shall handle the document in the manner agreed (security agreement or equivalent) and in compliance with the instructions given by the authority that has granted access. The recipient shall ensure that third parties do not gain access to a classified document. A classified document is always also secret and the provisions of the Act on the Openness of Government Activities concerning secrecy, non-disclosure and prohibition of use (sections 22 and 23) and the provisions of the Information Management Act therefore naturally apply to classified materials. It is recommended that a party in receipt of information supplement its own handling guidelines with the instructions relating to the classified documents and arrange training relating to these.

Also an information management entity other than one subject to the obligation to security classify shall, under section 25 of the Information Management Act, without delay register in the document register any document of which it is in receipt or which it has prepared. The recipient of a document, for example a registry, shall check which official has the right *ex officio* to handle the document. When dispatching the document to the said official, regard shall be had to the procedures in chapter 4.4 relating to carriage of documents. When an actor other than an information management entity within the meaning of the Information Management Act is in receipt of a classified document, the actor shall check who has the right of access to the classified information and supply the document only to such persons.

4.3 Transfer of a document over a data network

Classified documents may be transferred outside the security areas of authorities or via an information system or telecommunications arrangement at a lower security level than the said security classification level only in encrypted form of sufficient reliability. If the transfer of classified documents takes place in a security area in other than a public data network and sufficient protection of the information can be implemented by physical protection measures, unencrypted transfer or encryption at a lower security level may

be used (Security Classification Decree, section 12). In order for the said section on non-encryption or encryption at a lower security level to be applicable, access to the said information by unauthorised persons must be prevented by means of physical access control. The following aspects shall be taken into consideration in the transfer:

1. When transferring classified information outside physically protected areas, for example via a public network, the material or traffic shall be protected with encryption of sufficient security.
    - For example the Internet and the MPLS networks provided by operators shall be considered public networks.
    - In practice, manners of implementation include e.g. VPN solutions between users' terminal devices and the information systems of the authority, IPSec encryption between the networks of organisations, and secure email and file encryption solutions provided to end users.
2. When transferring classified information within physically protected areas and inside a network protected at an at least equivalent level, lower-level encryption or unencrypted transfer may be used on the basis of the outcomes of the risk management process.
3. The encryption procedure processes and encryption key management processes shall have been designed and implemented. The practices and the processes shall have been described and instructed to users, who shall have been provided with training.
4. Only authorised users and processes have access to the protected data of encryption keys. The processes require at the least:
    - keys of sufficient cryptographical strength,
    - secure key distribution,
    - secure key storage,
    - regular key rollovers,
    - changing of outdated or exposed keys, and
    - prevention of unauthorised key changes.

When choosing protection solutions for the classified information of an authority, it is recommended that the choice be made primarily from among the encryption solutions approved by the Finnish Transport and Communications Agency National Cyber Security Centre (Encryption solutions approved by NCSA-FI [in Finnish] (Finnish Transport and Communications Agency Traficom 2020). It should be noted that encryption solutions must be configured and used in accordance with settings that have been assessed to be secure.

4.4 Carriage of documents

The risks relating to carriage shall be assessed and the necessary information security measures designed and implemented on a risk basis on the basis of the identified risks. Under section 13 of the Security Classification Decree, classified documents may be carried outside security areas by protecting the electronic data carriers with adequate encryption. It is up to the authority to assess the adequate encryption solution for the security classification level in question. When the data storage media has been adequately encrypted, it may be dispatched to the recipient e.g. by post. The carriage of classified documents outside the physically protected security areas of an authority shall be executed securely. The security of encryption solutions is discussed in more detail in chapter 7.11.

4.4.1 Carriage of unencrypted documents at security level IV

In the carriage of documents at security level IV, attention shall be paid to the requirements of the adequate encryption of electronic data carriers (e.g. flash drive, CD-ROM or DVD) laid down in section 13 of the Security Classification Decree. No specific requirements apply to the carriage of these, any more than to the carriage of paper documents at security classification level IV. Both may therefore e.g. be dispatched by post as ordinary packages. However, the package must bear no outward signs that it contains secret, classified information.

4.4.2 Carriage of unencrypted documents at security levels III–I

In the carriage of documents at security levels III-I, attention shall be paid to the requirements of the adequate encryption of electronic data carriers (e.g. flash drive, CD-ROM or DVD) laid down in section 13 of the Security Classification Decree. An unencrypted document at security classification levels III–I (paper or electronic format, e.g. flash drive, CD-ROM or DVD even if encrypted) shall be appropriately packaged for carriage and

carried to the recipient under continuous control, or the document shall be carried to a recipient in another safe manner approved by a central government authority whereby the confidentiality and integrity are ensured in a manner that is adequate for the said security classification level. Documents, for example, shall be carried to the recipient by a personal courier or a courier service, or be collected by the recipient. The procedure employed and the related actors shall have the approval of an authority for the carriage of documents at the security classification level in question based on a risk-basis assessment conducted by the authority.

The delivery of unencrypted documents at security classification levels III–I for carriage may be implemented within an organisation by means of a centralised function. In authorities, this is typically the registry of the authority. The said function shall have in place the necessary policies, guidelines and tools to allow the implementation of secure carriage. The internal function and the handling chain may only consist of security-cleared personnel.

For the carriage of documents at security classification levels III–I, the organisation shall have secure envelopes, secrecy envelopes or security pouches. These shall always be sealed inside an ordinary envelope. In packaging, care shall be taken to ensure that the package bears no outwards signs of it containing classified information. The outermost cover of the package shall indicate the address of the recipient authority (typically its registry) and also the return address in case the package cannot be delivered. Any indication that the package contains classified information should first appear only inside the external cover of the package. The envelope or package shall be non-transparent.

In internal distribution, a document may be delivered in a sealed pouch or directly to the recipient in person. The date of dispatch and the recipient shall be recorded by the dispatching organisation and the dispatching party shall monitor the delivery to ensure that it reaches its destination. The recipient shall inspect the integrity of the seal on the envelope or package and immediately report any doubt about the integrity. Advice of receipt shall be submitted to the dispatcher by returning the enclosed tracking form or by other means of tracking the delivery.

Deliveries containing information at security classification levels III–I shall primarily be made to the registry of an authority or to another party responsible for receiving deliveries and registering documents. It is recommended that the recipients of the document (by name or position) inclusive of organisation details should be recorded on the document itself in as much detail as possible.

4.5 Copying of documents

Both electronic and paper format copies may be made of classified documents, taking into account the restrictions relating to copying and the handling rules pertaining to copies as well as all other requirements concerning the handling of classified documents (e.g. information system and telecommunications arrangement requirements). Copies of documents at security classification levels II–I may not be made without the permission of the authority which prepared the document (Security Classification Decree, section 14). The permission given shall be documented in writing and it shall include a mention of the copying permission and the possible wider distribution of the document. This permission shall be attached in connection with the document in an archive into which the details of those who have gained access to the information in the document also accrue. When copies are made of documents at security classification levels II–I, a list shall be made of the copies and of the persons handling the copies (Security Classification Decree, section 14). Each copy made shall be numbered and listed.

The copying of documents at security classification levels II–I shall be implemented in a centralised manner within the organisation in compliance with specific instructions issued on the topic. The equipment used to copy paper documents shall have the approval of an authority for the copying of documents at the security classification levels in question.

4.6 Storage of information

4.6.1 Storage of information, security classification level IV (TL IV)

Information pools containing documents at security classification level IV (KÄYTTÖ RAJOITETTU; TL IV) and the information systems used to handle such documents shall be located inside a security area and paper documents at security classification level IV shall be stored inside a security area ((Security Classification Decree, section 10). Paper documents at security classification level IV shall be stored in lockable office furniture that has been assessed as appropriate for the purpose and is located inside an administrative or security area. Such documents may temporarily be stored outside a security area or administrative area when the holder of documents commits to compliance with the substitute measures laid down in the security instructions issued by the authority.

In situations where information at security classification level IV is handled and stored in a terminal device consistent with the security classification level in question that is located outside security areas, the information in the terminal device shall be protected with an encryption solution of sufficient security for the security classification level in question. In

particular, the sufficient integrity of the terminal device for the security classification level in question shall be ensured so as not to compromise confidentiality as a result of loss of terminal device integrity. The protection of information systems and telecommunications arrangements is discussed in more detail in chapter 7.

4.6.2 Storage of information, security classification levels III, II and I (TL III, TL II, TL I)

Documents at security classification level I (ERITTÄIN SALAINEN; TL I) may only be stored or otherwise handled inside a secured area (Security Classification Decree, section 10).

Documents at security classification levels III and II (LUOTTAMUKSELLINEN; TL III and SALAINEN; TL II) may be handled inside and outside security areas, however so that information pools containing documents at security classification level II or III and information systems used in the handling of these documents shall be placed in a secured area, and documents in paper form at security classification levels II and III shall be stored in a secured area (Security Classification Decree, section 10).

Paper documents at security classification levels III, II and I (TL III, TL II and TL I) shall be stored inside a secured area in a storage solution that has been assessed as appropriate for the purpose, such as a safe or a vault.

Documents at security classification levels II–III may also be handled inside and outside administrative areas by using a terminal device and telecommunications arrangement that fulfils requirements. A terminal device used to handle documents at security classification level II shall be stored inside a secured area, however. When electronic documents at security classification level III are stored in a terminal device outside secured areas, they shall be protected with an encryption solution of sufficient security for the security classification level. The information security of the terminal device shall be ensured. (Security Classification Decree, section 10) The protection of information systems and telecommunications arrangements is discussed in more detail in chapter 7.

4.7 Destruction of documents

Under section 15 of the Security Classification Decree, a classified document which is no longer required shall be destroyed in such a way that recreation and reconstruction of the information in whole or in part is prevented in a manner that is sufficiently reliable for the said security classification level. The recipient of a document shall also attend to its appropriate destruction. If the document has been prepared by another authority,

the authority that prepared the document shall be notified of the destruction of the document at security classification levels I and II that is no longer required unless it is returned to the authority that prepared the document (Security Classification Decree, section 15). The dispatching and receiving authority may agree on the practical procedures relating to notification, for example on submitting notifications relating to security classification level II on a semi-annual basis. Documents at security classification levels I and II may be destroyed only by a person assigned to this task by an authority. Any draft versions of a document may be destroyed by the person who prepared them.

