Katakri 2020

Information Security Audit Tool for Authorities

National Security Authority of Finland

Foreword

The first Katakri - or the national security audit criteria - was finished in 2009 as part of the government's Programme for Internal Security. The work was led by the Ministry of Defence in close cooperation with other authorities and the business community. On completion of the first Katakri version the responsibility for the further development of the criteria was transferred to the Ministry of the Interior. The first updated version of Katakri was published in 2011.

In August 2012 the Ministry of the Interior established an advisory group, which then proposed to the relevant ministries (Ministry of Finance, Ministry for Foreign Affairs, Ministry of Transport and Communication, Ministry of the Interior, Ministry of Defence and the Prime Minister's Office) an idea to transfer the responsibility of the maintenance and administration of Katakri to the National Security Authority (NSA) in the Ministry for Foreign Affairs. The third version of Katakri, published in 2015, renewed the structure of the criteria, with the focus on the security of the Classified Information. The term Katakri is, however, so established and so well known that it was decided to maintain it also in the future as the name for the security audit tool for authorities.

The work to update and administer the fourth version of Katakri was done under the steering group, established by the NSA's cooperative working group. The steering group consisted of representatives of the ministries listed above, but also of the industry.

Katakri has proven a well working tool, giving added value in international information security cooperation both for authorities and for the industry. One of the triggering factors to the latest update was the need to cope with changes in the national legislation. The fourth version of the criteria pays special attention to the development steps of the digital data processing. Furthermore, it contains guidance to the use of the tool itself.

The revision work was coordinated by a steering group comprised of the following members:

Mikael Raivio, Deputy Director of NSA, Ministry for Foreign Affairs (chair)
Tuija Kuusisto, Senior Adviser for Information Management, Ministry of Finance (vice chair)
Rauli Paananen, National Cyber Security Director, Ministry of Traffic and Communications
Juha Pallaspuro, Chief Specialist, Prime Minister's Office
Tapio Pihlajamäki, Deputy Security Director, Ministry of Defence
Aki Tauriainen, Director, Finnish Transport and Communications Agency Traficom
Kari Santalahti, Chief Security Officer, Ministry of Interior
Elina Immonen, Director of Unit, Ministry of Traffic and Communications
Toni Lahti, Lieutenant Commander, Defence Command
Richard Wunsch, Lieutenant Commander, Defence Intelligence Agency
Ilkka Hanski, Head of Department, Finnish Security and Intelligence Service
Tuomas Hyvärinen, Senior Officer, Legal Affairs, Ministry of Defence
Reijo Kaariste, Lieutenant Senior Grade, Defence Command
Mikko Viitasaari, Security Director, UPM
Markku Rajamäki, Chief Specialist, Confederation of the Finnish Industries
Ville Jääskeläinen, Superintendent, Finnish Security and Intelligence Service
Tero Leppänen, Security Director, Insta Group
Ville Salmi, Legal Officer of NSA, Ministry for Foreign Affairs (secretary)

Subdivisions of Katakri were drafted in expert groups, consisting of:

Subdivision T – Security Management:

Juha Pallaspuro, Prime Minister's Office (chair)
Anna von Fieandt-Lehtonen, Finnish Transport and Communications Agency Traficom
Olli-Pekka Soini, Nixu Certification
Toni Lahti, Defence Command
Erja Kinnunen, Digital and Population Data Services Agency

Subdivision F – Physical Security:

Ville Jääskeläinen, Finnish Security and Intelligence Service (chair)
Janne Allonen, Finnish Transport and Communications Agency Traficom
Mika Tikkanen, Prime Minister's Office
Kalle Seppänen, UPM
Jani Rantanen, Defence Command

Subdivision I – Information Assurance

Tomi Kelo, Finnish Transport and Communications Agency Traficom (chair)
Niko Mäkilä, Prime Minister's Office
Antti-Ilari Söderholm, Prime Minister's Office
Ville Kuumola, Insta DefSec
Pinja Koskinen, Finnish Transport and Communications Agency Traficom
Henri Kettunen, Finnish Security and Intelligence Service
Juha Saarisilta, Finnish Air Force
Mikko Hakuli, Finnish Tax Administration
Mika Raappana, Government ICT Centre
Jarkko Majava, Nixu Certification
Pasi Koljonen, Defence Command
Pertti Pyysing, Defence Command
Jarmo Pietikäinen, Digital and Population Data Services Agency
Jan Partanen, Digital and Population Data Services Agency
Juha Huikari, Defence Forces C5 Agency

Contents

Traficom publication series

ISBN 978-952-311-767-9

29/2021

ISSN 2669-8757

Introduction

As an information security audit tool for authorities, Katakri can be used to assess the *capability of the organisation to protect national or international Classified Information* [1]. It brings together the minimum security requirements based on national legislation and international information security obligations. Katakri itself does not set mandatory requirements on information security [2] but is a compilation of existing national legislation and of such international information security requirements, which can be seen binding for Finland.

The most important pieces of legislation in the context of Katakri are the Act on Information Management in Public Administration (906/2019) and the Government Decree on Security Classification of Documents in Central Government (1101/2019), which are applicable in Finland for protecting national, as well as international Classified Information.

As an international source for requirements Katakri uses the Council Decision on the security rules for protecting EU classified information (2013/488/EU), which lays down the basic principles and minimum standards of security for protecting EU Classified Information (EUCI).

The structure of Katakri

The requirements in Katakri have been divided into three subdivisions. The aim of the **subdivision on security management (T)** is to ensure that the organisation has a well-functioning procedure to manage the security of information, as well as sufficient personnel security measures in place to protect the Classified Information. The **subdivision on physical security (F)** describes the security requirements for the physical environment where Classified Information is handled. In the **subdivision on information assurance (I)**, the security requirements for the IT environment are given.

Requirements have been set to allow different implementation options. To facilitate interpretation, examples of implementation have been compiled in the Additional Information field. This field contains examples of procedures to fulfil the minimum protection requirements in most of the cases. The examples given may be replaced by other protection means of an equal protection level. Recommendations of the Information Management Board, national VAHTI information security instructions, as well as policies and guidelines that complement the EU's Security Rules have been used as sources for the implementation examples.

[1] By the term "International Classified Information" Katakri refers to the Classified Information of the EU, but also to the Classified Information of NATO, ESA and OCCAR when applicable. The international Classified Information covered by bilateral information security agreements (General Security Agreements, GSAs) has to be, however, protected with protection means used to protect national Classified Information on the equal protection level. Potential special requirements set in each international information security agreement have to be taken into account on the protection of international Classified Information. Additional information concerning the international information security agreements in force is available on the portal of the Ministry for Foreign Affairs (https://um.fi/information-security-agreements-in-force-in-finland).

[2] Information Security consists of procedures used to protect the content of the information from unauthorized access (confidentiality), the unchanging of the information (integrity) and the availability of the information. Assurance methods of the information security may vary. The most usual ones are the methods to ensure the reliability of the personnel and the security of premises, the regulation about confidentiality and the restrictions to use the information only to purposes agreed, as well as requirements for information handling and transfer. Information security requirements cover the entire life cycle of the information. This includes the reception, modification, usage, transfer, archiving and destruction of the information. (Government proposal 66/2004). Information security measures consist of administrative, operational and technical functions to ensure the availability, integrity and confidentiality of the data. (Act 906/2019).

Requirements or given examples do not describe protection measures for every single environment or every special case. As an example, when handling Classified Information which may be a target for particular external interest, it is justifiable to use additional protective measures.

Usage

Katakri can be used as an audit tool for a Facility Security Clearance (FSC) to assess how a company's security arrangements are implemented and to assess the authorities' information assurance. The use case of the FSC is described more in detail in the Annex I. The use case for assessing information systems is described more in detail in the Annex II. Katakri may also be used as a common basis for security work and development between companies, communities and authorities.

The assessment of sufficient security arrangements shall be based on systematic risk assessment. Security risk management shall be used to implement a combination of security measures, which will create a satisfactory balance among user requirements, costs and residual risks. The Katakri security model and the role for risk management on different use cases are described in the Annex III.

Most of the protection requirements for the Finnish national and for the EU Classified Information are the same. Individual differences are indicated in the source references. Katakri may, hence, be used for assessing the security of both national and international Classified Information. The requirements set for the national information, classified to the security level IV (i.e. RESTRICTED), may be used as guidance when handling such unclassified national information which cannot be considered releasable for public.

Katakri, as such, is not meant to be used as a security requirement in public procurement. For public procurement, accurate security requirements should be defined separately by taking into account procurement related risks and special needs. A single procurement may involve other requirements than those collected for Katakri about handling and protecting Classified Information. The fulfilment of requirements which are not covered by Katakri can be assessed, for instance, by the authority owning the information used in the project.

Competent Authorities in Katakri supported use cases

When the security assessment is done as a part of the **national** Facility Security Clearance procedure, the competent authority for T and F subdivisions is either the Finnish Security and Intelligence Service or the Defence Command. For the subdivision I the competent authority is the Transport and Communications Agency Traficom (Act 726/2014, section 9). In use cases where international Classified Information is concerned, the Ministry of Defence, the Defence Command and the Finnish Security and Intelligence Service act as specialist authorities under the National Security Authority on Security Areas dealing with personnel, enterprises and facilities. On the field of information assurance the Transport and Communications Agency Traficom has this same authority (Act 588/2004, section 4). In **international** Facility Security Clearance (FSC) processes the competent authorities for subdivisions T and F is either the Finnish Security and Intelligence Service or the Defence Command. For the subdivision I the competent authority is the Transport and Communications Agency Traficom.

When the assessment is done according to the Act on the Assessment of Security of Public Authorities' Information Systems and Telecommunications Arrangements (1406/2011), the Transport and Communications Agency Traficom assesses, whether the information system or the communication system arrangement fulfils those requirements, which have been chosen as the basis for the assessment (Act 1406/2011, section 7). On cases, when the assessment of the information system handling national Classified Information is done by an Information Security Inspection Body approved by the Transport and Communications Agency Traficom (Act 1406/2011, section 3), the Information Security Inspection Body is obliged to act according to the conditions set in the approval process by the Transport and Communications Agency Traficom. This is to guarantee that those parts of the assessment process, which require the assessment of the competent authority are done by the Transport and Communications Agency Traficom.

Area of application

On use cases supported by Katakri (Acts 726/2014, 588/2004, 1406/2011) the handling of Classified Information has to take place entirely under the competency of authorities addressed in the Finnish legislation. Special cases include, for example, international projects where the responsibilities of competences and inspections are separately agreed on between the security authorities of the relevant countries and where the information dealt with can be shared between the authorities of the countries involved.

Katakri has been established as a tool for normal times and conditions and it does not, for instance, handle the specific planning needed for exceptional conditions. However, when the authority owning the information so approves, Katakri may be used also for exceptional situations, like for virus pandemic or military conflicts.

International readers are asked to bear in mind comparisons of Finnish national security classification levels to the ones used internationally (EU, NATO):

- Finnish classification level IV equals RESTRICTED
- Finnish classification level III equals CONFIDENTIAL
- Finnish classification level II equals SECRET.

In cases where a requirement is valid only for Finnish national classified information, this has been separately noted in the text.

Subdivision T: Security Management

This subdivision deals with the methods through which security and its management are implemented to be part of the entire organisation's activities. Security management, which comprises both administrative information security and personnel security aims at a well-functioning information security management system and at sufficient methods to ensure that the personnel handles Classified Information of authorities in an appropriate manner.

Security management should be an integral part of an organisation's management. On the basis of risk assessment, information security management procedures should be seen in relation to the protection of Classified Information and the organisation's activities.

Reviewing of security management should be focused on that part of the organisation, which has an impact on how Classified Information is handled. This may be the part of the organisation, which manages the IT environment, such as a subsidiary or equivalent. Especially when personnel security requirements are assessed, it should be noted that sufficient implementation may vary from one organisation to another. For example, the contents of the instructions for personnel handling information in classification level II (SECRET) generally varies significantly from instructions meant for the entire organisation.

The organisation has to ensure that requirements to protect Classified Information are followed also in situations where the handling of information is based on the commission of the organisation itself.

The documentation of practices and especially of risk management is an integral part of proper security management.

The plans and the instructions, as well as the results and conclusions of the assessment should be presented in a written form. It is advisable to include the information of the outcome of taken measures into this documentation. The outcome may address the effectiveness of the assessments in the security management process. The term documentation refers in this context to a record, such as an internet page or a ticket in the resource planning system, which can be produced into a written format.

Administrative Information Security

T-01 – SUPPORT FROM THE MANAGEMENT, GUIDANCE, RESPONSIBILITIES – SECURITY PRINCIPLES

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/ EU)
The management of the organisation is responsible for a) approved by the senior management, the organisation has introduced security principles, which describe how information security measures are linked to the organisation's activities. b) security principles are comprehensive and appropriate for the protection of Classified Information. c) security principles provide guidance for security measures, and d) sufficient monitoring has been put in place to ensure that the organisation follows the requirements and guidance on the handling of Classified Information.	906/2019 section 4 (1 and 2)	Art 9(1)

Additional information

General: The support, guidance and responsibilities of the management are expressed in the security principles approved by the top management, indicating how the information security measures are linked to the organisation's activities. This shows that the management of the organisation is committed to security principles and that these principles express the ambition of the management, thus supporting the functions of the organisation. Principles may be expressed in various forms, for example in a single document or as a part of general operating procedures, policy or strategy. The approved security principles are adequate and appropriate for the protection of Classified Information and they are guiding the information security functions. The realization of information security functions is followed and reported regularly to the top management. The management has to make sure that sufficient control methods are in place for the realization of statutory orders, regulation and guidance in information management. The surveillance of the information management, as well as the handling of Classified Information on general level is the responsibility of the management of the organisation together with respective forepersons. The monitoring can also be done automatically in information systems through various control methods. It is recommended that the organisation describes the monitoring responsibilities of the management and forepersons, including the method for evaluating the quality of the monitoring system.

Other sources of information: SFS-EN ISO/IEC 27002:2017 5.1.1; SFS-EN ISO/IEC 27001:2017 5.1, 5.2, 5.3, 9.3; PiTuKri TJ-01; Recommendation of the Information Management Board 2020:18

T-02 – DEFINING THE TASKS AND RESPONSIBILITIES OF THE SECURITY MANAGEMENT

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/ EU)
The organisation has defined the tasks and responsibilities of security management.	906/2019 section 4 (1 and 2)	Art.7(5)

Additional Information

General: The goal of defining security tasks and responsibilities is to ensure that responsible people are designated for the key subareas and that they are aware of their responsibilities and competences. Tasks related to information security have to be written into rules of procedures and job descriptions of the organisation and the employees, as well as to operating instructions. The management of the organisation is tasked to define the responsibilities for the management of the handling of Classified Information. It is not a question of delegating responsibilities of the information management, but defining them. Areas of responsibility should include especially the maintenance of information security guidelines, risk management, preparedness and the persons generally responsible for the security of information.

Example of the implementation: The organisation has defined the tasks and responsibilities for security implementation at least in the following areas:
a) security management
b) physical security
c) information assurance.

Description includes the responsibilities of the owner of the handling environment for Classified Information and other information security related responsibilities. Responsibilities are defined for monitoring the coverage of the information security documentation and ensuring that it is up-to-date. Accessible on a need-to-know basis, the documentation covers the processes of and the handling environments for Classified Information during the entire life cycle of information.

To be notified in Facility Security Clearance procedures: the target organisation needs to have a Facility Security Officer (FSO). FSO is the person who has sufficient security skills and who has been nominated by the management of the organisation to look after security in cases where the protection of Classified Information is dealt with. The FSO works in close cooperation with competent security authorities. The FSO ensures that the organisation, which is under the FSC evaluation, will implement the security measures required.

Other sources of information: SFS-EN ISO/IEC 27002:2017 5.1.1; SFS-EN ISO/IEC 27001:2017 5.1, 5.2, 5.3, 9.3; PiTuKri TJ-01; Recommendation of the Information Management Board 2020:18

T-03 – MANAGEMENT OF INFORMATION SECURITY RISKS

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/ EU)
The organisation has assessed the essential risks for Classified Information and established the information security measures accordingly.	906/2019 section 13(1) 1101/2019 sections 6 and 7	Art. 5, Annex IV (4–7) and (12)

Additional Information

General: The management of information security risks consists of a systematic, coordinated and continuous action, which makes it possible to analyse, estimate, handle and follow information security risks. The information security risk handling process includes the definition of the handling environment, risk assessment (recognition, analysis, estimation of significance), risk handling, risk approval (appetite), risk communication, risk monitoring and audits. The security model which Katakri uses, as well as the role for risk management in use cases supported by Katakri, is described in Annex III.

Example of the implementation:

1. The management of information security risks is part of organisation's operation and management of other risks.
2. The management of information security risks ensures that sufficient information security measures to protect Classified Information are in place.
3. The procedure for assessing and analysing information security risks produces appropriate and understandable information for the decision-making.
4. Information security risks are managed by sufficient amount of specialized personnel.
5. The management of information security risks takes care of risks deriving from other organisations and supply chains. Ref. risks concerning supply chains for security critical devices and software (requirements I-01, I-12 and I-13).
6. The results of the assessment and analysis of information security risks are used in the planning and in the implementation of the protection of Classified Information, in the assessment of the impact of security incidents, in the change management and when possible, in procurement.
7. Information security measures are scaled based on risks and taking into account, e.g., the classification level, quantity, format, classification justification and storage of the information with relation to the assessed risks.
8. The organisation has documented the relevant parts of the monitoring and security measures, as well as the risk assessment, which these measures are based on.

Other sources of information: SFS-EN ISO/IEC 27001:2017 chapter 6.1 and chapters 8-10, SFS-EN ISO/IEC 27005:2018 chapter 6, SFS ISO 31000:2018, VAHTI 22/2017; PiTuKri TJ-03; Recommendations of the Information Management Board 2020:29 and 2020:61.

T-04 – SECURITY GUIDANCE

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/ EU)
The organisation possesses up-to-date guidance for the handling of Classified Information, for the use of information systems, for access rights to the information, for realization of responsibilities in information management, for realization of access rights to the information and for information security measures. **Security instructions cover the processes and handling environments that are related to Classified Information during the entire life cycle of the information.**	906/2019 sections 4 and 13; 1101/2019 sections 6 and 8	Annex I (29–31) Annex IV (21–22)

Additional Information

General: Documentation of essential security issues ensures that the operation does not depend on certain individuals.
Ref. The role of documentation in change management and in the ability to observe deviations and incidents (I-16).

It is the responsibility of the management of the organisation to ensure that the organisation has up-to-date guidance for the handling of information, for the use of information systems, for access rights to the information, for realization of responsibilities in information management, for realization of access rights to the information and for information security measures. In reality, it is the management of the organisation which defines how the up-to-dateness of the guidance is ensured and who is responsible for this procedure. It is recommended that the responsibility to keep the guidance up-to-date is given to those, who bear the general responsibility for information security, information systems, data storage, registers, decisions for publishing documentation on demand, case management and archiving.

Example of the implementation:

1. In case the person is due to handle Classified Information, the person will be guided through the security regulation and procedures for protecting the information. When handling Classified Information of the EU or NATO, it is required that the person signs an affirmation to protect this information.
2. The security guidance takes into consideration the needs deriving from the duties of the personnel.
3. The scale and the up-to-dateness of the security guidance is monitored regularly and the guidance is available for all who need it.

Other sources of information: SFS-EN ISO/IEC 27002:2017 7.2.2, 5.1.1, 5.1.2, 12.1.1; SFS-EN ISO/IEC 27001:2017 7.5; VAHTI 4/2003; VAHTI 2/2008; PiTuKri HT-04; Recommendation of the Information Management Board 2020:18.

T-05 – RESOURCES FOR THE SECURITY WORK

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/ EU)
There is a sufficient level of expertise in the organisation to ensure information security.	906/2019 section 4(2)	Annex IV (4)

Additional Information

In general: A sufficient level of expertise ensures that the goal for information security is achieved and the measures to mitigate risks are introduced in a cost-effective way. Sufficiency of resources is regularly assessed.

As general requirements, it can be seen that the organisation has an adequate number of personnel, the personnel has sufficient knowledge about security and up-to-date instructions and security training has been implemented, appropriate tools are used and that the monitoring of security actions and inspections has been organised.

Example of the implementation:

1. Personnel responsible for security have the needed expertise and this has been verified.
2. Resources, tasks, responsibilities and authorisations of the security work have been defined comprehensively enough, bearing in mind the functions, size and risks of the organisation.
3. There are enough resources to create, build, maintain and constantly improve the management system for information security.
4. Sufficiency of resources is regularly assessed.

Other sources of information: SFS-EN ISO/IEC 27001:2017 7.1, 7.2, 5.1

T-06 – MALFUNCTIONS AND EXCEPTIONAL SITUATIONS

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/ EU)
The organisation has defined preventive and corrective measures to minimize effects of significant malfunctions and exceptional events to the handling and storage of Classified Information. a) The organisation has noted the need to protect Classified Information in emergency OR in disruptive situations. b) Protective measures are considered adequate to prevent unauthorised access and disclosure to Classified Information and to ensure the integrity and availability of the CI. c) Classified Information has been protected against technological and physical accidents.	906/2019 15.1 §	Art.5 (3–4)

Additional Information

In general: The organisation has to have confidence about the protection of the system or information handled in emergency OR in disruptive situations. These situations may be fires, water leakages, vandalism or unauthorized intrusion, as well as physical damages caused with electronic means, such as device breakdowns. When protecting the information or the system the protective measures have to be appropriate, but proportioned to the risk analysis.

The key personnel for the protection of Classified Information throughout the life cycle have to be defined. The organisation has to be able to protect the Classified Information even in situations when the key personnel are inhibited to take action.

Other sources of information: SFS-EN ISO/IEC 27002:2017 17.1.1, 17.1.2, 17.2.1, 12.3.1, 16.1.2, 16.1.6; VAHTI 2/2009; VAHTI 2/2016; PiTuKri TJ-05; Recommendation of the Information Management Board 2020:61, chapter 6.

T-07 – MANAGEMENT OF SECURITY EVENTS

Requirement	§ Source (906/2019 and/ or 1101/2019)	§ Source (2013/488/EU)
1. **Detected or possible security event, which has put the security of international Classified Information in danger, has to be reported immediately to the competent security authority.** 2. **The organisation has a set of procedures in place to handle security events.** a) The organisation has the guidance and procedure in place to immediately share information within the organization about such a detected or suspected security event, which may have put the Classified Information in danger. b) The organisation has defined the persons/actors to whom to report on (possible) security events. c) The organisation has figured out, what kind of security events trigger the communication with authorities.	1. – 2. 906/2019 section 4(2) and section 13; 1101/2019 section 7	1. Art. 5(4), art.14(3) 2. Art. 5(4), art.14(3)

Additional Information

In general: The reason for the management of security events concerning Classified Information is to ensure that the organisation is able to operate efficiently in unwanted and unexpected situations and thus is able to minimize the damages and to recover the normal situation and to ensure that similar events cannot happen elsewhere within the organisation. The organisation needs to have a process to deal with exceptional events. The process has to include the definition method for the gravity of the situation, mechanisms to prevent further damage, to collect evidence, to sort out the situation, to take corrective actions and to learn about the event. Sufficient resources are also needed to handle exceptional situations.

Classified Information can be seen endangered, when it has been disclosed or has possibly been disclosed to unauthorized people. Most owners of Classified Information (such as EU), as well as authorisations which are in force, require immediate communication about such security events, which have (possibly) put the Classified Information in danger.

Example of the implementation: Management of security events is

1. planned
2. provided with instructions/training,
3. documented on a sufficient level in view of the handling environment,
4. practised, and in particular
5. communication practices and responsibilities have been agreed on, and furthermore,
6. defined, which national and international regulation or contract signed by the organisation require communication about security events or about their possibility, and what is the procedure for communicating.

Other sources of information: SFS-EN ISO/IEC 27002:2017, chapter 16, 6.1.3; VAHTI 8/2017; PiTuKri TJ-04

T-08 – CLASSIFICATION OF INFORMATION

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/ EU)
This requirement will apply only on the information management of authorities **1. Information has been classified on the basis of statutory requirements:** a) The authority has instructions for classification of information. a) Classified Information (including drafts) is marked to indicate the protection level. b) A document is marked to indicate the highest classification level of its parts (e.g. annexes). c) If the classification level of the main document and annexes is not the same, this must be indicated in the document.	906/2019 section 18; 1101/2019 sections 3 and 5	Annex III (2,6 and 7)

Additional Information

In general: The purpose of classification is to identify and scale correctly the security measures based on protection needs. Depending on the information, handling environment and users, classification may be indicated in various ways. By classifying handling environments according to the level of Classified Information it is possible to indicate clearly the security measures related to each IT environment.