Technological advances will also have an impact on the reliable destruction of classified information. Available computing capacity, for example, allows the more efficient computer-assisted reconstruction of shredded information in paper format. On the other hand, it is becoming increasingly justified to accomplish the reliable destruction of storage media for information in electronic format (hard drives, USD drives and the like) by means of e.g. melting instead of the traditional shredding.

The protection of information shall be ensured until the very end of the lifecycle of the information. This shall be taken into account especially in situations where a third-party service is used for information destruction, for example melting hard drives. In practice, the approach employed is usually a procedure in which the organisation responsible for the information supervises the information destruction process all the way to the end of the lifecycle.

The role of personnel should also be taken into account in destruction processes. Organisations shall arrange for their personnel an explicit manner of destruction of classified information. In practice, this may translate into appropriate paper shredders and ensuring the security awareness of personnel, for example.

4.7.1 Destruction by shredding, security classification level IV (TL IV)

The shredding of information at security classification level IV may be accomplished, for example, so that

- remaining paper particle size is no more than 30 mm2 (DIN 66399 / P5 or DIN 32757 / DIN 4),
- remaining magnetic hard drive particle size is no more than 320 mm2 (DIN 66399 / H-5),
- remaining SSD drive and USB drive particle size is no more than 10 mm2 (DIN 66399 / E-5), and
- remaining optical media particle size is no more than 10 mm2 (DIN 66399 / O-5).

4.7.2 Destruction by shredding, security classification level III (TL III)

The shredding of information at security classification level IV may be accomplished, for example, so that

- remaining paper particle size is no more than 30 mm2 (DIN 66399 / P5 or DIN 32757 / DIN 4),
- remaining magnetic hard drive particle size is no more than 10 mm2 (DIN 66399 / H-6),
- remaining SSD drive and USB drive particle size is no more than 10 mm2 (DIN 66399 / E-5), and
- remaining optical media particle size is no more than 5 mm2 (DIN 66399 / O-6).

4.7.3 Destruction by shredding, security classification level II (TL II)

The shredding of information at security classification level II may be accomplished so that, for example

- remaining paper particle size is no more than 10 mm2 (DIN 66399 / P6).
- remaining magnetic hard drive particle size is no more than 10 mm2 (DIN 66399 / H-6),
- remaining SSD drive and USB drive particle size is no more than 1 mm2 (DIN 66399 / E-6), and
- remaining optical media particle size is no more than 5 mm2 (DIN 66399 / O-6).

4.7.4 Destruction by shredding, security classification level I (TL I)

The particle sizes for security classification level II may be employed in the destruction of information at security classification level I when protection is augmented by procedures approved by the authority. Such procedures typically consist of methods such as the controlled further treatment of the shredded particles by means of incineration or melting.

4.7.5 Destruction using combined methods

Destruction may be executed instead of or in addition to shredding by using various other methods which are secure enough to prevent the reconstruction of destroyed information (e.g. melting hard drives). The risks to classified information can also be reduced considerably through encryption at the various stages of the lifecycles of information and equipment. The destruction of information in electronic format is described in more detail in the National Cyber Security Centre guideline on overwriting and recycling [in Finnish] (Finnish Communications Regulatory Authority 2016).

4.7.6 Destruction of information in electronic format

Especially the reliable destruction of electronic material should cover all devices which have been used to store classified information at some part of their lifecycle. Procedures shall be mutually agreed with service providers. In addition, it must be ensured that personnel are able to comply with the procedures. One has to make it sure that the individual components of devices (hard drives, memory components, solid state disks etc.) containing classified information have to be destroyed in a reliable manner especially when the device will be delivered to service, becomes obsolete, or is taken into use as a part of a recycling process. In case a reliable deletion manner (like an overwriting procedure approved by a competent authority) cannot be used, the component containing classified information cannot be delivered to a third party. In service situations where it is impossible to delete the memory content in a reliable way before the servicing, the service should be carried out under supervision in order to ensure that classified information does not end up in the hands of third parties during the service.

A security agreement shall be concluded with the organisation that carries out the servicing. Service personnel shall be designated by the service provider and security clearance shall be obtained for them before any service measures are undertaken so as to ensure the security of the service personnel and service organisation.

5 Points of departure for multi-tier protection of documents and data processing

5.1 Information management design and security design

Information management is based on the needs of the activities of the authorities. The Information Management Act creates the framework for the consistent and high-quality management of datasets. The design of information management shall take into account the different formats of datasets, the different stages of handling, the management of the information contained in the datasets, and the changes taking place in the information management entity. Provisions on an information management model and assessment of transformative impact are laid down in section 5 of the Information Management Act. When essential administrative reforms with an effect on the contents of the information management model take place or are planned or new information systems are introduced within an information management entity, it shall assess the impacts of these changes in relation to information security requirements and information security measures as well. The changed requirements shall be taken into account in the information management model. The Information Management Board's recommendation for an information management model [in Finnish] (Ministry of Finance 2020:29) provides guidance on preparing the information management model and the recommendation on the assessment of the transformative impact of information Management [in Finnish] (Ministry of Finance 2020:53) provides recommendations for performing the assessment of the transformative impact.

The central aspect of arranging information management is to design the key actions and information security measures. This design should be based on risk management and the requirements imposed on the activities of the authority. Information security arises from a combination of different measures. Provisions on multi-tier protection are laid down in section 7 of the Security Classification Decree. Multi-tier protection helps ensure that in the event of the failure of one layer of protection, the remaining security measures will prevent, preclude and contain any damage. In addition, measures shall be designed to detect and trace any actions and events that compromise protection. Security measures shall also be designed to restore activities, as quickly as possible, to the pre-compromise security level.

5.2 Risk assessment

The protection of classified information is based on risk management. Security measures shall be designed on the basis of an assessment of risks. Risk management is supported by assessments and audits of various kinds. In designing security measures, attention shall be paid in particular to:

- the activities or sector of the authority,
- the security classification level, meaning and intended use of the classified information,
- personnel security, for example the risk of undue influence on public officials,
- the volume and aggregation of information,[6]
- the manner of handling of classified information,
- the environment of the place where classified information is handled and stored (building setting, placement within building, premises or part thereof),
- the environment of handling and storing classified information in electronic format, for example the location of the information in various cloud computing services that may be situated in different States and thus be subject to different legislation,
- any threat factors to the information, such as the assessed risk to the information arising from intelligence services, criminal activity and the organisation's own personnel, and
- the costs incurred from the information security measures.

5.3 Catering for aggregation

The aggregate effect involves a phenomenon where a large quantity of data may constitute a whole of greater significance than its individual components. In such a case, classification and protection needs may differ from those applicable to individual data elements. An aggregate of classified information at a given security classification level in information systems may warrant a level of protection corresponding to a higher classification than that of its individual components – for example, a large quantity of information at security classification level IV in a compiled form creates an information pool at security classification level III. Quantity is not the only determining factor; in some

cases, the combination of two data sources, for example, may result in an upgrade of the information pool's security classification level.

No method of calculation generally applicable in all circumstances is available for assessing the aggregate effect. When assessing the aggregate effect, the requirements of the Information Management Act on the performance of security classification shall be taken into account. Even a large quantity of non-classified secret information will not always result in an aggregate effect and fulfilment of the grounds for classification; instead, the end result is often only a non-classified aggregate subject to secrecy. Correspondingly, even a large quantity of classified information will not always result in an aggregate effect. The assessment of the aggregate effect on a case-by-case basis always calls for determination of the current and estimated substantive content of the information pool in question and an assessment of whether the aggregate shall be classified at a higher level.

Aggregation to security classification level IV, even up to level III, may under some circumstances occur in respect of non-classified data elements subject to secrecy. Data collected on enterprises which are central to security of supply or which maintain Finland's critical infrastructure, for example, might as individual data elements be interpreted to constitute business secrets and, as such, non-classified information subject to secrecy. However, a given group of data elements could, when combined, constitute an aggregate which, falling into the hands of third parties, could cause harm to e.g. national defence, security of supply or preparedness for emergency conditions. The substantive content of such an aggregate might also warrant protection from the viewpoint of national safety (the public interest) and thus fulfil the grounds for security classification.

When the security classification level of an information system or other key information pool is interpreted to stand at a higher level than that of individual data elements due to the aggregate effect, the protection measures for this information pool should be implemented according to the requirements for the higher security classification level. According to this procedure, access to the information should be limited, following the need-to-know principle, to give access only to the necessary parts of the information. The procedure should also detect unauthorised access attempts to the part of the classified information where no need-to-know can be recognised.

6 Using security areas to protect document handling and information systems

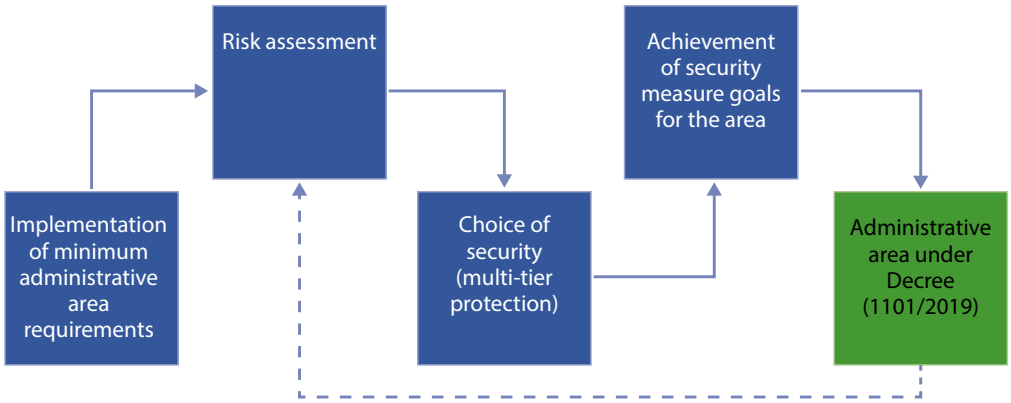
Under section 9 of the Security Classification Decree, the information management entity shall determine the physically protected *security areas* to protect the handling of classified documents and the information systems. Security areas consist of physically protected administrative areas and secured areas.