The classification of an information system or a target containing several data sets is primarily defined by the highest classification level of information included. If the amount of Classified Information is big, there is a need to estimate, whether the protection level should be elevated (i.e. aggregation effect).

Information generated for or received from the authority will be classified by the authority. The classification marking may also be done by the authority.

Other sources of information: Recommendation of the Information Management Board 2020:19; SFS-EN ISO/IEC 27002:2017 8.2.1, 8.2.2; PiTuKri TJ-06

Personnel Security

T-09 – CHANGES IN THE HANDLING OF CLASSIFIED INFORMATION THROUGHOUT THE EMPLOYEMENT

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/ EU)
The changes in the handling of Classified Information are noted in different phases of the life cycle of the employment. Special attention has to be paid to the measures in recruitment, in changes of responsibilities and in the termination of the employment contract.	906/2019 section 4(2), section 12, section 16; 1101/2019 sections 6 and 8	Annex I (29 and 31)

Additional Information

In general: The measures during the employment are, e.g., personnel security clearances, handling rights, rights to use, access rights, awareness of the responsibility for not disclosing information, security training, and keeping all of these updated when changes occur, including the training sessions before changes. Measures when terminating the employment are, e.g., collection of keys, badges and Classified Information and Material, as well as deletion of access rights, handling rights and rights to use the above mentioned. When terminating the employment contract it is also necessary to remind about remaining responsibilities concerning non-disclosure and secrecy. The measures described here typically require documented instructions, which have been taught and are available for personnel involved. Instructions may be divided into parts, according to the periods of the employment. Such periods might be the instruction for recruitment, introductive instructions, instructions for changes in responsibilities, instruction for the termination of the employment contract and specific instructions for, e.g, changes in the rights to handle, use or access.

Other sources of information: SFS-EN ISO/IEC 27002:2017 7.1, 7.2, 7.3; PiTuKri HT-01

T-10 – ASSESSMENT OF THE TRUSTWORTHINESS AND RELIABILITY OF THE PERSONNEL

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/ EU)
1. **The trustworthiness and reliability of individuals handling Classified Information is determined, if necessary, by means of security clearance methods for the relevant level.** 2. **When international information security requirements so demand, the person may be given access to the information classified to classification level III (CONFIDENTIAL) and higher only after the person has been issued a Personnel Security Clearance (PSC) for the respective level.**	906/2019 section 12	Annex I (2c, 2b and 29)

Additional Information

In general: The authority has to recognize those functions, which require special trustworthiness and reliability concerning the personnel employed or working for the authority. The Personnel Security Clearance is sought by the authority, which owns the Classified Information.

The clearance will be sought from the Finnish Security and Intelligence Service, which will then decide if the clearance procedure is needed. The clearance will be sought from the Defence Command - which also decides the need for the clearance - in cases when the person involved is about to work for the Defence Forces or in cases when the clearance is sought as a part of procurement procedures of the Defence Forces. The PSC can be based on concise, basic or comprehensive scale investigations, depending on the Classified Information at stake.

When the need for the Personnel Security Clearance arises from international information security requirements, the National Security Authority in the Ministry for Foreign Affairs will be addressed. For example, handling of Classified Information of EU or NATO belonging to classification level CONFIDENTIAL or higher requires a PSC.

Other sources of information: Act on security clearances 726/2014; Act on international information security obligations 588/2004.

T-11 – NON-DISCLOSURE AND CONFIDENTIALITY COMMITMENT

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/ EU)
Security principles and procedures for protecting Classified Information have been sorted out for the personnel dealing with it and the personnel has signed an agreement for non-disclosure and confidentiality. **Non-disclosure agreement or confidentiality commitment is in place in cases where the person handling Classified Information is not bound by the responsibility of an official.**	1101/2019 sections 6 and 8	Annex I (2 and 29)

Additional Information

SFS-EN ISO/IEC 27002:2017 7.1.2, 13.2.4; PiTuKri HT-03

T-12 – SECURITY EDUCATION

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/ EU)
1. The management has to make sure that the organisation offers education, which ensures that the personnel and other people working for the organisation have appropriate knowledge of relevant legislation, rules and regulations for information management, data management, as well as of the publicity and non-disclosure of the information (ref. T-04). **2. Threats against Classified Information and the updated instructions (ref. T-04) have been taught for the personnel.** **3. The education and training concerning the handling of Classified Information is done on a regular basis and the participation is registered.**	906/2019 sections 4 and13; 1101/2019 sections 6 and 8	Annex I (29–31), Annex IV (21–22)

Additional Information

In general: The management of the organisation has to make sure that the organisation offers education which ensures that the personnel and other people working for the organisation have appropriate knowledge of the relevant legislation, rules and regulations for information management, data management, as well as publicity and non-disclosure of the information.

In practice, the management has to make sure that the education plan of the organisation covers the sufficient lessons on the handling of Classified Information, of data management and of rules and regulations linked to Classified Information.

The education may be regular or based on the need stemming from discussions with the personnel.

Example of the implementation:

1. All individuals who handle Classified Information have been made aware of security instructions and procedures concerning the protection of information. Handling of the EUCI and NATO's Classified Information requires that the individuals also acknowledge in writing their obligations to protect such information.
2. Security education and instructions are carried out, targeting to the needs which the personnel experience in their work.
3. The contents of security education are documented.

Other sources of information: SFS-EN ISO/IEC 27002:2017 7.2.2, 5.1.1, 5.1.2, 12.1.1, 7.5; VAHTI 4/2003; VAHTI 2/2008; PiTuKri HT-04; Recommendation of the Information Management Board 2020:18.

T-13 – NEED-TO-KNOW AND ACCESS RIGHTS

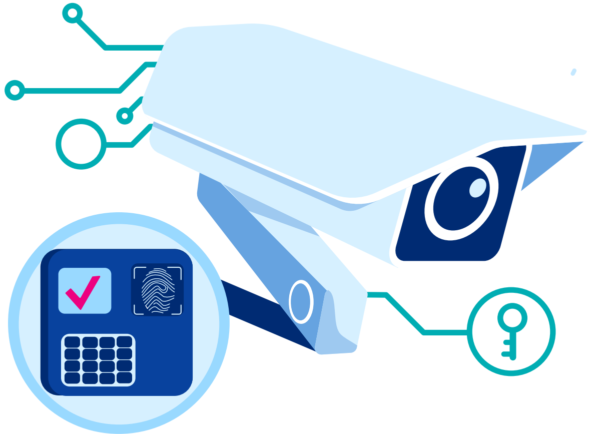
Requirement	§ Source (906/2019 and/or1101/2019)	§ Source (2013/488/EU)
1. An up-to-date list of personnel with access rights to Classified Information on classification level II and III (SECRET and CONFIDENTIAL) is maintained in the organisation. **2. The above mentioned list has to include the tasks on which the right to handle Classified Information is based on.** **3. Access to Classified Information can only be granted after an individual's task-based need-to-know has been determined.** **4. The organisation has a procedure in place to remove an individual's access rights after the need-to-know has ended.**	906/2019 sections 12 and 16; 1101/2019 section 8, section 11 (1)3.	Annex I (2a and 3)

Additional Information

In general: It is easier to determine the need-to-know when the organisation has described the principles to Classified Information and processes for granting task-based access and managing it in changing situations. In addition a process or guidance needs to be described for granting and administering the access rights based on tasks. In determining handling rights, tasks and roles it should be ensured that dangerous role combinations are not created.

Other sources of information: SFS-EN ISO/IEC 27002:2017 9.1.1, 9.1.2, 6.1.2; VAHTI 2/2008; PiTuKri HT-05

Subdivision F: Physical Security



The term *physical security* refers to the implementation of physical and technical security measures in order to prevent unauthorised access to Classified Information. The subdivision of physical security (F) may be used to estimate the adequacy of security measures to protect national or international Classified Information (Decree 1101/2019, section 9; Act 588/2004, section 10).

Information of authorities needs to be handled and stored in premises, which are secure enough to cover the requirements set for the confidentiality, integrity and availability of the information (Act 906/2019, section 15). When designing and planning new facilities, physical security requirements and their functional definitions have to be part of the construction planning. Concerning the existing premises, physical security requirements have to be put in place as completely as possible (2013/488/EU, annex II (7)).

In order to physically protect Classified Information, two types of physically protected Security Areas can be defined: *Administrative Areas and Secured Areas* (including *Technically Secured Areas*). Objectives for physical security measures have to be fulfilled before security areas can be approved for use.

Risk assessment for physical security, as well as the effectiveness of individual security measures and of the entire defence-in-depth (i.e. multilayer protection) has to be reconsidered on a timely manner and in conjunction with each audit (2013/488/EU, annex II, section 11). The NSA unit of the MFA, using the expertise of the Finnish Security and Intelligence Service or the Defence Command (Act 588/2004, section 4; 2013/488/EU, Art. 8), always accredits areas, where international Classified Information will be stored.

The structure of the subdivision F is formed in a way that the minimum requirements for each security areas are collected on separate chapters. Using this renewed structure the auditor can see all the minimum requirements and additional information concerning the security area to be audited in a well-structured way, without having the need to jump between the requirements. The requirements for different security areas are partially equal.

The choice of sufficient security measures is always based on risk assessment results. However, in the column desired level, which has been added to minimum requirements, a sufficient level or guidance to match the standard has been presented for most of the defence-in-depth cases.

At the end of the subdivision F there is a dedicated data security section for Classified Information in a paper format. This section has been compiled for practical reasons to facilitate the audit procedure itself.

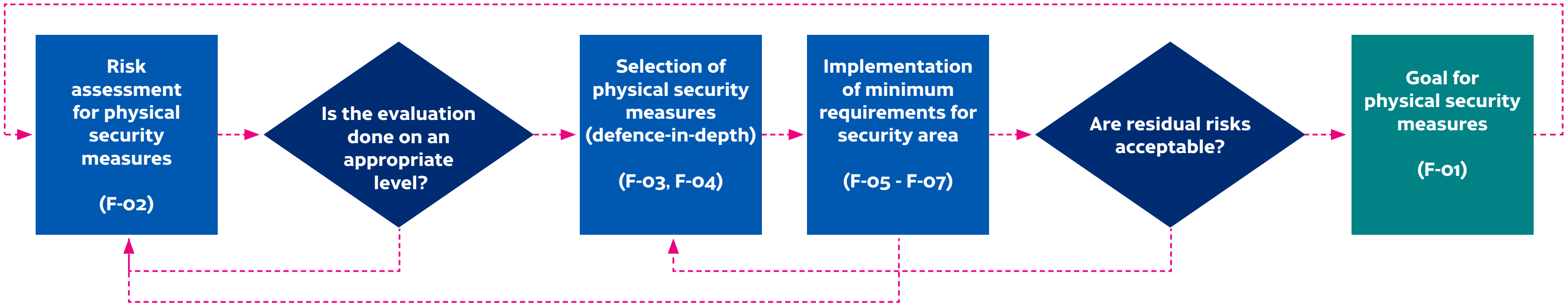
The life cycle management of the data has been covered in the data security section. The data security requirements for the electronic handling of Classified Information have been covered in the subdivision I.

The physical security evaluation process, mentioned above, has been described in the figure below. The subdivision F of Katakri 2020 has been formed to proceed according to this process.

In the beginning one has to identify the Classified Information handled in the organisation and to evaluate the risks for the physical environment (F-02). The auditor must pay attention to the sufficiency of the risk assessment and, when needed, to ask for a new evaluation. The results of the risk assessment are notified (Act 906/2019, section 13) in the selection of physical security measures (F-03). The requirements F-05 - F-07 concentrate on Security Areas to protect the Classified Information and on their minimum requirements. The minimum requirements have been directly derived from the recommendation for handling classified documents, given by the Ministry of Finance (VM 2020:19). This recommendation is based on the decree 1101/2019, concerning the classification of documents within the government.