6.1 Protection in administrative areas

Administrative area refers to the areas and spaces used for the authority's ordinary work, such as office space or entities made up of multiple office premises. These may include e.g. server rooms, data centres or business premises, for example. The actor which controls the premises ensures that only persons pre-authorised by the authority have independent access to the premises. No particular requirements apply to the structures defining an administrative area.

In addition to the minimum requirements for an administrative area presented in this Recommendation, the choice of physical security measures shall be influenced by the outcome of the authority's risk assessment. Risk assessment is discussed in chapter 5.2. The effectiveness of individual security measures and of the overall security system in the area shall be re-evaluated at regular intervals. The process of vision achievement and regular evaluation is illustrated in the Figure below.

Figure 2. Vision process and regular evaluation



6.1.1 Goal and tools of physical security measures

The goal of physical security measures is to prevent unauthorised access to classified information:

a) by ensuring that classified information is handled and stored in an appropriate manner,

b) by allowing for segregation of personnel in terms of access to classified information on the basis of their need-to-know and, where appropriate, their security clearance,

c) by deterring, impeding and detecting unauthorised actions, and

d) by denying or delaying surreptitious or forced entry by intruders.

6.1.2 Choice of physical security measures

Based on the risk assessment and in keeping with the principle of multi-tier protection, the authority shall determine the appropriate combination of security measures that is sufficient relative to the risk assessment. This combination shall consist of administrative, functional and physical tools including:

- structural barriers: a physical barrier with which the area or space to be protected is defined and unauthorised intrusion is impeded and slowed down.
- access control: access to the area or space is restricted through controls. The goal is to detect unauthorised access attempts, to prevent the access of unauthorised persons and to monitor those persons moving within the area. Access control may be exercised over an area, one or more building in an area, or areas or rooms within a building. Control may be exercised by mechanical, electronic or electro-mechanical means, by security personnel and/or a receptionist, or by any other physical means.
- intrusion detection system (IDS): an IDS (burglar alarm system) may be used to enhance the level of security offered by the structural barrier. The system may also be used in place of, or to assist, security staff.
- security personnel: trained, supervised and, where necessary, appropriately security-cleared security personnel may be employed for, among other things, in support of access and control and in order to detect and deter from action individuals planning covert intrusion.
- closed circuit television (CCTV): CCTV may be used by security personnel in order to impede and investigate incidents and to verify alarms in the area or space. Security personnel may use CCTV for active real-time surveillance or for passive footage analysis after the fact.
- procedures to maintain security: determination of responsibilities and duties, various processes and operating models including access control and key management, instructions to and training of personnel, and servicing and maintenance of systems.
- lighting: potential intruders may be deterred by using lighting that permits the effective surveillance of the area by security personnel either directly or indirectly through a CCTV system.
- any other appropriate physical measures designed to deter and detect unauthorised access or prevent loss of or damage to classified information.

6.1.3 Minimum requirements for physical security measures in an administrative area

The administrative area determined by the authority shall fulfil the minimum requirements presented in the table below. In addition, the authority shall design, assign responsibilities for and implement other risk management measures based on the risk assessment and the principle of multi-tier protection and also maintain these so that the residual risk to the classified information is at an acceptable level and the goals of the security measures can be achieved.

Table 3. Minimum requirements for physical security measures in an administrative area

Security component	Minimum requirement	Further information and recommendations
Area perimeter and structures (walls, doors, windows, floor and ceiling structures)	The area shall have a visible, clearly defined perimeter. No specific requirements apply to the structure that defines the perimeter.	Any openings in the area not used for access shall be lockable so as to allow appropriate management of access to the area. The structures in the area shall be reinforced when classified information is stored in the area and the risk of burglary is estimated as likely.
Grant of access rights	Only persons duly authorised by the authority have independent access to the area. The authority shall determine the procedures and roles for access right management and key management.	Access to the area may be restricted by mechanical or electronic means or on the basis of personal recognition. A person responsible for the management of access rights, access passes and keys shall be designated for the area. The authority shall have determined or approved at least the following procedures and roles: • the procedures and roles for access right management and key management have been created, documented and instructed. • there is a list of the holders of access rights and keys. • access rights are checked on a regular basis and kept up to date. • responsibility for measures to change or re-order keys and access passes has been assigned. • key cards, non-distributed keys and access passes are stored appropriately.

Security component	Minimum requirement	Further information and recommendations
Visitors	Persons other than those duly authorised by the authority (visitors) shall always be escorted.	The authority shall have approved a visitors policy. The visitors policy approved by the authority may address topics including: • identifying the visitor and issuing a visitor pass. • logging the visit. • no unsupervised visitors allowed into or left in the area. The host of the visit shall be responsible for outside persons throughout the visit. • personnel have been instructed on hosting visitors • ensuring that a visitor does not gain unauthorised visual, auditory or other access to classified information.
Sound insulation	Sound insulation in the area shall be sufficient to prevent discussions relating to classified information from being plainly overheard by unauthorised persons. Sound insulation shall be taken into account also inside the area when classified information that is not subject to everyone's need-to-know is discussed there.	The sound insulation requirement only applies to those spaces in the area where classified information is discussed.
Technical security systems	The authority shall ensure that the security systems and devices introduced for the purpose of physically protecting classified information (e.g. storage solutions, paper shredders, locks, electronic access control systems, CCTV systems, intrusion detection systems and alarm systems deemed suitable) are appropriate for the purpose and in proper working order.	It is recommended that any such devices satisfy technical standards and the minimum requirements. The devices shall be kept in proper working order by ensuring that appropriate repairs and maintenance are undertaken, the operation of the devices is tested and documentation is kept up to date in accordance with the instructions and recommendations of the device manufacturer. In the management of rights to the system, the principle of least privilege shall be complied with (see chapter 7.6).

Security component	Minimum requirement	Further information and recommendations
Intrusion detection system	No requirements.	The area or the routes leading to the area may be equipped with an intrusion detection system (burglar alarm system) when classified information is stored in the area and the risk of burglary is assessed to be likely. It is recommended that the area be monitored by the system when it is unoccupied.
Prevention of unauthorised observation	When classified information is subject to the risk of unauthorised observation, accidental unauthorised observation included, appropriate measures shall be taken to mitigate against the risk.	The risk of unauthorised observation may be reduced, for example, through appropriate placement of workstations and screens, and by using blinds, curtains or display privacy filters.
Inspections of premises and devices	The authority shall inspect all electronic devices before these are used in an administrative area where classified information at security classification level SALAINEN (TL II) is handled and, on the basis of a risk assessment, in an administrative area where classified information at security classification level LUOTTAMUKSELLINEN (TL III) is handled when the threat to such information is assessed to be high. The area itself shall also be subject to physical or technical inspection at regular intervals. Inspections should also be carried out after any occurrence or suspicion of unauthorised access.	When the said electronic devices cannot be reliably inspected (e.g. mobile phones, smartwatches), the devices shall be left outside the area, for example in a storage solution put in place for this purpose.

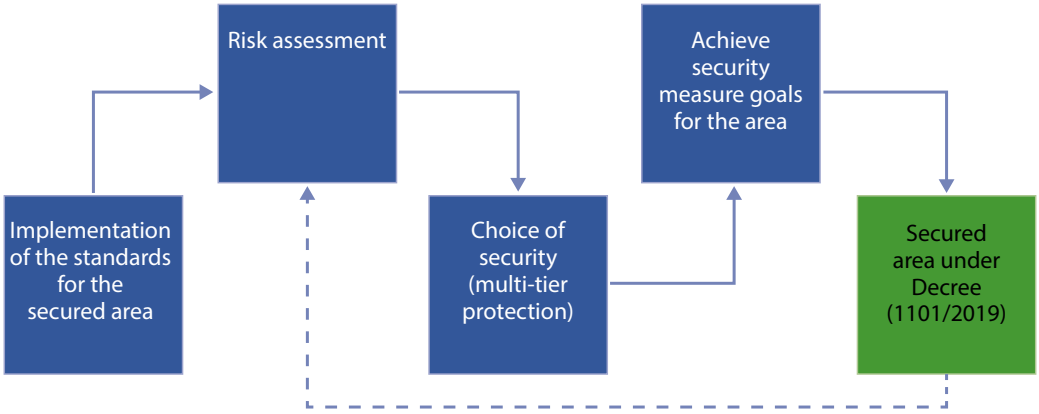
Security component	Minimum requirement	Further information and recommendations
Storage of information	Information at security classification level KÄYTTÖ RAJOITETTU (TL IV) may be stored in the area. The information shall be stored in appropriate lockable office furniture. When electronic documents at security classification level III or IV are stored in a terminal device outside secured areas, the documents shall be protected with an encryption solution of sufficient security for the security classification level. The information security of the terminal device shall be ensured.	

6.2 Secured areas

Secured areas refer to the authority's working areas and spaces that are better protected than administrative areas and where classified information is handled and stored. Secured areas include server rooms, data centres, archives and e.g. business premises that fulfil secured area requirements when classified documents are handled or stored in these in the manner laid down in section 10 of the Security Classification Decree. A secured area may be temporarily established in an administrative area for the purpose of a classified meeting or other equivalent purpose when the minimum requirements for a secured area can be implemented in the said space.

In addition to the minimum requirements for a secured area presented in this Recommendation, the choice of physical security measures shall be influenced by the outcome of the authority's risk assessment. Risk assessment is discussed in chapter 5.2. The effectiveness of individual security measures and of the overall security system in the area shall be re-evaluated at regular intervals. The process of vision achievement and regular evaluation is illustrated in the Figure below.

Figure 3. Vision process and regular evaluation



6.2.1 Goal and tools of physical security measures

The goal of physical security measures is to prevent unauthorised access to classified information:

a) by ensuring that classified information is handled and stored in an appropriate manner,

b) by allowing for segregation of personnel in terms of access to classified information on the basis of their need-to-know and, where appropriate, their security clearance,

c) by deterring, impeding and detecting unauthorised actions, and

d) by denying or delaying surreptitious or forced entry by intruders.

6.2.2 Choice of physical security measures

Based on the risk assessment and in keeping with the principle of multi-tier protection, the authority shall determine the appropriate combination of security measures that is sufficient relative to the risk assessment. This combination shall consist of administrative, functional and physical means including:

- structural barriers: a physical barrier with which the area or space to be protected is defined and unauthorised intrusion is impeded and slowed down.
- access control: access to the area or space is restricted through access control. The goal is to detect unauthorised access attempts, to prevent the access of unauthorised persons and to monitor those persons moving within the area. Access control may be exercised over an area, one or more building in an area, or areas or rooms within a building. Control may be exercised by mechanical, electronic or electro-mechanical means, by security personnel and/or a receptionist, or by any other physical means.
- intrusion detection system (IDS): an IDS (burglar alarm system) may be used to enhance the level of security offered by the structural barrier. Surveillance may also be used in spaces, rooms and buildings in place of, or to assist, security staff.
- security personnel: trained, supervised and, where necessary, appropriately security-cleared security personnel may be employed for security surveillance, among other things in support of access and control and in order to detect and deter from action individuals planning covert intrusion (response).
- closed circuit television (CCTV): CCTV surveillance may be used by security personnel in order to impede and investigate incidents and to verify alarms in the area or space. Security personnel may use CCTV for active real-time surveillance or for passive footage analysis after the fact.
- procedures to maintain security: determination of responsibilities and duties, various processes and operating models including access control and key management, instructions to and training of persons, and servicing and maintenance of systems.
- lighting: potential intruders may be deterred by using lighting that permits the effective surveillance of the area by security personnel either directly or indirectly through a CCTV system.
- any other appropriate physical measures designed to deter and detect unauthorised access or prevent loss of or damage to classified information.

6.2.3 Minimum requirements for physical security measures in a secured area

The secured area determined by the authority shall fulfil the minimum requirements presented in the table below. In addition, the authority shall design, assign responsibilities for and implement other risk management measures based on the risk assessment and the principle of multi-tier protection and also maintain these so that the residual risk to the classified information is at an acceptable level and the goals of the security measures can be achieved.

Table 4. Minimum requirements for physical security measures in a secured area

Security component	Minimum requirement	Further information and recommendations
Area perimeter and structures (walls, doors, windows, floor and ceiling structures)	The area shall have a visible, clearly defined perimeter. When the area has no storage solution deemed adequate for information storage, the walls, floor, ceiling, windows and doors in the area shall provide the security level required for the storage of the information.	Any openings in the area not used for access shall be lockable so as to allow reliable management of access to the area. The structures in the area shall be reinforced when classified information is stored in the area and the risk of burglary is assessed to be significant. Whenever possible, the emergency exits of the administrative area must not pass through the secured area. This shall be taken into account in the construction of new buildings in particular. Emergency exit arrangements may not be allowed to undermine security measures.
Access control	All entry into and exit from the area shall be monitored at the area perimeter by means of access passes or through personal recognition.	Access control may be accomplished by electronic means or on the basis of personal recognition. Only persons authorised for the area may access the secured area. Access to the area shall be verifiable after the fact.

Security component	Minimum requirement	Further information and recommendations
Grant of access rights	Independent access to the area may only be granted to a person duly authorised by the authority: • whose reliability has been verified. • who has express permission to enter the area. The authority shall determine the procedures and roles for access right management and key management.	Reliability should primarily be verified by means of security clearance vetting. The basis for access to the area should be need-to-know. On a case-by-case basis, express permission can also refer to a need to work in the area. A person responsible for the management of access rights, access passes and keys shall be designated for the area. The authority shall have determined or approved at least the following procedures and roles: • the procedures and roles for access right and key management have been created, documented and instructed. • there is a list of the holders of access rights and keys. • access rights are checked on a regular basis and kept up to date. • responsibility for measures to change or re-order keys and access passes has been assigned. • key cards, non-distributed keys and access passes are stored appropriately.

Security component	Minimum requirement	Further information and recommendations
Visitors	Persons other than those granted right of independent access to the area (visitors) shall always be escorted. When entry into a secured area, for all intents and purposes, constitutes direct access to the classified information contained in it, the following additional requirements shall apply: the highest security classification level of information customarily stored in the area shall be clearly indicated. When access to the secured area constitutes direct access to the classified documents handled in the area or the information contained in these documents, persons gaining unescorted access to the area shall also have the need-to-know referred to in section 8, subsection 1 in respect of this information. In the absence of need-to-know, information security measures shall be implemented to ensure that there is no access to classified information.	The authority shall have approved a visitors policy. The visitors policy approved by the authority may address topics including: • identifying the visitor and issuing a visitor pass, • logging the visit, • no unsupervised visitors allowed into or left in the area. The host of the visit shall be responsible for outside persons throughout the visit, • personnel have been instructed on hosting visitors, ensuring that a visitor does not gain unauthorised visual or auditory access to classified information.
Security instructions	Security procedures containing provisions on the following topics shall be prepared for each secured area: • the security classification level of classified information that may be handled and stored in the area, • applicable surveillance and protection measures, • persons who have unescorted access to the area on the basis of express permission and verification of reliability, • when necessary, procedures on visitor escorting or protecting classified information when other persons are granted access to the area, • other appropriate measures and procedures.	

Security component	Minimum requirement	Further information and recommendations
Sound insulation	Sound insulation in the area shall be sufficient to prevent discussions relating to classified information from being plainly overheard by unauthorised persons. Sound insulation shall be taken into account also inside the area when classified information that is not subject to everyone's need-to-know is discussed there.	The sound insulation requirement only applies to those spaces in the area where classified information is discussed.
Technical security systems	The authority shall ensure that the security systems and devices introduced for the purpose of physically protecting classified information (e.g. storage solutions, paper shredders, locks, electronic access control systems, CCTV systems, intrusion detection systems and alarm systems deemed suitable) are appropriate for the purpose and in proper working order. The systems and devices shall be inspected and serviced at regular intervals.	It is recommended that any such devices satisfy technical standards and the minimum requirements. The devices shall be kept in proper working order by ensuring that appropriate repairs and maintenance are undertaken, the operation of the devices is tested and documentation is kept up to date in accordance with the instructions and recommendations of the device manufacturer. In the management of rights to the system, the principle of least privilege shall be complied with (see chapter 7.6).
Intrusion detection system	A secured area which is not occupied by duty personnel on a 24-hour basis shall be inspected at the end of regular working hours and at random intervals outside regular working hours unless an intrusion detection system (burglar alarm system) is in place.	It is recommended that the area be monitored by the system when it is unoccupied.
Prevention of unauthorised observation	When classified information is subject to the risk of unauthorised observation, accidental unauthorised observation included, appropriate measures shall be taken to mitigate against the risk.	The risk of unauthorised observation may be reduced by means of screens at workstations, for example, and by using blinds, curtains or display privacy filters.
Inspections of premises and devices	Only electronic devices approved by the authority may be introduced into areas where information at security classification level I or II is handled. The area itself shall also be subject to physical or technical inspection at regular intervals. Inspections should also be carried out after any occurrence or suspicion of unauthorised access.	When the said electronic devices cannot be reliably inspected (e.g. mobile phones, smartwatches), the devices shall be left outside the area, for example in a storage solution put in place for this purpose.

Security component	Minimum requirement	Further information and recommendations
Storage of information	Information at all security classification levels may be stored in the area based on an assessment of risks and the choice of physical security measures. Information at security classification level LUOTTAMUKSELLINEN (TL III) and higher (TL II, TL I) shall be stored in a storage solution assessed to be appropriate. The authority shall determine the management procedures applicable to the keys and combination settings of the storage solution. Combination settings shall be issued to as few people as possible on a need-to-know basis. The said persons shall memorise the combination settings by heart. The combination settings of storage solutions containing classified information shall be changed • when receiving a new security container. • always in the event of a change in the personnel who knows the combination setting. • always in the event of an actual or suspected compromise of the information. • whenever one of the locks has been serviced or repaired. • every 12 months at least. Classified information at security classification level ERITTÄIN SALAINEN (TL I) shall be stored in a secured area in compliance with one of the following conditions: • a technically controlled storage solution, • a storage solution without technical controls, the condition of which is inspected on a regular basis, • a storage solution without technical controls that is equipped with an intrusion detection system and the alerts from which are met by a trained response unit, • a separate space that is equipped with an intrusion detection system and the alerts from which are met by a trained response unit.	

7 Minimum requirements for the protection of information systems and telecommunications arrangements

Under section 13 of the Information Management Act, an information management entity shall monitor the state of the data security of its operating environment and ensure the data security of its datasets and information systems over their entire lifecycle. The information management entity shall determine the material risks to data processing and dimension the data security measures in accordance with the risk assessment. Under section 6 of the Security Classification Decree, an authority shall also ensure in advance that the protection of a classified document is duly organised if the authority grants access to a classified document to a party other than a central government authority. It is reasonable to assume that actors interested in classified information are often not the same as actors interested in information that is secret but not subject to security classification, for example secret but non-classified personal data.

The protection of classified information must also take into account legislation-derived risks. The term refers to possibilities under the legislation of different countries to obligate service providers to cooperate with the authorities of the country in question and to provide, for instance, direct or indirect access to the service customers' secret information. In addition to the physical location of secret information, legislation-derived risks may extend to disclosure of information administrated from another country through management connections. In many countries, legislation-derived disclosure and right to view data are limited to the police and the intelligence authorities. The processing of classified information should be limited only to processing environments and information systems, the sufficient information security of which – relative to the risks – can be assured by the authority responsible for information security.