After fulfilling the minimum requirements together with defence-in-depth protection principle the auditor evaluates physical security measures and considers if the residual risks are on acceptable level. When needed, the measures to fulfil defence-in-depth principle may be corrected until the auditor is ready to accept residual risks and can be sure that the objective for physical security measures is fulfilled (F-01). The risk assessment and the effectiveness of individual security measures, as well as the entire defence-in-depth principle have to be re-evaluated on a timely manner and as a part of each audit.

.


Risk assessment for physical security measures
(F-02)
Is the evaluation done on an appropriate level?
Selection of physical security measures (defence-in-depth)
(F-03, F-04)
Implementation of minimum requirements for security area
(F-05 - F-07)
Are residual risks acceptable?
Goal for physical security measures
(F-01)

Picture: Evaluation process for physical security measures

General Requirements

F-01 – Goal for physical security measures

F-01 – GOAL FOR PHYSICAL SECURITY MEASURES		
Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/ EU)
1. **The goal for physical security measures is to prevent unauthorised access to Classified Information by:** a) ensuring that Classified Information is handled and stored in an appropriate manner ; b) ensuring that the access to Classified Information for the personnel is based on the need-to-know and the personnel has been cleared to the required classification level when needed; c) deterring, impeding and detecting unauthorized actions ; and d) denying or delaying surreptitious or forced entry by intruders	1. 1101/2019 sections 7 and 10; VM 2020:19, 12 and 18	1. Annex I (2)
Additional Information		
In general: Requirements for physical security measures have to be fulfilled before the Security Area can be accredited.		

F-02 – Risk assessment of physical security measures

The choice of physical security measures has to be based on risk assessment. Risk management process must be used to protect Classified Information on the premises of the organisation, in order to ensure that the physical security measures match the risks evaluated, that residual risks might be accepted and the chosen security measures fulfil the requirements (F-01).

When evaluating the risks and the chosen security measures, interpretations of both the organisation to be audited as well as of the auditor have to be taken into account. The organisation to be audited, as well as the auditor have to accept the residual risks concerning physical security measures. The organisation has to be able to point out the rationale for the chosen measures.

F-02 – RISK ASSESSMENT

Requirement	§ Source (906/2019 and/ or 1101/2019)	§ Source (2013/488/ EU)
1. A risk management process has to be applied for protecting confidential information on the premises to ensure that a commensurate level of physical protection is afforded against the assessed risk. **2. The risk management process has to take into account all relevant factors, in particular :**	1. 906/2019 section 13(1); VM 2020:19, 12 and 18 2. VM 2020:19, 12 and18 3.	1. Annex II (3) 2. Annex II (3) 3. Annex II (3)

a) A risk management process has to be applied for protecting confidential information on the premises to ensure that a commensurate level of physical protection is afforded against the assessed risk.
b) Ways of handling and storing Classified Information, bearing in mind that large amounts of Classified Information compiled together might cause a need to strengthen the risk management measures.
c) The handling and storage time of Classified Information.
d) The environment for the handling and storage of Classified Information (Security Area): surroundings of the facility, location inside the facility or at one of its parts;
e) Reaction time in alarm situations;
f) Outsourced functions, like maintenance, cleaning and security services
g) The estimated threat to the information caused by intelligence services, criminal actions or own personnel;

3. In case the Classified Information is international by nature, the choice of controls and risk assessment has to be based on the threat assessment of the Finnish Security and Intelligence Service or the Defence Command.

Additional Information

In general: In the risk assessment the principles of, e.g., need-to-know, separation of duties and least privileges, embedded in processes dealing with access control management and other security arrangements have to be taken into account. Risk assessment of physical security measures has to be done regularly as one part of the risk management process of the organisation. All evaluated risks must be connected to nominated risk owners. The risks related to the changes of accredited physical security measures have to be evaluated in association with the changes. Especially when taking compensatory physical security control measures, the rationale has to be indicated.

F-03 – Selection of physical security measures (defence-in-depth)

The results of the risk assessment of physical security measures (F-02) have an impact on the selection of physical security measures which need to be implemented using the principle of defence-in-depth (F-03) in addition to the minimum requirements (F-05 - F-07) to fulfil the goal (F-01) for physical security measures. The necessity of security measures has to be evaluated one Security Area at a time. This means that not all physical security measures are needed on each situation or on all Security Areas. The evaluation of security measures is a complexity, consisting - e.g. - of taking into account the physical security of such spaces where terminals or other electronic devices and cross-connections are located.

The principle of defence-in-depth means implemention of number of security measures which complement each other. When possible, security areas and other premises around form together nested zones, where the Security Areas are located in the middle. An example of the defence-in-depth: physical security measures have been implemented in a way, where the possible intruder will be detected already at the outer boundary of the facility, thus making it possible for the security personnel to move onto the Security Area and be ready to prevent the intrusion.

The Security Areas and the premises around slow down the intrusion and together with the security personnel finally prevent intrusions. In normal situations, the zoning of premises and the limitation of access rights to the information only for those who have the need-to-know, are good enough to prevent unauthorized access to Security Areas and to Classified Information from the own personnel without need-to-know. In addition, security systems record the information, which can be used to investigate possible unauthorized actions.

F-03 – SELECTION OF PHYSICAL SECURITY MEASURES (DEFENCE-IN-DEPTH)

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/ EU)
1. In Security Areas and in premises around, preventive and limiting measures have to be taken into use to ensure the security of the Security Area. Actions to detect and track the intensives have to be included. Procedure to recover normal functions immediately has to be in force. **2. The principle of defence-in-depth has to be used to evaluate and accredit an appropriate and - based on risk assessment - sufficient combination of security measures, consisting of administrative, functional and physical means, like:** a) structural barriers: physical obstacle(s) which sets the boundary for Security Areas and the premises around it, causing complications and delays for the intrusion;	1. 1101/2019 section 7 2. VM 2020:19, 13 and 19 3. VM 2020:19, 23	1. – 2. Annex II (4) 3. Annex II (10)

F-03 – SELECTION OF PHYSICAL SECURITY MEASURES (DEFENCE-IN-DEPTH)

b) Access control: access to Security Areas and premises around them is limited with access control mechanisms. The goal is to detect unauthorised attempts, to prevent the access of unauthorised people and to monitor the individuals moving around and inside the area. Access control may be targeted on an area, on one or more facilities on the area, on areas within facilities or on rooms. The monitoring may be based on mechanical or electronic systems or on the combination of these or on some other physical means. Security personnel, receptionist and own personnel may be used as part of the monitoring procedure.
c) Intrusion detection system: in order to improve the security level given by a perimeter barrier, an intrusion detection system (burglar alarm) may be used. The system may also be used in place of, or to assist, security staff.
d) Security personnel: trained, supervised and, where necessary, appropriately security-cleared security personnel may be employed, inter alia, in order to deter individuals planning covert intrusion.
e) CCTV: closed circuit camera surveillance may be used on Security Areas or around it especially for preventing illegal intelligence actions and other unwanted actions, as well as for verification of alarms and unexpected findings. The security personnel may use CCTV as a real time tool for monitoring or as a passive means to analyze the footage.
f) Measures which maintain the level of security: Definition of responsibilities and tasks. Various processes and working models, like the management of access rights and keys, introduction of new personnel and instructing them, and the service and maintenance processes of different systems.
g) Lighting: the possible intruder may be detected with the help of proper lighting. It also makes the monitoring of the area more efficient for the guarding personnel either visually or by using the CCTV.
h) Other relevant physical measures aiming at preventing or detecting unauthorised access or to prevent the loss or damage of Classified Information.

3) The devices have to be inspected and serviced on a regular basis.

Additional Information

In general: The use of devices and systems based on European standards and on their minimum requirements is recommended, when used as a part of defence-in-depth system. The table below describes standards, which can be used as minimum references. The choice of the right standard class is always based on the evaluation of risks. However, on the column desired level one can find a sufficient class or instructions to cover most defence-in-depth implementation needs. The fulfilment of the desired level is not mandatory for the approval of a single security procedure, because the evaluation of physical security measures is based on the evaluation of risks and on the complexity of defence-in-depth. In some cases it is possible to require higher level security measures than the desired level to be used, based on the risk assessment.

F-03 – SELECTION OF PHYSICAL SECURITY MEASURES (DEFENCE-IN-DEPTH

Security equipment and systems	Reference standard	Classes on Standard
Safes	SFS-EN 1143-1	I – V
Element vaults	SFS-EN 1143-1	I – XII
Paper shredders	DIN 32757 (old)	DIN 1 – DIN 6
	DIN 66399 (new)	P1 – P7
Locks and their assembly parts	SFS 7020 (+SFS 5970)	1 – 4
Electronic access control systems	SFS-EN 60839-11-1 , SFS-EN 60839-11-2	1 – 4
CCTV	SFS-EN 62676	–
Walls, doors, floor and ceiling structures	SFS-EN 1627	RC1 – RC6
Windows (security glass)	SFS-EN 356	P4A – P5A and P6B – P8B
Intrusion detection systems	SFS-EN 50131	1 – 4
Alarm relaying in intrusion detection systems	SFS-EN 50136-1	DP1 DP4 and SP5 SP6
Alarm centres of the Security Company	SFS-EN 50518	–

When evaluating the equipment and systems it is important to verify that they are in operational condition and suitable for the cause. Documentation of inspections from the time of the delivery and when in use, as well as all service functions should be available. When evaluating system rights, the principle of least privilege and separation of duties should have a special focus.

Security equipment and systems should be located inside the Security Area they are used to protect for. The installation, inspection, service and cleaning operations of security equipment and systems and the premises they are located in may be carried out only by personnel authorized with individual access rights to the area or under supervision of such a person.

Remote connections and remote installations of security equipment and systems shall be done in a secure way and based on the risk assessment, in order to give access from authorised terminal devices or networks only and to ensure that interfaces between communication systems and devices are secure enough to prevent unauthorised access to the information transferred.

.

F-04 – Handling and storage of information

Classified Information must be handled in the way that the access of unauthorised people to the information is prevented in all conditions. Prevention means the protection of the information from such people who do not have the need-to-know for the information at stake, as well as from illegal intelligence actions.

Protection means the preventions of, e.g., direct visual OR oral connection to the Classified Information and sufficiently secure storage of the equipment, which contains such information.

When handling Classified Information also the pauses in the work have to be organised in a way which does not put paper documents or data equipment in danger. In most of the cases these will be put into security containers or into Security Areas fulfilling the requirements for the specific classification level. The term storage refers to situations where the information is not directly supervised or controlled by the handler.

The general rule is to handle and store Classified Information within Security Areas (F-05 - F-07) but there are situations - like remote working or other tasks outside the perimeter of Security Areas - when there is a need to handle Classified Information outside this general rule.

In Katakri the term *terminal device* means an information system or a part thereof, which is used by the individual for electronic handling of the information related to one's professional tasks. The term *terminal device fulfilling the requirements* refers to equipment, which fulfils specific requirements set in the subdivision of Information Assurance (I) for such devices.

F-04 – HANDLING AND STORAGE OF INFORMATION IN SECURITY AREAS AND OUTSIDE

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/ EU)
1. **National Classified Information has to be handled both in Security Areas and outside of their perimeter in a way that the access to Classified Information is protected from unauthorised people.** 2. **International Classified Information has to be handled both in Security Areas and outside of their perimeter in such a way that the access to Classified Information is protected from unauthorised people.**	1. 1101/2019 section 10; VM 2020:19, 26–30 2. –	1. – 2. Annex II (23–28)

Additional Information

The basic requirements for the handling and storage for both national and international Classified Information have been described in tables on the following pages.

F-04 – HANDLING AND STORAGE OF INFORMATION IN SECURITY AREAS AND OUTSIDE

HANDLING AND STORAGE OF NATIONAL CLASSIFIED INFORMATION

National security classification level	Handling			Storage		
	Outside of Security Area	Administrative Area	Secured Area	Outside of Security Area	Administrative Area	Secured Area
II	Paper documents: Yes, in case the unauthorised access is prevented In terminal device: Yes, in a terminal device fulfilling the requirements in case the unauthorised access is prevented	Paper documents: Yes, in case the unauthorised access is prevented In terminal device: Yes, in a terminal device fulfilling the requirements in case the unauthorised access is prevented	Paper documents: Yes, in case the unauthorised access is prevented In terminal device: Yes, in a terminal device fulfilling the requirements in case the unauthorised access is prevented	Paper documents: No In terminal device: No	Paper documents: No In terminal device: No	Paper documents: Yes, in an appropriate container solution In terminal device: Yes, in a terminal device fulfilling the requirements
MARKING:	Paper documents: Yes, in case the unauthorised access is prevented In terminal device: Yes, in a terminal device fulfilling the requirements in case the unauthorised access is prevented	Paper documents: Yes, in case the unauthorised access is prevented In terminal device: Yes, in a terminal device fulfilling the requirements in case the unauthorised access is prevented	Paper documents: Yes, in case the unauthorised access is prevented In terminal device: Yes, in a terminal device fulfilling the requirements in case the unauthorised access is prevented	Paper documents: No In terminal device: Yes, in a terminal device fulfilling the requirements and additional demands*	Paper documents: No In terminal device: Yes, in a terminal device fulfilling the requirements and additional demands*	Paper documents: Yes, in an appropriate container solution In terminal device: Yes, in a terminal device fulfilling the requirements
SALAINEN (IN FINNISH) HEMLIG (IN SWEDISH)	Paper documents: Yes, in case the unauthorised access is prevented In terminal device:Yes, in a terminal device fulfilling the requirements in case the unauthorised access is prevented	Paper documents: Yes, in case the unauthorised access is prevented In terminal device: Yes, in a terminal device fulfilling the requirements in case the unauthorised access is prevented	Paper documents: Yes, in case the unauthorised access is prevented In terminal device: Yes, in a terminal device fulfilling the requirements in case the unauthorised access is prevented	Paper documents: Yes, temporarily when additional demands are fulfilled** In terminal device: Yes, in a terminal device fulfilling the requirements and additional demands*	Paper documents: Yes, in an appropriate locked furniture In terminal device: Yes, in a terminal device fulfilling the requirements	Paper documents: Yes, in an appropriate locked furniture In terminal device: Yes, in a terminal device fulfilling the requirements

Additional demands:
***It is possible to store Classified Information belonging to national classification levels III or IV in a terminal device fulfilling the requirements in Administrative Area or outside the perimeter of Security Area in cases when the terminal device is stored:**

a) in a monitored space (ref. F-05.5) or
b) in an appropriate locked furniture, inside a specific, sealed secure envelope (or in an equivalent manner)

**** It is possible to store Classified Information belonging to national classification level IV, when the individual handling the information is committed to follow compensative controls described in the security guidance.**

F-04 – HANDLING AND STORAGE OF INFORMATION IN SECURITY AREAS AND OUTSIDE

HANDLING AND STORAGE OF INTERNATIONAL CLASSIFIED INFORMATION

Security classification level	Handling			Storage		
	Turvallisuusalueiden ulkopuolella	Hallinnollinen alue	Turva-alue	Turvallisuusalueiden ulkopuolella	Hallinnollinen alue	Turva-alue
II SECRET	Paper documents: Yes, temporarily when additional demands are fulfilled* In terminal device: Yes, in a terminal device fulfilling the requirements and additional demands*	Paper documents: Yes, in case the unauthorised access is prevented In terminal device: Yes, in a terminal device fulfilling the requirements in case the unauthorised access is prevented	Paper documents: Yes, in case the unauthorised access is prevented In terminal device: Yes, in a terminal device fulfilling the requirements in case the unauthorised access is prevented	Paper documents: No In terminal device: No	Paper documents: No In terminal device: No	Paper documents: Yes, in an appropriate container solution In terminal device: Yes, in a terminal device fulfilling the requirements
III CONFIDENTIAL	Paper documents: Yes, temporarily when additional demands are fulfilled* In terminal device: Yes, in a terminal device fulfilling the requirements and additional demands*	Paper documents: Yes, in case the unauthorised access is prevented In terminal device: Yes, in a terminal device fulfilling the requirements in case the unauthorised access is prevented	Paper documents: Yes, in case the unauthorised access is prevented In terminal device: Yes, in a terminal device fulfilling the requirements in case the unauthorised access is prevented	Paper documents: No In terminal device: No	Paper documents: No In terminal device: No	Paper documents: Yes, in an appropriate container solution In terminal device: Yes, in a terminal device fulfilling the requirements
IV RESTRICTED	Paper documents: Yes, temporarily when additional demands are fulfilled* In terminal device: Yes, in a terminal device fulfilling the requirements and additional demands**	Paper documents: Yes, in case the unauthorised access is prevented In terminal device: Yes, in a terminal device fulfilling the requirements in case the unauthorised access is prevented	Paper documents: Yes, in case the unauthorised access is prevented In terminal device: Yes, in a terminal device fulfilling the requirements in case the unauthorised access is prevented	Paper documents: Yes, temporarily when additional demands are fulfilled*** In terminal device: Yes, in a terminal device fulfilling the requirements and additional demands***	Paper documents: Yes, in an appropriate locked furniture In terminal device: Yes, in a terminal device fulfilling the requirements	Paper documents: Yes, in an appropriate locked furniture In terminal device: Yes, in a terminal device fulfilling the requirements

Additional demands:

* **It is possible to handle international Classified Information belonging to classification levels SECRET and CONFIDENTIAL outside Secured Areas in case**

- the information is transported according to Katakri requirement F-08.1
- the individual possessing the information is committed to follow compensative controls given by the Finnish Security and Intelligence Service or the Defence Command or, when terminal devices are concerned, by NCSA of Traficom to ensure that unauthorised access to the information has been prevented
- the individual possessing the information keeps the information under the personal surveillance at all times; and
- in the case of documents in paper format, the individual has notified the relevant registry of the fact.

F-04 – HANDLING AND STORAGE OF INFORMATION IN SECURITY AREAS AND OUTSIDE

HANDLING AND STORAGE OF INTERNATIONAL CLASSIFIED INFORMATION

**** It is possible to handle international Classified Information belonging to classification level RESTRICTED outside Security Areas in case:**

- the information is transported according to Katakri requirement F-08.1
- the individual possessing the information is committed to follow compensative controls given by the Finnish Security and Intelligence Service or the Defence Command or, when terminal devices are concerned, by NCSA of Traficom to ensure that unauthorised access to the information has been prevented

*** It is possible to store international Classified Information belonging to classification level RESTRICTED outside Security Areas in case:

- the individual possessing the information is committed to follow compensative controls given by the Finnish Security and Intelligence Service or the Defence Command or, when terminal devices are concerned, by NCSA of Traficom to ensure that unauthorised access to the information has been prevented

When NATO requirements for security zones and the handling of NATO Classified Information is concerned, the requirements have to verified from the Finnish Security and Intelligence Service or the Defence Command case by case.

Discussing about Classified Information inside Security Areas and outside: it is possible to discuss about CI in Security Areas and outside their perimeter when unauthorised access to discussions has been prevented. The term preventing means here the protection of information from individuals without need-to-know to the information discussed, as well as from illegal intelligence actions.

Evaluation of TEMPEST risks: When evaluating the handling of information in the terminal device together with location of Security Areas it is relevant to take into account the TEMPEST risk dealt with in requirement I-14. In many cases, the change of the location within the facility may decrease the risk.

Requirements for Security Areas

F-05 – Administrative Area

The term *administrative* area refers to areas and spaces planned for normal working conditions. These areas may consist of offices or form an entity comprising spaces of different nature. The owner of Classified Information ensures that individual access to these premises is allowed only for authorised people.

This chapter introduces the minimum requirements for Administrative Areas. In addition to them, there is a need to form responsibilities, plan, implement and maintain other risk management procedures based on risk assessment (F-02) and defence-in-depth principle (F-03). By combining these actions, the organisation will be able to accept residual risks and to fulfil the requirements set for security measures (F-01).

F-05.1 – BOUNDARY AND STRUCTURES FOR THE AREA (WALLS, DOORS, WINDOWS, FLOOR AND CEILING STRUCTURES)

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/ EU)
The area must have a clearly defined and visible boundary. **There are no specific requirements for the structure setting the boundary.**	1101/2019 section 9 (1)1; VM 2020:19, 15	Annex II (14)

Additional Information

In general: Before the approval of the area the physical security requirements have to be fulfilled. The structure may be normal office structure. In case Classified Information is stored in the area and the risk for intrusion is considered probable, the boundary structures have to be strengthened. When strengthening the structures it is advisable to estimate the protection offered by the environment around the area and the reaction time of the security personnel. Holes and other openings, which are not used for trespassing, have to be lockable or closable in order to administer the access to the area appropriately. In case mechanical locks are used at the outer boundary of the Administrative Area, copying of keys needs to be prevented with patent protection. When possible, the emergency exits may not be planned through the area. As a recommendation, solutions used for defence-in-depth should follow European standards and their minimum requirements. The table below lists standards which can be used as references when evaluating the bounder structures of the area:

Structures	Reference standard	Standard classes	Desired level
Walls, doors, floor and ceiling structures	SFS-EN 1627	RC1–RC6	–
Windows (protective glass)	SFS-EN 356	P4A–P5A and P6B–P8B	–

F-05.2 – MANAGEMENT OF ACCESS RIGHTS

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/ EU)
Only authorised personnel have an individual access to the area. It is necessary for the organisation to define the roles and procedures concerning access rights and (physical) key management.	1101/2019 section 9; VM 2020:19, 15	Annex II (14 and 30)

Additional Information

Access to the area may be limited mechanically, electronically or based on the individual recognition of personnel. A dedicated person has to be nominated responsible for managing access rights and key management processes.

At least the following procedures and roles have to be defined:

- Procedures and roles for access rights and key management have been defined, documented and instructed.
- List of access rights and key holders exists.
- Access rights are checked regularly and kept up-to-date.
- People responsible for changes and reorders of keys and electronic credentials (like key tags) have been nominated.
- Key cards (for reorders) and undelivered keys and key tags are stored in an appropriate manner.
- Rationale for handing over keys is documented.
- Keys can only be handed over for a person having individual access right to the area concerned.
- Rights to possess keys are notified when relevant changes in personnel occur.

Access to the area has to be monitored in case the risk assessment indicates the need for it. Access control procedure may be relevant in cases where handling of Classified Information belonging to classification level III (CONFIDENTIAL) or higher is concerned.
Recommendation to implement access rights:

- ID cards (badges) with photo or equivalent visible identifiers are used in the organisation.
- Only access rights needed for the job are issued.
- The rationale for access rights is documented and only the designated persons have an access to the area.
- Changes in the personnel are notified in access rights, when relevant.
- Management of the access control system may be outsourced in cases when the management of it has been well organised.

F-05.2 – MANAGEMENT OF ACCESS RIGHTS

Spare keys for Administrative Areas need to be stored securely, inside a secure and sealed envelope, indicating the date of sealing with signature of the sealer. Alternatively, keys may be stored in a key safe, which is connected to the access control system. Keys are handed over after signature and based on the working task. The procedure has been described in security instructions.

It is recommended that devices and systems belonging to the complexity of defence-in-depth are based on European standards and on their minimum requirements. The table below lists standards which can be used as references when evaluating an appropriate solution:

Locking and access control	Reference standard	Standard classes	Desired level
Locks and accessory	SFS 7020 (+SFS 5970)	1 – 4	1
Electronic access control systemst	SFS-EN 60839-11-1 SFS-EN 60839-11-2	1 – 4	E.g. requirements of the SFS-EN 50131 standard should be notified in case the access control system functions as a part of intrusion detection system

F-05.3 – VISITORS

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/ EU)
People who do not belong to the authorised personnel (i.e. visitors) have to be escorted at all times or be subject to equivalent controls.	1101/2019 section 9; VM 2020:19, 15	Annex II (14)

Additional Information

Example of the implementation: the host of visitors has to have an individual access right to the Security Area where the host is escorting visitors, as well as the right to host visitors. The visitor procedure must ensure that the confidentiality of the information handled or stored within the area will not be put in danger.

The procedure for visitors needs to be accepted by the organisation. The visitor-instruction may include the following:

- Visitors are recognised and marked with visitor badges
- Visits are registered
- Visitors are not allowed to enter and are not left alone in Security Areas. The host is responsible for visitors throughout the visit.
- Personnel have been instructed for hosting visitors.
- Visitors are not lead into situations where they might see, hear or otherwise get access in an unauthorised manner to Classified Information.
- Personnel have been instructed to react on people without ID cards.

Maintenance and service work inside the area may be done only by persons who have an individual access right to the area or under surveillance of such a person.

Handling of Classified Information is prohibited during the service, installation and cleaning activities, if there is a danger for the disclosure of Classified Information to unauthorized people.