Whether the information is subject to an international information security agreement is also a factor of relevance to information protection and risk assessment. When national classified information may come under the jurisdiction of another country's authorities, for example as a result of technical surveillance, it must be ensured that this potential situation is duly addressed in risk assessment and that the residual risk arising is at an acceptable level. The specifics of classified international undertakings are discussed in more detail in the guidelines issued by the National Security Authority (NSA), the Industrial Security Manual (Ministry for Foreign Affairs NSA 2015) and the Instructions for handling international classified information [in Finnish] (Ministry for Foreign Affairs NSA 2020).

7.1 Protection of information inside and outside premises

In situations where information at security classification level IV or III is handled and stored outside secured areas on a terminal device consistent with the relevant security classification level, or information at security classification level III is stored on a terminal device inside an administrative area, the information on the terminal device shall be protected with an encryption solution of sufficient security for the security classification level in question, and the sufficient integrity of the terminal device for the security classification level in question shall in particular be ensured so as not to compromise the confidentiality of the information as a result of the terminal device's loss of integrity.

Typically, information system integrity is ensured by protecting it through physical access control to secured areas, including e.g. all physical servers, network devices, terminal devices and cabling relating to the information system. For example, when protecting the integrity of an information system at security classification level IV against general risks to classified information, it may be sufficient to situate the information system's information pools in an administrative or secured area and, in respect of terminal devices equipped with sufficient encryption, also to a limited extent to allow storage in another lockable space, for example the home of an official.

Information systems at security classification level III should be situated in their entirety in a secured area while, **for example, a fixed data network at security classification level III or II cannot extend into an administrative area.** When a terminal device used to handle information at security classification level III has to be stored in an administrative area or wholly outside security areas, the lack of the integrity protection arising from physical access control should be compensated for on a risk basis, e.g. by situating the terminal device in a casing or packaging that reveals unauthorised access. 'Security briefcases' currently available on the market aim to detect attempted unauthorised access to their contents. Such briefcases may either generate a notice of any detected incidents to the terminal device user or the user's organisation or be designed so that any tampering is evident on the casing or packaging.

As a rule, classified information should not be taken along on trips abroad. Instead, e.g. a 'travel device policy' of taking along only the information and devices essential on the trip should be utilised. In addition, particular care should be taken on trips never to leave devices that contain classified information unattended, for example in a hotel safe, and to rely on other procedures to protect integrity and confidentiality only in situations where this is absolutely necessary.

In its risk assessment, the authority shall nonetheless take into account that outside security areas, both classified information and the terminal devices used for its handling

– especially at security classification level III and higher – are subject to risks which in many cases be highly challenging if not impossible to mitigate to a sufficient extent. In handling information, attention shall additionally be paid to protection against unauthorised observation and eavesdropping, as well as e.g. protection against electromagnetic radiation risk on a risk basis.

7.1.1 Means of handling, security classification level IV (TL IV)

Electronic processing (also by means of remote access) at security classification level IV is possible by using the tools and systems provided, approved and instructed by the employer for this purpose. A document may be printed on a shared networked multifunctional device, provided that the said network and device fulfil the requirements for security classification level IV. Information may be handled outside the office of the authority when third-party visual observation of or other access to the information has been prevented.

7.1.2 Means of handling, security classification level III (TL III)

Electronic processing (also by means of remote access) at security classification level III is possible by using certain tools and systems provided, approved and instructed by the employer for this purpose. An official may not copy a document at security level III to which they have gained access in order to widen its distribution because the dispatch and receipt of documents shall be registered separately for each document.

7.1.3 Means of handling, security classification level II (TL II)

Electronic processing, printing included, at security classification level II is possible by using certain tools and systems provided, approved and instructed by the employer for this purpose. When information is handled orally, this shall take place in specifically designated spaces (inside a secured area). An official may not copy a document at security level II to which they have gained access.

7.1.4 Means of handling, security classification level I (TL I)

Materials at security classification level I shall primarily be handled in the same manner as materials at security classification level II, taking into account the following, stricter requirements: information at security classification level I may only be handled inside

secured areas, documents shall be prepared on a workstation that fulfils requirements, documents may be printed and copied only on printers that meet the requirements for the said security classification level and have been approved by the authority. Cf. the separation of information systems at different security classification levels discussed in chapter 7.2.

7.2 Separation of information systems

Under section 11, subsection 1, paragraph 1 of the Security Classification Decree, the information systems and telecommunications arrangements used for handling classified documents shall be implemented so that taking into account the security classification level of the documents handled therein, they are separated in a sufficiently reliable manner from the information systems and telecommunications arrangements at a lower security level. The separation of information systems is one of the factors of the greatest impact in protecting secret information. The separation aims to limit the handling environment of secret information into a manageable entity and, in particular to accomplish limitation of information handling only to environments of sufficient security.

The separation of information systems and telecommunications arrangements at security classification level IV from environments at different levels may be implemented by means of firewall solutions and by limiting the traffic of security-critical services at a lower security classification level (web browsing, email and the like) by directing it through separate proxy servers, which filter their content. It is possible to connect information systems and telecommunications arrangements at security classification level IV to the Internet or to other untrusted networks, provided that the risks arising from such linkage can be adequately reduced, by means of other protection, to the standard required by security classification level IV. This requires attention in particular to software updates, access rights in keeping with the principle of least privilege (see chapter 7.6), configurations with dedicated system parameters, and incident detection and recovery capabilities.

A typical application of a handling environment at security classification level IV is a part of the office network's information processing environment that may consist of e.g. workstations and case management software as well as the arrangements put into place to protect these (e.g. firewalling and access rights management). A similar separation is also suited to protecting non-classified secret information as well as to protecting the integrity and availability of public information.

At security classification level III and higher, the separation into environments at different levels may be implemented by means of gateway solutions of sufficient security. In these, the general design principle relies on implementing the "No Read Up" and "No Write

Down" rules of the Bell-LaPadula model. In other words, gateway solutions must reliably block the flow of information at a higher security classification level to environments at a lower level. Such solutions include one-way data flow regulators, for example data diode solutions. The separation of information systems and telecommunications arrangements at security classification level II can, as a rule, only be implemented with high-reliability data diode solutions. In the separation of information systems and telecommunications arrangements at security classification level I, it shall furthermore be taken into account that as a rule, the separation must be implemented through complete physical separation and only exceptionally with data diode solutions. Design principles are discussed in more detail in the NCSA guide for planning principles and solution models for gateway solutions [in Finnish] (Finnish Communications Regulatory Authority 2018).

When international classified information is handled in the information systems, connecting information systems and telecommunications arrangements must take into account international information security obligations which may wholly prohibit any connection. Under the Act on the Assessment of the Information Security of Public Authorities' Information Systems and Telecommunications Arrangements (1406/2011) [In Finnish], a central government authority may request a conformity assessment of an information system or telecommunications arrangement from the Finnish Transport and Communications Agency. It is recommended that an assessment be requested, particularly in respect of connections of information systems and telecommunications arrangements at security classification levels I and II to information systems and telecommunications arrangements at lower levels, so that the authority responsible for the security of the information system or telecommunications arrangement, in support of its risk management decisions, can rely also on the expert assessment of the Finnish Transport and Communications Agency National Cyber Security Centre as to possible residual risks associated with connection. For more information, please see the Finnish Transport and Communications Agency guideline (2019) on the assessment and accreditation process of information systems [in Finnish].

7.3 Vulnerability management

The security of an information system relies materially on the reliability of the software used (e.g. operating systems and applications). The production of flawless software has proven a challenge. In practice, no software is without its faults, i.e. vulnerabilities, that may be exploited to bypass the protections on the information handled in the information system. Responsible actors remedy vulnerabilities discovered in their software. Software risks may be reduced considerably through software testing, and by installing all security patches (updates).

Key aspects to be organised:

- an effective, regular process for security patch installation, and
- ensuring the practical functioning of the process.

Aspects essential to the update processes are the sufficient speed and coverage of update rollouts. The processes shall cover all software having a material impact on security. Typically, these include the operating systems, system software and third-party applications on servers and terminal devices as well as network device software. Means to ensure the functioning of update processes include regular configuration reviews and technical vulnerability scans.

7.4 Change management methods that cater for security

The security of even the most securely designed information system will erode over time when the changes made to the system are not managed appropriately. Maintaining credible system security calls for a procedure in which the security effects of changes impacting on the system are assessed and also tested, whenever possible, and the necessary additional protection is implemented as required before any changes are introduced. Change management also allows the more efficient administration of the system and supports the other administration processes.

7.5 Backup copy procedures

Backup copying is vital especially to ensuring the availability of information. It is also often a procedure in which the other information protection needs (integrity, confidentiality) must be taken into account by methods consistent with the original information. Backup and recovery processes shall be designed, implemented, tested and documented as a part of the continuity plan so that the functional needs and other obligations of the organisation and relating to the information system in question can be fulfilled. Particular attention shall be paid to the following:

- sufficient frequency of backup copying relative to the criticality of the information backed up. This requires determination of how much of the data can be lost (recovery point objective, RPO).
- sufficient recovery process speed relative to operational requirements. This requires determination of how long recovery may take (recovery time objective, RTO).

- the correct functioning of the backup and recovery processes is tested regularly.
- the physical location of backup copies is sufficiently removed from the system proper (different sag/fire space, sufficient distance between backups and the system room).
- backup copies are protected throughout their lifecycle by methods of at least comparable standard as those protecting the original information. A large quantity of information may necessitate stricter protection (aggregate effect).
- access to the backup copies is restricted, in keeping with the principle of least privilege, only to approved persons or roles.
- the backup and recovery processes are traceable (logging) and controlled in a way that enables detection of unauthorised action.
- where backup copies are stored at a different physical location, this location as well must be of at least comparable standard with regard to physical and logical access control.
- where backup copies containing secret information are transferred outside a physically protected area (e.g. between data centres) over a network, the information or the telecommunication shall be adequately encrypted.
- where backup copies containing secret information are transferred outside a physically protected area (e.g. between data centres) in transfer media (e.g. backup tapes or disks), the instructions described in chapter 4.4 shall be complied with. Encryption of the transfer media or the information it contains is recommended.
- backup media shall be destroyed in a reliable manner.