Unescorted visits may be possible for those visitors who fulfil the requirements set in F-05.2.

F-05.4 – SOUNDPROOFING

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/ EU)
Soundproofing of the area has to be good enough to prevent unauthorised people to hear on an understandable level the discussions dealing with Classified Information. Soundproofing has to be taken into account also inside the area in cases Classified Information is discussed and people without the need-to-know may be around.	VM 2020:19, 15	–

Additional Information

In general: *Prevention* means in this context protection of information from people without the need-to-know, as well as of illegal intelligence actions.

Soundproofing requirement is targeted only on those premises within the area where Classified Information is discussed.

Soundproofing level may be estimated, e.g., by listening the discussion from outside nearby doors, walls, air ventilation channels and nearby other openings or holes. The level of soundproofing may also be compared to the air sound insulation requirement set for different structures. The requirement may be set according to the standard SFS-EN-ISO 717-1. The air sound insulation capability may be estimated based on measurements according to the standard SFS-EN-ISO 16283-1. During the estimation, also the structural sound insulation capability has to be noted.

Soundproofing requirement may be achieved by, e.g., relocation of the office space, improvement of sound insulation in structures and around holes or by increasing noise outside the target area.

F-05.5 – INTRUSION DETECTION SYSTEMS

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/ EU)
No specific requirements. Intrusion detections systems may be used as a risk management method, complementing the defence-in-depth, or as means to achieve the requirement F-05.8 2a.	VM 2020:19, 16	–

Additional Information

In general: the area and the doors leading to it may be equipped with an intrusion detection system (burglar alarm) in cases when Classified Information is stored in the area in locked furniture and the risk for intrusion has been estimated as probable. When estimating the use of intrusion detection system (or equivalent) for the area, it is advisable to notify the reaction time estimate, which has been dealt with together with the requirement concerning the structures of the area. In cases when the area has been equipped with an intrusion detection system, it is recommendable to use the system for security monitoring on those times when no one is working in the area. Intrusion detection system should be located inside the Security Area it is planned to protect.

It is recommended that devices and systems belonging to the complexity of defence-in-depth are based on European standards and on their minimum requirements. The table below lists standards which can be used as references when evaluating an appropriate solution:

Systems and alarm centres	Reference standard	Standard classes	Desired level
Intrusion detection systems	SFS-EN 50131	1 – 4	2
Alarm relays of intrusion detection systems	SFS-EN 50136-1	DP1 - DP4 and SP5 - SP6	–
Alarm control centres of security companies	SFS-EN 50518	–	–

F-05.6 – PROTECTION FROM UNAUTHORISED OBSERVATION

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/ EU)
In case a risk to disclose Classified Information through unauthorised observation or unintended overlooking exists, appropriate measures shall be taken to counter this risk.	VM 2020:19, 16	Annex II (6)

Additional Information

In general: The risk for unauthorised observation may be reduced by relocation of working places and by using different kind of shields (standing screens, curtains, window blinders, computer screen privacy filters).

F-05.7 – INSPECTIONS OF WORKING SPACES AND DEVICES (ONLY FOR NATIONAL CLASSIFICATION LEVEL II OR EU SECRET)

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/ EU)
1. Organisation has to inspect all electronic equipment, which are used in such an Administrative Area, where classification level II (SECRET) information is handled. This requirement is relevant in cases when the threat against disclosure of the information has been evaluated high. **2. In addition, the area needs to be regularly inspected, physically and technically. Such inspections shall also be conducted following any unauthorised entry or suspicion of such entry.**	1. VM 2020:19, 16 2. VM 2020:19, 16	1. Annex II (18) 2. Annex II (17c)

Additional Information

In general: In case it is not possible to inspect electronic devices (e.g. cell phones, smart watches) properly, they have to be left on dedicated lockers outside the perimeter.

See F-07 – Technically Secured Area.

F-05.8 – HANDLING AND STORAGE OF INFORMATION		
Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/ EU)
1. Classification level IV (RESTRICTED) information may be stored in the area. Information has to be stored in locked furniture. Terminal device containing above mentioned information has to be stored in appropriate locked furniture, when possible. **2. In Administrative Area it is possible to store information belonging to national classification level III in terminal devices which have been approved for the level and when the terminal device is stored in: a) monitored space or b) in sealed security envelope inside locked furniture (or in equivalent secure way). Potential monitoring of the storage space has to be done according to the requirement F-05.5. As an exception to this rule for storing national classification level III information, it is not allowed to store international CONFIDENTIAL information in Administrative Areas.** **3. Keys or combination settings to the appropriate locked furniture have to be kept under control of such personnel, which has the need-to-know to the information stored in the above-mentioned manner. Combination settings have to be committed to memory by the authorized individuals.** **Combination settings to storage units containing Classified Information have to be changed:** • on receipt of a new container; • whenever there is a change in personnel knowing the combination; • whenever a compromise has occurred or is suspected; • when a lock has undergone maintenance or repair. **4. It is allowed to handle information classified on national levels IV-II in the Administrative Area when access to the information by unauthorised persons has been prevented. When the Classified Information is used by means of terminal devices it is necessary to take care that both the terminal device, as well as the data communication arrangement fulfil the requirements set for them.**	1. 1101/2019 section 10 (3)4; VM 2020:19, 16 2. 1101/2019 section 10(4); VM 2020:19, 28-29 3. – 4. 1101/2019 section 10 (4); VM 2020:19, 26-28	1. Annex II (24) 2. Annex II (26) 3. Annex II (31) 4. Annex II (25)

F-05.8 – HANDLING AND STORAGE OF INFORMATION

Additional Information

In general: When handling information it is essential to ensure the protection of Classified Information while pauses. Information in paper format as well as terminal devices needs to be taken either into the Security Area or into an appropriate storage unit, depending on the classification. It is important to ensure, or at least be able to appropriately monitor the integrity of the terminal device in situations when a terminal device, which is used to handle information belonging to the national classification level III, has to be temporarily stored in an Administrative Area.

When locked furniture is used to store Classified Information it is necessary to ensure that intrusion to such furniture can be detected by marks of the burglary.

It is possible to discuss about Classified Information when it can be ensured that unauthorised people cannot hear the discussions. Ensuring, in this context, means the protection of the information from people who do not have the need-to-know to the information discussed, as well as from illegal intelligence actions.

Evaluation of TEMPEST risks:

- When evaluating the handling of information in the terminal device versus the location of Security Areas, TEMPEST risks handled in requirement I-14 need to be taken into consideration. In many cases these risks may be reduced by changing the information handling location within premises.

F-06 – Secured Area

The term *secured* area refers to areas and spaces planned for handling and storing Classified Information in a secure way, thus providing additional protection compared to Administrative Areas. A Secured Area may temporarily be established within an Administrative Area for hosting a classified meeting or for other relevant purposes.

This chapter introduces the minimum requirements for Secured Areas. In addition to them, there is a need to form responsibilities, plan, implement and maintain other risk management procedures based on risk assessment (F-02) and defence-in-depth principle (F-03). By combining these actions, the organisation will be able to accept residual risks and fulfil the requirements set for security measures (F-01).

F-06.1 – BOUNDARY AND STRUCTURES FOR THE AREA (WALLS, DOORS, WINDOWS, FLOOR AND CEILING STRUCTURES)

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/ EU)
1. The area must have a clearly defined and visible boundary. **2. In case the area does not have an appropriate solution for information storage, the walls, the floor, the ceiling, windows and doors of the area must provide the required level of security for the storage.**	1. 1101/2019 section 9 (1)2; VM 2020:19, 21 2. VM 2020:19, 21	1. Annex II (15) 2. Annex II (22)

Additional Information

In general: Holes and other openings, which are not used for trespassing, have to be lockable or closable with bars or with a strong steel grill in order to administer the access to the area appropriately. The openings have to be controlled by means of an intrusion detection system, unless the space is manned around the clock or unless the space is checked at the end of working hours and randomly outside working hours.

The structure of the area needs to be strengthened in case Classified Information is stored in the area and in case the risk for intrusion or burglary is considered probable. In that case the boundary and protective structures should be made of concrete, steel, tile or strong wood. Inadequate structures, like normal office structures, have to be strengthened. It shall not be possible to detach the wall elements from outside. Fortifications need to be evaluated in relation to the protection level provided by the premises around the area and to the reaction time of the security personnel. In door structures special attention has to be payed to the structure of the frame, the gap between the door and the frame and the attachment of the frame to the wall structure.

Unless the area has secure storage possibilities for the information, the walls, the floor, the ceiling, windows and doors of the area must fulfil the protection level of the class RC3 in the standard SFS-EN-1627.

F-06.1 – BOUNDARY AND STRUCTURES FOR THE AREA (WALLS, DOORS, WINDOWS, FLOOR AND CEILING STRUCTURES)

Emergency exits may not lead through Secured Areas. If, however, there is a necessity for the emergency exit to use the Secured Area, the emergency exit has to be equipped with an intrusion detection system. If the emergency exit uses the area in a way that directly discloses the Classified Information for the users of the exit or the area is not equipped with a storage solution, which could be considered secure enough, the area cannot be accredited as a Secured Area.

It is recommended that solutions belonging to the complexity of defence-in-depth are based on European standards and on their minimum requirements. The table below lists standards, which can be used as references when evaluating appropriate solutions for boundary structures:

Structures	Reference standard	Standard classes	Desired level
Walls, doors, floor and ceiling structures	SFS-EN 1627	RC1 – RC6	RC 3, based on burglary risk assessment
Windows (protective glass)	SFS-EN 356	P4A–P5A and P6B–P8B	P5A, as a part of other structure and based on burglary risk assessment. The protective glassing should be a normal part of the window structure. Retrofit solutions should be avoided.

F-06.2 – ACCESS CONTROL

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/ EU)
A visibly defined and protected perimeter has to be established, through which all entry and exit are controlled by means of a pass or personal recognition system.	1101/2019 section 9 (1)2; VM 2020:19, 21	Annex II (15)

Additional Information

In general: Access to the area may be controlled electronically or based on the individual recognition of personnel. At the border of the area two-way access control may be used. It is recommended to use double identification on entrances and exits.

Example of the implementation: Recommendation for access control measures:

- ID cards (badges) with photo or equivalent visible identifiers are used in the organisation.
- Organisation has nominated a person responsible for approving access rights to Secured Area.
- Procedure of the management system of access rights has been instructed and documented:
    - Approved access rights have been documented and a nominated person is keeping the document up-to-date
    - Only access rights needed for the job are issued.
    - The rationale for access rights is documented and only the designated persons have an access to the area.
    - Changes in the personnel are notified in access rights, when relevant.
    - A separate access right documentation is maintained for permanent personnel and for other personnel having access rights.
    - Access rights are evaluated regularly, like every 6 months, by the nominated and responsible person
    - Management of the access control system may be outsourced in cases when the management of it has been well organised.
    - Electronic opening of doors to the Secured Area from the work station of a regular employee has to be prevented.
- Access right to Secured Area can be issued only for those who have a need to use the area. Entry to the area must be verifiable afterwards.
- Credentials have to use a modern, encrypted reading technology or else double identification must be required.

Remote connections of the access control system and installation of credential readers shall be done in a secure way and based on the risk assessment in order to give access from authorised terminal devices or networks only and to ensure that the data connection and interfaces to access control system are secure enough to prevent unauthorised access to the information transferred. Access control system should be placed inside the Secured Area it is protecting.

F-06.2 – ACCESS CONTROL

It is recommended that devices and systems belonging to the complexity of defence-in-depth are based on European standards and on their minimum requirements. The table below lists standards which can be used as references when evaluating an appropriate solution:

Access control	Reference standard	Standard classes	Desired level
Electronic access control systems	SFS-EN 60839-11-1	1 – 4	E.g. requirements of the SFS-EN 50131 standard should be notified in case the access control system functions as a part of intrusion detection system
CCTV systems	SFS-EN 62676		Planning according to the K standard of the Finance Finland. Disposal schedule for CCTV recordings is based on risk management and the capability for the organisation to detect deviations, bearing in mind preventive and reacting procedures. Minimum time for maintaining recordings is one month. In addition the CCTV may be connected to the intrusion detection system.