7.6 Principle of least privilege

Under chapter 11, section 3 of the Security Classification Decree, the information systems and telecommunications arrangements used for handling classified documents shall be implemented so that the information system users are provided only with the information, rights or authorisations that are necessary to perform the tasks.

Ensuring that access rights are up to date usually requires the access and user rights of all employees, suppliers and third parties to be audited at regular intervals, for example every six months. Additionally, in the event of changes in an individual's duties due to e.g.

promotion, job rotation and especially in connection with termination of employment, a clear and effective procedure must be in place for modifying or removing rights. This may be accomplished e.g. by the supervisor notifying any changes in advance to the persons tasked with rights management so that all rights can be kept up to date. This may further mean the removal or modification of user and access rights either from a centralised management system or separately for individual systems.

The management of user rights shall comply with the principle of least privilege:

1) user rights management has been tasked to one or more persons.
2) a pre-defined process must be in place for the creation, approval and administration of user accounts.
3) users of the information handling environment are provided only with the information, rights or authorisations that are necessary to perform the tasks.
4) user rights management shall comply with the principle of separation of duties: order, approval and implementation may not be carried out by the same person.
5) a list shall be kept of system users. Every user right issuance must be documented (electronically or in paper format).
6) the issue of user rights shall include verification that the recipient of the right is a member of personnel or otherwise authorised to hold the right.
7) instructions for the processing and issue of user rights shall be in place.
8) user accounts and rights that are no longer necessary (e.g. because the user is no longer with the organisation or when the user account has been dormant for a pre-determined period of time) shall be removed.
9) a clear and effective way of notifying any changes in personnel to the appropriate parties without delay and an effective way of making the necessary modifications must be in place.
10) user and access rights shall be audited regularly and at least annually. In addition, the audits shall take into account also persons who have access to the system logs, database or servers.

7.7 Identification of users and equipment

7.7.1 Inside a physically protected administrative area or secured area

Under section 11, subsection 1, paragraph 5 of the Security Classification Decree, the information systems and telecommunications arrangements used for handling classified documents shall be implemented so that persons using them, as well as equipment and information systems are identified in a sufficiently reliable manner.

With regard to security classification level IV, the user and equipment identification requirement may be fulfilled by implementing the following measures:

1) individual user identifiers are in use.

2) all users are identified and authenticated.

3) in authentication and in identification, a well-known and reliable technique consistent with current security requirements is used or the requirement has been covered in another reliable way.

4) too many false attempts in the identification will result in the locking of the identifier.

5) maintenance identifiers for systems and applications are personal. Where this is not technically possible, documented and settled password management procedures that enable unique user identification are required for identifiers in use by multiple persons.

6) authentication is done at least by the use of passwords in keeping with approved password policies. Password policies should also be reviewed e.g. annually and they should include policies concerning system identifiers.

7) in traffic outside physically protected areas, strong user identification based on at least two factors must be in use and the connection shall be encrypted with sufficient strength.

In respect of security classification levels III–II, the requirement may be fulfilled by implementing the following measures in addition to measures **1–5** above:

1) strong user identification based on at least two authentication factors is required.

2) terminal devices shall be technically identified (device identification, 802.1X or equivalent procedure) before allowing access to the network or the service, unless access to the network has been limited by physical security methods (e.g. setting the server in a locked rack cabin inside a technically protected secured area which has been approved by the authority for the protection level in question.

3) in traffic outside physically protected areas, the connection shall be encrypted with sufficient strength.

Section 8a of the Act on Strong Electronic Identification and Electronic Trust Services (2016/533) lays down provisions on the authentication factors to be used in the identification means. At least two of the following authentication factors shall be used in the identification means. The factors are:

1) a knowledge-based authentication factor that the subject is required to demonstrate knowledge of,

2) a possession-based authentication factor that the subject is required to demonstrate possession of,

3) an inherent authentication factor that is based on a physical attribute of a natural person.

When reference is made to the use of two factors, two or three passwords are not sufficient for identification because they are all based on the first factor (what the person knows). When using bank identifiers, for example, identification is based on what the person knows (user ID and possible password) and on what is in the person's possession (PIN code list, PIN code device or mobile device).

7.7.2 Substitute procedures

The procedures for strong user identification and terminal device identification for security classification levels III and II may in some cases be implemented by restricting access to the information system to be possible only from a strictly defined physically protected area (in most cases, either a technically protected secured area, a locked rack

cabin or equivalent) to which the person concerned has been issued personal right of access and the access control system of which uses strong identification based on at least two authentication factors. In such a case, user identification in the system can be implemented with a user ID/password combination.

7.7.3 Further information

Setting up a reliable identification and authentication procedure contains at least the following:

1) the authentication method has been protected against man-in-the-middle manoeuvres,
2) at the log in phase, before the actual authentication of the user, no additional information disclosed,
3) the credentials used for authentication are always in encrypted format in cases where they are sent over a network,
4) the method of authentication is protected against repetitive transmission attacks, and
5) the authentication method has been protected against brute force attacks.

7.8 Necessary functionalities

Under section 11, subsection 1, paragraph 6 of the Security Classification Decree, the information systems and telecommunications arrangements used for handling classified documents shall be implemented so that only the necessary functionalities to meet the operational requirements are implemented.

Writing secure software code has turned out to be challenging. The more software code an environment includes, the higher the risk of software flaws, that is, vulnerabilities. The higher the number of services relying on the security of software code, the more probable it is that the services also include vulnerabilities. Risks can be reduced by reducing the attack surface, that is, by exposing only the necessary services to attacks.

Systems are usually full of features. These features are usually enabled by default and easy to take into use, while on the other hand these features are also often run with settings that are excessively vulnerable. If unnecessary features are not removed from use, they

are available also for a malicious party. By default, systems often include predefined maintenance passwords, preinstalled unnecessary software and unnecessary user accounts.

Hardening of the system means, in general terms, making changes to the settings to reduce the system's attack surface. In general, only functions, equipment and services that are essential to meet the service requirements should be taken into use in systems, and the visibility of services, for example, should be limited to as little as possible. Similarly, for instance, automated processes should be only provided with data, rights or authorisations that are necessary to perform their tasks in order to limit damage caused by accidents, errors or unauthorised use of system resources. Any unsecure default settings and e.g. unnecessary default user accounts in a system must be changed or removed. For more information on system hardening, please consult the most recent version of Katakri.

7.9 Traceability

Under section 17 of the Information Management Act, an authority shall ensure that the necessary log data is compiled of the use of its information systems and the disclosure of information therefrom if the use of the information system requires identification or other login. The purpose of use of log data is to monitor the use of the information in the information systems and its disclosure and to investigate technical errors in the information system.

Traceability refers to recording the events of the system environment so that, in abnormal situations, it is possible to find out what measures had been taken in the environment and by whom, and what effects such measures have had. Essential recordings typically include the log data of fundamental network devices and servers. In addition, the log data of workstations, etc. is also very often covered by this.

The coverage requirement can in most cases be met by checking that logging is enabled at least for workstations, servers, network devices (especially firewalls, including software firewalls on workstations) and the like. It should be possible to afterwards check from the network device logs as to what management functions were performed on the network device, when and by whom. Event logs should be compiled of the use of the system, user activities as well as security-related functions and exceptions.

A recommended method to protect the logs is to forward all essential logging information to a strongly safeguarded logging server, the information content of which is regularly backed up in a separate environment that is at least at an equivalent security classification level. The compilation and storage of logging data should be implemented in a manner that enables the detection of logging data removal or alteration also in situations where the network connection between e.g. the log source and the log collector is unavailable. Correspondingly, log compilation on workstations permanently disconnected from the network and backups of compiled logging data require a regular process. To support the legal protection of administrators and to promote the investigation of suspected security breaches, it is recommended to separate tasks so that the logging data maintenance duty is separated from other maintenance duties. Traceability implementation should also cater for 'user impersonation' situations, i.e. situations where a person who has logged into the system can execute actions by using the account of another. The functioning of logging data storage and analysis software must also be monitored and any failures must be detectable at a short time lag – for example within 24 hours of log source stopping to supply log data.

The log data storage periods must take into account the needs of the use case in question. It may be justified to require different storage periods for some information processing and transfer logs than for log data compiled to investigate incidents, for example. In the activities of the authorities, for example, statutes of limitation in criminal law can typically lead to a required storage period of at least five years A common practice is for log data covering the past six months to be available in real time and log data covering a longer period of time available when necessary within a few working days. Various log data use cases are discussed in more detail in the Information Management Board's Collection of recommendations on the application of certain information security provisions [in Finnish] (Ministry of Finance 2020:21, chapter 7).

In implementation, bringing the storage space and storage period of log data up to an adequate level must also often be taken into account. It is recommended that a volume deemed adequate be set aside in the environment for logs. An adequate period of time may be determined e.g. by using the logs accrued over a period of one month as the basis for estimating the space adequate for the required storage period. It should be noted that the space calculation should include a considerable buffer, as incidents and also certain types of attacks serve to significantly increase log data volume.

Implementation example

In a processing environment at security classification level IV, the requirement may be fulfilled by implementing the following measures:

1) a log compilation, transfer, alert and monitoring policy or guideline formulated in writing with consideration to the requirements of the activities has been rolled out,

2) records are comprehensive enough to detect occurred or attempted security breaches after the fact,

3) essential records are kept for at least six months, unless legislation or contracts specify a longer retention period. Processing logs and records subject to e.g. a statute of limitations under criminal law in respect of official activities are kept for at least five years,

4) log files and respective register services are protected against unauthorised access (access rights management, logical access control) in accordance with the principle of least privilege.