F-06.3 – MANAGEMENT OF ACCESS RIGHTS

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/ EU)
1. Individual access right for the area may only be given to a person duly authorised by the organisation after ensuring about the trustworthiness of the individual and after providing with a specific permission to enter the area (need to access the area).	1. 1101/2019 section 9 (1)2; VM 2020:19, 21	1. –
2. Organisation has to define the procedures and roles concerning management of access rights, combination settings and keys.	2. VM 2020:19, 21	2. Annex II (30)
3. In cases when international Classified Information is handled and stored in the Secured Area, the individual access right to the area can be issued by the organisation only for a person duly authorised, who carries a valid personal security clearance (PSC) and has been provided with a specific permission to enter the area based on the need-to-know.	3. –	3. Annex II (15)

Additional Information

In general: The trustworthiness should be verified primarily by personnel security clearance procedure (see T-10).

The rationale to access the area should be the need-to-know. Specific permission may also be based on the need to access the area. A person shall be nominated to manage access rights, credentials (key tags etc.) and keys.

Example of implementation: At least the following procedures and roles have been approved by the organisation:

- Procedures and roles for access rights and key management have been defined, documented and instructed.
- List of access rights and key holders exists.
- Access rights are checked regularly and kept up-to-date.
- People responsible for changes and reorders of keys and electronic credentials (like key tags) have been nominated.
- Key cards (for reorders) and undelivered keys and key tags are stored in an appropriate manner.
- Rationale for handing over keys is documented.
- Keys can only be handed over for a person having individual access right to the area concerned.
- Rights to possess keys are notified when relevant changes in personnel occur.

F-06.3 – MANAGEMENT OF ACCESS RIGHTS

Spare keys for Secured Areas need to be stored in an appropriate container unit and in sealed envelope, indicating the date of sealing with signature of the sealer. Alternatively, keys may be stored in a key safe, which is connected to the access control system. Keys are handed over after signature and based on the working task. The procedure has been described in security instructions. Access to the Secured Area with a master key of a lower Secured Area must be prevented.

Keys to the Secured Area reserved for security and maintenance personnel have to be kept sealed and used only in exceptional situations. In emergency situations two persons may be required to enter the area simultaneously in case the access to the Secured Area directly means access to Classified Information or the area lacks appropriate storage solutions.

It is recommended that devices and systems belonging to the complexity of defence-in-depth are based on European standards and on their minimum requirements. The table below indicates a standard, which can be used as a reference when evaluating an appropriate solution:

Locking and access control	Reference standard	Standard classes	Desired level
Locks with accessories	SFS 7020 (+SFS 5970)	1 – 4	3

F-06.4 – VISITORS

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/ EU)
1. **People without an individual access right to the area (i.e. visitors) need to be escorted.** 2. **Where entry into a Secured Area constitutes direct access to the classified information contained in it, the following additional requirements will apply:** • the highest classification level for the information normally stored in the area has to be clearly indicated • all visitors must have a specific permission to enter the area, they have to be escorted at all times and their trustworthiness has to have appropriately verified in advance, unless it has been ensured that visitors cannot have access to Classified Information.	1. 1101/2019 section 9 (1)2; VM 2020:19, 22 2. VM 2020:19, 22	1. Annex II (15) 2. Annex II (16)

Additional Information

Example of implementation: the host of visitors has to have an individual access right to the Secured Area where the host is escorting visitors, as well as the right to host visitors. Taking the visitor to Secured Area has to be based on prior information to and approval by the person responsible for the security of the area. The visitor procedure must ensure that the confidentiality of the information handled or stored inside the area will not be put in danger.

The procedure for visitors needs to be accepted by the organisation. The visitor-instruction may include the following:

- Visitors are recognised and marked with visitor badges
- Visits are registered
- Visitors are not allowed to enter and are not left alone in Secured Areas. The host is responsible for visitors throughout the visit.
- Personnel have been instructed for hosting visitors.
- Visitors are not lead into situations where they might see, hear or otherwise get access in an unauthorised manner to Classified Information.
- Personnel have been instructed to react on people without ID cards.

Maintenance and service work inside the area may be done only by persons who have an individual access right to the area or under surveillance of such a person.

Handling of Classified Information is prohibited during the service, installation and cleaning activities, if there is a danger for the disclosure of Classified Information to unauthorized people.

Unescorted visit approvals may be possible for those visitors who fulfil requirements set in F-06.3.

F-06.5 – SECURITY INSTRUCTIONS

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/EU)
1. **Security instructions have to be drafted to each Secured Area. Instructions include procedures concerning:** a) Handling and storage of information in the area (F-06.10): classification of the information which may be handled and stored in the area. b) Protection and surveillance measures to be implemented (including F-06.7 – F-06.9). c) Approval of access rights to the area (F-06.3): persons who have access to the area without escorting, based on specific permission and verification of trustworthiness d) Visitors (F-06.4): procedure to use escorting when needed or to protect Classified Information in cases when exceptional people are approved access to the area e) Other relevant procedures.	1. VM 2020:19, 22	1. Annex II (21)

Additional Information

In general: Security instructions cover all processes dealing with Classified Information, including Secured Areas for the entire life cycle of the information (see F-08). Compliance with security instructions is monitored and need for changes is evaluated regularly. The use of security instructions and of being up-to-date is verified regularly, at least on annual basis.

F-06.6 – SOUNDPROOFING

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/ EU)
Soundproofing of the area has to be good enough to prevent unauthorised people to hear on an understandable way the discussions dealing with Classified Information. Soundproofing has to be taken into account also within the area in cases Classified Information is discussed and people without the need-to-know may be around.	VM 2020:19, 22	–

Additional Information

In general: *Prevention* means in this context protection of information from people without the need-to-know, as well as of illegal intelligence actions.

Soundproofing requirement is targeted only on those premises inside the area, where Classified Information is discussed.

Soundproofing level may be estimated, e.g., by listening the discussion from outside nearby doors, walls, air ventilation channels and nearby other openings or holes. The level of soundproofing may also be compared to the air sound insulation requirement set for different structures. The requirement may be set according to the standard SFS-EN-ISO 717-1. The air sound insulation capability may be estimated based on measurements according to the standard SFS-EN-ISO 16283-1. During the estimation, also the structural sound insulation capability has to be noted.

Soundproofing requirement may be achieved by, e.g., relocation of the office space, improvement of sound insulation in structures and around holes or by increasing noise outside the target area.

F-06.7 – INTRUSION DETECTIONS SYSTEMS

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/ EU)
Area without 24/7 staffing has to be inspected after working hours, when relevant, and in irregular intervals outside working hours, unless an intrusion detection system covers the area.	VM 2020:19, 23	Annex II (19)

Additional Information

In general: the boundary of the area and structures in it (walls, doors, windows, floor and ceiling structures) and/or routes leading to the area may be equipped with an intrusion detection system (burglar alarm) in cases when Classified Information is stored in the area in locked furniture and the risk for intrusion has been estimated as probable. When estimating the use of intrusion detection system (or equivalent) for the area, it is advisable to notify the reaction time estimate, which has been dealt with in conjunction with the requirement concerning the structures of the area. In cases when the area has been equipped with an intrusion detection system, it is recommendable to use the system for security monitoring on those times when no-one is working in the area.

Alarm relaying should use a controlled or duplicated connection. The device which relays the alarm should transfer at least the following information to the security company's alarm control centre (or equivalent monitoring post): burglary, on/off, sabotage, failure. The system needs to be operated by a person with an individual code. Remote connections and installations of control devices have to be implemented in a secure way and based on risk assessment, in order to ensure that only authorized terminal devices and networks can access the system. Interfaces of the data connection and the intrusion detection system have to be protected to prevent unauthorized access to the data transferred. Intrusion detection system should be located inside the Secured Area it is planned to protect.

Intrusion detection system has to be managed by the organisation itself. The management may be outsourced, based on risk assessment and separation of duties. Procedures dealing with the management of the system, alarms and reaction to them need to be evaluated. Testing of alarm relaying (once a month) and reactions (annually) have to be regular and documented.

Reacting personnel (guards) have to be well trained to understand the specific details of the area. Their training and tools need to match the risks. In alarm situations, two persons may be requested to enter the area simultaneously in cases when entering the area directly leads into the situation where Classified Information may be accessed or when there is no secure storage solution in place for the information.

It is recommended that devices and systems belonging to the complexity of defence-in-depth are based on European standards and on their minimum requirements. The table below lists standards which can be used as references when evaluating an appropriate solution:

F-06.7 – INTRUSION DETECTION SYSTEMS

Devices and systems	Reference standard	Standard classes	Desired level
Intrusion detection systems	SFS-EN 50131	1 – 4	3
Alarm relays of intrusion detection systems	SFS-EN 50136-1	DP1 DP4 and SP5 SP6	DP3-DP4 (dual path) or SP5-SP6 (single path)
Alarm control centres of security companies	SFS-EN 50518		The company has to fulfil requirements set by the standard and it has to maintain a quality management system certified according to SFS-EN ISO 9001 or the company has to have an approval to match the requirements of this standard in relevant areas.

F-06.8 – PROTECTION FROM UNAUTHORISED OBSERVATION

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/EU)
In case a risk to disclose Classified Information through unauthorised observation or unintended overlooking exists, appropriate countermeasures have to be taken into use.	VM 2020:19, 23	Annex II (6)

Additional Information

In general: The risk for unauthorised observation may be reduced by relocation of working places and by using different kind of shields (standing screens, curtains, window blinders, computer screen privacy filters).

F-06.9 – INSPECTIONS OF WORKING SPACES AND DEVICES (ONLY FOR NATIONAL CLASSIFICATION LEVEL II OR EU SECRET)

Requirement	§ Source (906/2019 and/or1101/2019)	§ Source (2013/488/EU)
1. Organisation has to inspect all electronic equipment, which are used in such an Administrative Area, where classification level II (SECRET) information is handled. This requirement is relevant in cases when the threat against disclosure of the information has been evaluated high. **2. In addition, the area needs to be regularly inspected, physically and technically. In addition, inspections have to be conducted following any unauthorised entry or suspicion of such entry.**	1. VM 2020:19, 23 2. VM 2020:19, 23	1. Annex II (18) 2. Annex II (17c)

Additional Information

In general: In case it is not possible to inspect electronic devices (e.g. cell phones, smart watches) properly, they have to be left on dedicated lockers outside the perimeter.

See F-07 – Technically Secured Area.

F-06.10 – HANDLING AND STORAGE OF INFORMATION

Requirement

1. **Classified Information of all classification levels may be stored in the area, based on risk assessment and physical security measures.**
2. **Information belonging to the classification level III (CONFIDENTIAL) or higher has to be stored using an appropriate storage solution. In addition, terminal devices have to be stored equally, when possible. In case appropriate storage solution is not available in the area, the walls, the floor, the ceiling and the doors have to offer the security level sufficient for the storage of information.**
3. **Keys or access codes have to be kept under control of such personnel, who has the need-to-know to the information stored in the storage solution. Access codes have to be committed to memory by the authorized individuals.**

Combination settings to storage units containing Classified Information have to be changed:

- on receipt of a new container;
- whenever there is a change in personnel knowing the combination;
- whenever a compromise has occurred or is suspected;
- when a lock has undergone maintenance or repair;

4. **It is allowed to handle information classified on all levels in the Secured Area when access to the information by unauthorised persons has been prevented.**

§ Source (906/2019 and/or1101/2019)

1. 1101/2019 section 10
2. VM 2020:19, 24
3. VM 2020:19, 21 and 24
4. VM 2020:19, 24
5. 1101/2019 section 10

§ Source (2013/488/EU)

1. Annex II (24, 26, 28)
2. Annex II (26)
3. Annex II (31)
4. Annex II (28)
5. Annex II (23, 25, 27)

Additional Information

In general: When handling information it is essential to ensure the protection of Classified Information while pauses. Information in paper format as well as terminal devices needs to be stored in an appropriate storage unit for the pause.

Unless the area has secure storage possibilities for the information, the walls, the floor, the ceiling, windows and doors of the area must fulfil the protection level of the class RC3 in the standard SFS-EN-1627.
When locked furniture is used to store Classified Information it is necessary to ensure that intrusion to such furniture can be detected by marks of the burglary.

It is possible to discuss about Classified Information, when it can be ensured that unauthorised people cannot hear the discussions. Ensuring, in this context, means the protection of the information from people who do not have the need-to-know to the information discussed, as well as from illegal intelligence actions.