In processing environments at security classification levels III–II, the requirement may be fulfilled by implementing the following measures in addition to those under items 1–4 above:

5) essential records are kept for at least five years, unless legislation or contracts specify a longer retention period. Records that are of minor relevance to e.g. the investigation of incidents or criminal law in respect of official activities may be kept for a shorter period, for example 2–5 years,

6) log files are backed up regularly,

7) the clocks of all relevant information processing systems within a security area are synchronised to an agreed reference time source,

8) a system to ensure the integrity of logs is in place, and

9) handling and usage of the log files are registered.

7.10 Detection

Technical incident detection capability is usually based on three sources:

1) events in network traffic,
2) compiled records (logs), and
3) events in hosts.

Sufficient detection capability can usually be implemented as a combination of the above detection sources. The better the understanding of the information processing environment in question and its normal functioning, the better the capability to detect abnormal events and anomalies. The detection of abnormal events and anomalies also supports the detection of attacks on which no identifiers (Io, Indicator of Compromise) are available. The normal functioning of the information processing environment should be known across its lifecycle, from start-up to decommissioning. Change management also supports detection capability by means that include regular analysis of changes in hardware and software configurations.

There are many solutions available for monitoring network traffic and limiting the effects of a detected attack, ranging from monitoring at the network node level to workstation/server sensors and combinations of these. Regardless of the network devices or operators, the actual capability to detect changes at the network level typically requires understanding the baseline of the network traffic. In processing environments at security classification level IV, the detection capability on the network traffic level should cover specifically the outmost border of the network or the target. At security classification level III and higher, coverage should extend to the gateway solution on the outmost border, as well as the traffic inside the network or target.

In practice, in most environments, automatic observation and alarm tools are required to be able to detect attempted attacks and misuse. In some cases, the manual review of logging data is also possible and perhaps even essential when, for example, an incident has gone undetected by the automated tools and it requires more detailed investigation. It should also be borne in mind that only data necessary to information security measures may be compiled in logs and that the implementation of measures may not restrict freedom of expression or violate privacy or the right to confidentiality of correspondence. Generally speaking, it should be noted that detection capability calls for familiarity with the characteristics of each information processing environment as well as measures including the determination of critical assets and monitored events and the tailoring of these measures to the environment in question. Detection capability must also be constantly maintained.

The restoration of an information processing environment to a protected state within reasonable time usually requires planned, described, trained and rehearsed processes and technical methods The role of the entire personnel must also be taken into account in the development and maintenance of detection capability. Observations reported by end users, for example, may be valuable inputs in the detection of attacks and attempted attacks.

Implementation example

In a processing environment at security classification levels IV–II, the requirement may be fulfilled by implementing the following measures:

1) the baseline of the network traffic (volume of traffic, protocols and connections) is known. A procedure exists to detect abnormal events in the network traffic (e.g. abnormal connections or attempts for such),
2) a procedure exists for detecting anomalies (especially attempted unauthorised use of the information system) from compiled records and situational data (e.g. changes in log activities),
3) a procedure exists for detecting anomalies in the information processing environment hosts (e.g. workstations and servers), and
4) a procedure is in place to recover from detected incidents.

7.11 Encryption solutions

Under section 11, subsection 1, paragraph 7 of the Security Classification Decree, the information systems and telecommunications arrangements used for handling classified documents shall be implemented so that the encryption solutions used are adequately secure, taking into account the security classification level of the documents handled in the information system or telecommunications arrangement.

Provisions on the transfer of secret data in a public network are laid down in section 14 of the Information Management Act. Under section 12 of the Security Classification Decree, classified documents may be transferred in other than a public network outside the security areas of authorities or via an information system or telecommunications arrangement at a lower security level than the said security classification level **only in encrypted form**. In addition, the data transfer shall be arranged so that the recipient is ascertained or identified in a sufficiently data secure manner before the recipient is allowed to process the transferred secret data. If the transfer of classified documents takes

place in a security area in other than a public data network and sufficient protection of the information can be implemented by physical protection measures, unencrypted transfer or encryption at a lower security level may be used.

Especially when traffic passes via a public or other lower security level network, encryption solutions are often the only protections for ensuring the confidentiality, and typically also integrity, of secret information. Because any shortcomings of encryption solutions are often extremely challenging to replace with other protections, particular attention must be paid to choice and secure usage of the encryption solution.

When transferring classified information outside physically protected areas, or via a public network, the material or traffic shall be protected with encryption of sufficient security. For example the Internet and the MPLS networks provided by operators shall be considered public networks. In practice, manners of implementation include e.g. VPN solutions between users' terminal devices and the information systems of the authority, LAN-2-LAN encryption between the networks of organisations, and secure email and file encryption solutions provided to end users. When transferring secret information within physically protected areas and inside a network protected at an at least equivalent level, lower-level encryption or unencrypted transfer may be used on the basis of the outcomes of the risk management process.

An authority must use encryption solutions with reliable evidence of their sufficient security. Several aspects must be taken into account in the assessment of encryption solutions. In addition to verifying the strength of the algorithm and the correct functioning of the encryption solution, also the threat level of the corresponding environment must be taken into account. For instance, in traffic across the Internet, the threat level is considerably higher compared with transferring encrypted information within a managed and protected physical area (for example, traffic between two secured areas via an administrative area). Other aspects to be taken into account when assessing the encryption solution include requirements of the use case with regard to the secrecy period and integrity of the information. For more information, please see Cryptographic requirements for confidentiality, National Cyber Security Centre guideline [in Finnish] (Finnish Communications Regulatory Authority 2018).

Different information types are exposed to different risks. For instance, it is generally considered that classified information of the authorities should be protected from the perspective of the security of the State (the public interest). It is reasonable to assume that actors interested in classified information are often not the same as actors interested in non-classified personal data, for instance. The differences in the risks should also be taken into consideration in the choice of encryption solutions.

When choosing a protection solution, reliance primarily on the Finnish Transport and Communications Agency's National Cyber Security Centre Encryption solutions approved by NCSA-FI [in Finnish] (Finnish Transport and Communications Agency Traficom 2020) is recommended. The acceptable use policy determined in the approval process is an essential element of the approval of encryption solutions. The policy contains those use cases and encryption solution settings with which, when applied, the encryption solution in question has been assessed to provide adequate protection for the information at the security classification level in question.

The protection effect of encryption may be fully or partially lost in situations in which the weaknesses of key management can be exploited by unauthorised actors. The management processes of the encryption solution's encryption keys must be planned, implemented and described/instructed. Only authorised users and processes shall have access to the encryption keys. The processes require at the least:

a) cryptographically strong keys,

b) secure key distribution,

c) secure key storage,

d) regular key rollovers,

e) changing of outdated or exposed keys, and

f) prevention of unauthorised key changes.

With regard to encryption solutions in particular, the risk assessment also needs to take into account the security of supply chains. Even if the encryption solution is sufficiently secure when leaving the provider of the encryption solution, shortcomings in the protection of the supply chain can facilitate tampering with the encryption solution and thereby result in the deployment of an insecure encryption solution as part of the authority's information system or telecommunications arrangement.

Ascertaining the recipient with a sufficient degree of reliability depends considerably on the encryption solution used. For example, the guideline Encryption solutions approved by NCSA-FI [in Finnish] of the Finnish Transport and Communications Agency National Cyber Security Centre (2020) addresses also the identification of recipients when the encryption solution in question is used e.g. in communication with a person within another organisation. On the other hand, in many encryption solutions the identification of the recipient relies on the reliability of key management (e.g. LAN-2-LAN encryption between establishments of a single organisation or between two different organisations based on shared secrecy, or file encryption based on shared secrecy).

The fact that provisions on user identification in digital services provided to the public are laid down in the Act on the Provision of Digital Services (306/2019) [In Finnish] shall be taken into account in the transmission of non-classified secret information in particular.

7.12 Handling in cloud services

Documents at security classification level IV may be handled and stored in cloud services that are not estimated to be subject to the legislation-derived risks described at the start of chapter 7, provided that the authority has also taken into account all other protection needs and obligations associated with the handling of classified information. Documents at security classification level IV may be stored in other cloud services only in reliably encrypted format so that they cannot be decrypted in the said service during the lifecycle of the information. A part of an authority's classified information handling environment may thus be implemented by using cloud technology. The Ministry of Finance has issued guidelines and recommendations concerning cloud services (Ministry of Finance 2018:35, 2020:66, 2020:73). In addition, the National Transport and Communications Agency National Cyber Security Centre has issued Criteria to Assess the Information Security of Cloud Services (PiTuKri) (2020:13).

Section 14 of the Information Management Act as well as section 11, paragraph 7 and section 12 of the Security Classification Decree enable the transfer of classified information over a public or other untrusted network in situations where the information is in sufficiently reliably encrypted format. A consideration that warrants particular attention is that decryption in the untrusted network must not be possible, and this covers both the software or device that accomplishes the encryption and the placement of key management outside the untrusted network The same principle may also be applied in situations where the need arises to transfer or store classified information in untrusted information processing environments such as multinational cloud services.

In applying the principle, it must always be taken into account that, as a rule, the cloud service provider always has access to the information processed in the service if the information during its lifecycle exists in its decrypted format (e.g. an image shown to customers). For instance, common solution models that are based on the use of own keys (BYOK, Bring Your Own Keys) or equipment-based security modules placed in the service provider's physical data centre (HSM, Hardware Security Model) limit but do not typically prevent the cloud service provider's access to the information processed by the service. However, encryption can be used for supplementary protection to support, for instance, the separation of the data of different customers, the destruction process of protected assets or separation of duties.

8 Statutes

Council Decision on the security rules for protecting EU classified information (2013/488/EU).

Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Act on the Provision of Digital Services (306/2019)

Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018)

Act on Information Management in Public Administration (906/2019)

Act on International Information Security Obligations (588/2004)

Act on Strong Electronic Identification and Electronic Trust Services (533/2016)

Act on the Openness of Government Activities (621/1999)

Government Decree on Security Classification of Documents in Central Government (1101/2019)

Act on the Assessment of the Information Security of Public Authorities' Information Systems and Telecommunications Arrangements (1406/2011)

Constitution of Finland (731/1999)

Data Protection Act (1050/2018)

9 Guidelines and other materials

Office of the Data Protection Ombudsman. https://tietosuoja.fi/etusivu

Finnish Transport and Communications Agency Traficom 2017. Assessment and approval of cryptographic products carried out by the Finnish Transport and Communications Agency Traficom [in Finnish]. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-salaustuotearvioinnit-ja-hyvaksynnat.pdf

Finnish Transport and Communications Agency Traficom National Cyber Security Centre 2019. Assessment and accreditation process of information systems carried out by the Finnish Transport and Communications Agency Traficom [in Finnish]. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje_NCSA-toiminnon_suorittamat_tietoturvallisuustarkastukset.pdf

Finnish Transport and Communications Agency Traficom 2020. Encryption solutions approved by NCSA-FI [in Finnish]. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/NCSA_salausratkaisut.pdf

Finnish Communications Regulatory Authority National Cyber Security Centre 2018. Guide for planning principles and solution models for gateway solutions [in Finnish]. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Yhdyskaytavaratkaisuohje.pdf

Finnish Transport and Communications Agency Traficom National Cyber Security Centre 2020:13- Criteria to Assess the Information Security of Cloud Services (PiTuKri). https://www.traficom.fi/sites/default/files/media/file/PiTuKri_v1_1_english.pdf

Ministry for Foreign Affairs 2015. Information security auditing tool for authorities – Katakri 2015 https://um.fi/information-security-auditing-tool-for-authorities-katakri-2015

Ministry for Foreign Affairs National Security Authority (NSA) 2015. Industrial Security Manual. https://um.fi/industrial-security-manual

Ministry for Foreign Affairs National Security Authority (NSA) 2020. Guideline for handling international classified information [in Finnish].. https://um.fi/turvallisuusluokitellun-tiedon-kasittelyohje

Ministry of Finance 2018:35. Guidelines for Public Sector on Data Communications Services [in Finnish]. https://julkaisut.valtioneuvosto.fi/handle/10024/161294

Ministry of Finance 2020:73. Guidelines on using cloud services. Practical guidelines for public sector organisations on making use of cloud computing services [in Finnish]. https://julkaisut.valtioneuvosto.fi/handle/10024/162453

Ministry of Finance 2020:18. Recommendations on the implementation of management responsibilities in information management [in Finnish]. https://julkaisut.valtioneuvosto.fi/handle/10024/162132

Ministry of Finance 2020:29. Recommendation for an information management model [in Finnish]. https://julkaisut.valtioneuvosto.fi/handle/10024/162176

Ministry of Finance 2020:53. Recommendation on the Assessment of the Transformative Impact of Information Management [in Finnish]. https://julkaisut.valtioneuvosto.fi/handle/10024/162330

Ministry of Finance 2020:21. Collection of recommendations on the application of certain information security provisions [in Finnish]. https://julkaisut.valtioneuvosto.fi/handle/10024/162150

Ministry of Finance 2020:66. Productivity through cloud services: Guidelines for making use of cloud computing services in the public sector [in Finnish]. https://julkaisut.valtioneuvosto.fi/handle/10024/162451

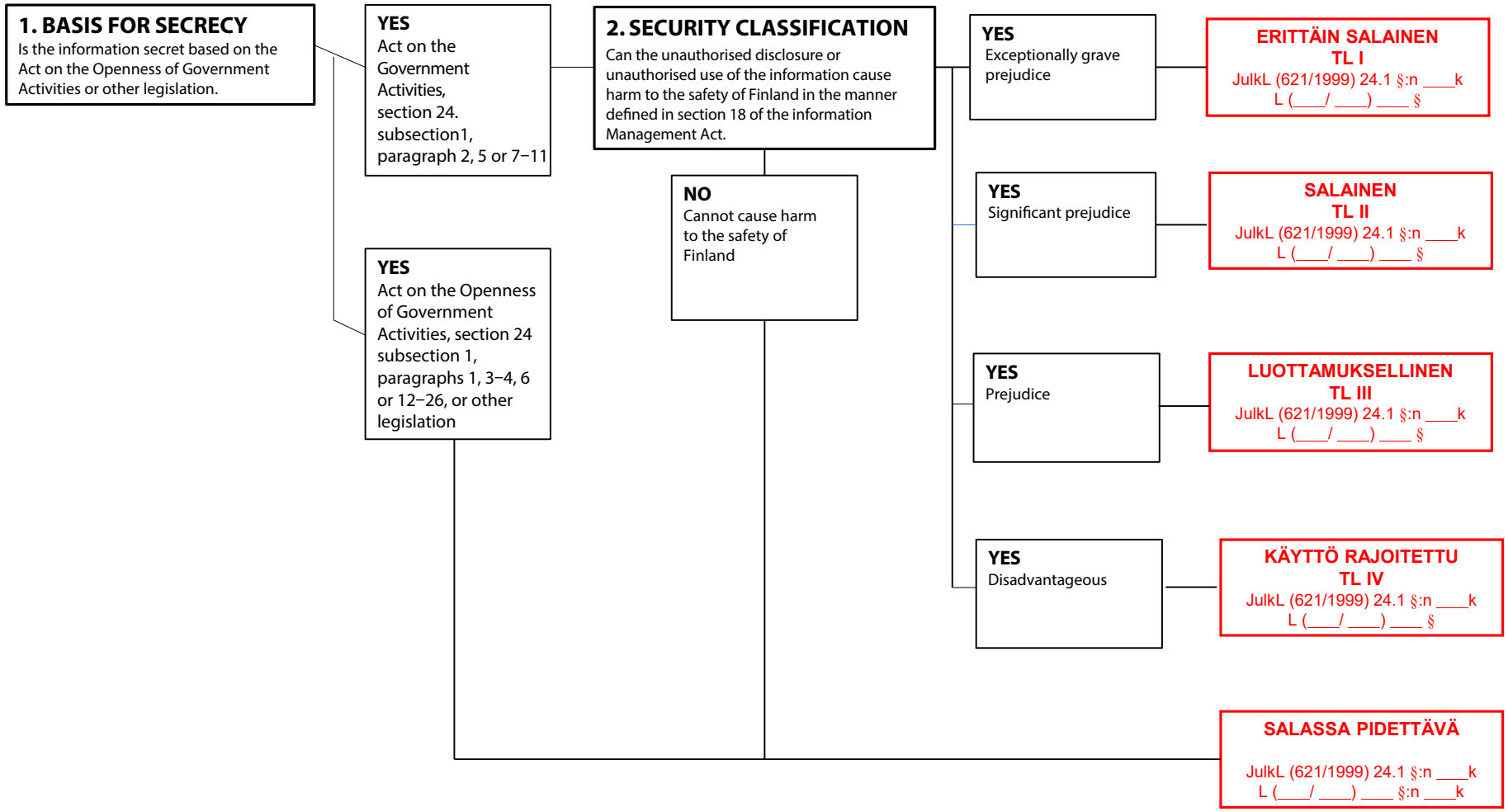
Finnish Communications Regulatory Authority National Cyber Security Centre 2016. Lifecycle management of hard drives – overwriting and recycling [in Finnish]. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-ylikirjoitus.pdf

Finnish Communications Regulatory Authority National Cyber Security Centre. 2018. Cryptographic requirements for confidentiality – national protection levels [in Finnish]. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-kryptografiset-vahvuusvaatimukset-kansalliset-suojaustasot.pdf

Finnish Communications Regulatory Authority National Cyber Security Centre 2018. Guide for planning principles and solution models for gateway solutions [in Finnish]. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Yhdyskaytavaratkaisuohje.pdf

Annex 1. Secrecy and security classification assessment process.

Please note that the Act on International Information Security Obligations is not taken into account in the flow chart.



Annex 2. Table for the assessment of harm.

The table provides **examples** on assessing the harm required for security classification from the viewpoint of a single interest to be protected. The classification shall always be performed on a case-by-case basis on the basis of the risk assessment. It is recommended that the information management entity prepare sector-specific classification guidelines, for example in accordance with the below table.

	TL IV	TL III	TL II	TL I
Description	The unauthorised disclosure or unauthorised use of the secret information contained in the document can be disadvantageous to the interests to be protected.	The unauthorised disclosure or unauthorised use of the secret information contained in the document can cause prejudice to the interests to be protected.	The unauthorised disclosure or unauthorised use of the secret information contained in the document can cause significant prejudice to the interests to be protected.	The unauthorised disclosure or unauthorised use of the secret information contained in the document can cause grave prejudice to the interests to be protected.
Detailed description	Disclosure of the information may result in a consequence or event that does not necessitate suspension of operations yet may force a change in operational plans.	Disclosure of the information may result in a consequence or event that necessitates suspension of operations.	Disclosure of the information may result in a consequence or event that necessitates suspension of operations and causes operations to be prevented for a fairly long time.	Operations are suspended, prevented permanently. The harm is wide-ranging and concerns e.g. areas/functions key to the functioning of society, such as critical infrastructure or vital operations.
Interest to be protected: E.g. preparedness for emergency conditions	May possibly jeopardise the activities of the authority. E.g. documents of essential information systems such as security arrangements, vulnerabilities and audit reports, continuity and recovery plans.	Will likely jeopardise the activities of the authority. E.g. security arrangements for vital functions, continuity and recovery plans.	May possibly prevent the activities of the authority. The safety of a large number of people cannot be guaranteed. E.g. key documents concerning security arrangements, vulnerabilities and audits of vital functions and the information systems in support of these.	Will likely prevent the activities of the authority and the achievement of the purpose of the security arrangements.

MINISTRY
OF FINANCE

MINISTRY OF FINANCE
Snellmaninkatu 1 A
PO BOX 28, 00023 GOVERNMENT
Tel. +358 295 160 01
financeministry.fi

ISSN 1797-9714 (pdf)
ISBN 978-952-367-512-4 (pdf)

February 2021