F-06.10 – HANDLING AND STORAGE OF INFORMATION

Evaluation of TEMPEST risks:

- When evaluating the handling of information in the terminal device versus the location of Secured Areas, TEMPEST risks handled in requirement I-14 need to be taken into consideration. In many cases these risks may be reduced by changing the information handling location within premises.

It is recommended that devices and systems belonging to the complexity of defence-in-depth are based on European standards and on their minimum requirements. The table below lists standards, which can be used as references when evaluating an appropriate storage solution:

Devices and systems	Reference standard	Standard classes	Desired level
Safes	SFS-EN 1143-1	I – V	II, need for fire protection should be evaluated when necessary. Based on risk assessment, the safe is monitored through sensors and anchored on the floor. As a rule safes should not be placed against the outer wall.
Vaults made of elements	SFS-EN 1143-1	I – XII	II. The space around the vault has to be equipped with intrusion detection or the outer structures of the vault have to be monitored through sensors.

F-07 – Technically Secured Area

The Finnish national legislation (1101/2019, section 9) does not define any technically protected secured area, but such an area has been included in the security regulation of the Council of EU, as well as the one of NATO. The area may be established to protect Classified Information of EU or NATO.

Areas, where international Classified Information is handled or stored and which have especially been identified as areas which need protection from unauthorised listening (audio eavesdropping), have to be defined as Technically Secured Areas. The organisation has to define a Technically Secured Area, when it organises meetings where information classified to EU SECRET / NATO SECRET is handled or if such information is regularly discussed on its premises.

F-07 – TECHNICALLY SECURED AREA

Requirement	§ Source (906/2019 and/or1101/2019)	§ Source (2013/488/EU)
1. **In addition to the minimum requirements set for Secured Areas (F-06), following requirements apply:** a) such areas have to be equipped with intrusion detection system, be locked when not occupied and be guarded when occupied. Any keys have to be controlled b) all persons and material entering such areas have to be controlled c) such areas have to be regularly physically and/or technically inspected as required by the Finnish Security and Intelligence Service or the Defence Command. In additions, such inspections have to be conducted following any unauthorised entry or suspicion of such entry. d) area may only be equipped with data connections, phones and other communication or electronic devices approved to be used in the area.	1. –	1. Annex II (17)
2. **All such communication devices, electric appliances or electronics have to be inspected before they can be used within areas where meetings handling EU SECRET / NATO SECRET information are organised or such information is worked with in cases when the threat against the Classified Information of EU or NATO is considered to be high. This procedure ensures that those devices cannot intentionally or unintentionally transfer information outside the perimeter of the Secured Area in an understandable form.**	2. –	2. Annex II (18)
3. **Threat analysis, risk management procedures and approval of security measures for the potential Technically Secured Area are done on case by case basis by the Finnish Security and Intelligence Service or by Defence Command.**	3. –	3. Annex II (3, 13)

Additional Information

In general: It is possible to establish a technically secured area temporarily inside an Administrative Area for the purpose of classified meetings (or equivalent). Inside the area there has to be a list of data connections, phones, other communication devices and electronics which have been approved for use.

Requirements for data security

F-08 – Data security

In the chapter dealing with data security, procedures for handling Classified Information in paper format are described, covering all phases of the information life cycle. In case the registration, printing, copying or destroying of Classified Information includes the use of information systems (e.g. multifunction device), the security of the information system has to be evaluated based on requirements presented in the subdivision I.

F-08.1 – TRANSFER OF INFORMATION BY USING POSTAL OR COURIER SERVICES

Requirement	§ Source (906/2019 and/or1101/2019)	§ Source (2013/488/EU)
1. Classified Information has to be transported or delivered according to the instructions given by the organisation, taking into account necessary protective measures. **2. Classified Information has to be packed in a manner, which prevents their unauthorised disclosure.** **3. Classified Information may be transported outside Security Areas in electronic format by using encryption accredited my authorities (see I-12).** **4. Information belonging to classification level IV (RESTRICTED) may be transferred in unencrypted form by using postal services.** **5. Classified Information belonging to level II (SECRET) or III (CONFIDENTIAL) needs to be packed in a secure way and transported in unencrypted form to the recipient under constant control. Also other methods may be used for transportation in case the confidentiality and integrity of the information can be sufficiently ensured, bearing in mind the classification level.** **6. Requirements for the transport of international Classified Information have to be asked case by case from the Finnish Security and Intelligence Service or from Defence Command.**	1. 906/2019 section 4 2. 1101/2019 section 13 3. 1101/2019 section 13 4. 1101/2019 section 13 5. 1101/2019 section 13 6. –	1. Art. 9 (4) 2. Annex III (32 and 37) 3. Art. 9 (4) 4. Annex III (34 and 40 5). 5. – 6. Annex III (chapter V)

F-08.1 – TRANSFER OF INFORMATION BY USING POSTAL OR COURIER SERVICES

Additional Information

In general: Certain international or national Classified Information may never be transported by using postal services. Accepted procedures have to be asked, case by case, from relevant authorities. National Security Authority will provide more information, when needed.

Classified material may be transferred in an electronic format (e.g. CD-ROM) within Finland or outside Finland in a chosen manner in case the information has been encrypted inside protected environment, using a crypto product which has been approved for the respective classification level (see I-12) by the competent authority.

Examples of the implementation:
On classification level IV (RESTRICTED) this requirement may be fulfilled by using following procedures:

1. Classified Information will be packed in an envelope or in other closable package. Packages are not marked with classification marking and they may not reveal from outside that they contain Classified Information (non-transparent envelopes or packages).
2. Classified Information may be transferred within Finland by regular mail, in a registered form or by using a courier procedure approved for the particular classification level. Outside Finland regular mail is used only after an approval by the respective authority.
3. Internal mail handling chain within the organisation consists only of approved personnel.
4. Organisation has recognized the requirements for the transfer of items requiring special attention (e.g. crypto keys) and the required measures have been taken into use.

On classification level III (CONFIDENTIAL) this requirement may be fulfilled by using following procedures in addition to the point 4 above:

5. Classified Information is packed in a non-transparent double envelope (or equivalent). The outmost envelope may not contain any sign of a classification and may not reveal from outside that it contain Classified Information.
6. Classified Information may be transferred to the recipient under constant supervision of a person authorised to handle information on the same classification level. Alternatively, the delivery may be done according to some other procedure for this classification level.
7. Internal mail handling chain within the organisation consists only of security-cleared personnel.

On classification level II (SECRET) this requirement may be fulfilled by using following procedures in addition to the points 4, 6 and 7 above:

8. Classified Information or material is packed in a non-transparent double envelope (or equivalent). The outmost envelope may not contain any sign of a classification and may not reveal from outside that it contain Classified Information. The inner envelope has to be sealed. The recipient has to be instructed to inspect the integrity of the seal and to inform the sender if there is any doubt about the integrity.

F-08.2 – COPYING OF CLASSIFIED INFORMATION

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/EU)
1. **The security measures applicable to the original document shall apply to copies and translations thereof.** **Classification level II (SECRET):** in addition to point 1 above 2. **Copies produced of the material belonging to classification level II (SECRET) have to be listed. Same applies to people handling these copies.** 3. **Before copying material belonging to classification level II (SECRET), an approval for copies has to be provided by the originating authority.** 4. **International Classified Information may be copied and translated, unless these procedures have been prohibited by the deliverer of the information.**	1. 1101/2019 section 2 (2) 2. 1101/2019 section 14 (1)4 3. 1101/2019 section 14 (1)3 4. –	1. Annex III (27) 2. – 3. – 4. Annex III (26)

Additional Information

In general: Printers and copy machines are considered to be information processing systems and thus they have to be approved to handle Classified Information to the respective classification level from technical, physical and administrative security perspective. Technical requirements may be fulfilled, e.g., by using independent devices.

Examples of implementation: Requirements for classification levels III (CONFIDENTIAL) and IV (RESTRICTED) may be fulfilled by implementing the following:

1. Copies are handled in a similar way as originals.
2. Copies may be handed over only for such personnel, which has the right to the information and need to the substance in it.
3. Copies or printouts may be taken only with machines, which fulfil the security requirements for the respective classification level.

For the information belonging to the classification level II (SECRET) the requirement may be fulfilled by adding to the points 1-3 above the following:

4. Copying and the handlers of copies are marked in a register or in a record or are listed in some other respective manner.

F-08.3 – REGISTERING OF CLASSIFIED INFORMATION

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/EU)
1. A registration point or a diary has to be dedicated for organisations, which handle international Classified Information. Registration points or diaries have to be defined as Secured Areas.	1. –	1. Annex III (17)
2. Reception and sending of information belonging to national classification levels II and III and international classification level CONFIDENTIAL or above has to be registered.	2. 1101/2019 section 14 (1)2	2. Art. 9 (2)
3. Handling of information belonging to classification level III (CONFIDENTIAL) or higher is marked either into an electronic log, information system, case processing system, case register or case information (e.g. as a part of the document).	3. 1101/2019 section 14 (1)1	3. Art. 9 (2)
4. Registration of international Classified Information belonging to classification level CONFIDENTIAL or above has to be done in a registration point dedicated for the purpose.	4. –	4. Art. 9 (2); Annex III (19)

Additional Information

In general: The term registration means in this context the use of a procedure, which registers the life cycle of the information, including the delivery and disposal. In case an information system is used, registration actions may be part of processes within the system.

In order to register the life cycle of the information typically requires, e.g., that assurance of tracing the incidents can be found.

F-08.4 – DISPOSAL OF INFORMATION IN NON-ELECTRONIC FORMAT

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/EU)
Classification level IV (RESTRICTED) 1. Disposal of Classified Information in non-electronic format has to be organised in a reliable manner. When disposing, such procedures are used which prevent reconstruction of the pieces of information in whole or in part. For the information in electronic format see I-21. Classification level III (CONFIDENTIAL): in addition to point 1 above 2. When international information belonging to the classification level CONFIDENTIAL is concerned, a disposal certificate has to be signed by the person disposing the information. This certificate will be saved at the registry. Registered information has to be updated correspondingly. The registry has to save certificates of disposal for at least five years (compare to F-08.3). Classification level II (SECRET): in addition to points 1 and 2 above 3. In case the originator of the information is another authority, it has to be informed about the disposal of the now unnecessary information, unless the information was returned to the originating authority. 4. Only a person nominated for the task by an authority may dispose information. The drafter may dispose draft versions. 5. International information belonging to the classification level SECRET has to be disposed in the presence of a witness. The person witnessing the disposal has to be security cleared at least to the classification level of the information being disposed.	1. 906/2019 section 21, 1101/2019 section 15 2. – 3. 1101/2019 section 15 4. 1101/2019 section 15 5. –	1. Annex II (8), Annex III (46) 2. Annex III (45), Annex III (43) 3. – 4. – 5. Annex III (44)

F-08.4 – DISPOSAL OF INFORMATION IN NON-ELECTRONIC FORMAT

Additional Information

In general: Disposal of non-electronic information needs to be organised in a reliable manner. The methods used in the disposal prevent reconstruction of the pieces of information in whole or in part.

Information has to be protected until the end of its life cycle. This has to be taken into account especially in situations when services of a third party are used for the disposal of the information. A practical solution is to follow the procedure, where the organisation responsible for the information monitors the handling of the information all the way until the end of the life cycle of the information, including the disposal.

It is recommended that devices and systems belonging to the complexity of defence-in-depth are based on European standards and on their minimum requirements. The table below lists standards, which can be used as references when evaluating an appropriate solution for the disposal of information:

Paper shredders	Reference standard	Standard classes	Desired level		
Paper shredders	DIN 32757 (old)	DIN 1 – DIN 6	**Classification level**	**National classified information**	**International classified information**
			II / S	DIN 5	DIN 6
			III / C	DIN 4	DIN 5
			IV / R	DIN 4	DIN 5
	DIN 66399 (new)	P1 – P7	**Classification level**	**National classified information**	**International classified information**
			II / S	P6	P7
			III / C	P5	P6
			IV / R	P5	P6

When particle sizes match the dimensions mentioned in standards above, the shredding waste can be disposed in a similar way as normal office waste. For the disposal, also other procedures may be used instead or for the support of shredding in order to guarantee that the reconstruction of information is prevented reliably (e.g. burning the shredding waste).

Subdivision I: Information Assurance

Subdivision I (Information Assurance) for Katakri provides requirements for appropriate protection when handling classified information in electronic format. Requirements have been divided in three chapters; communications security, systems security and operations security. Some specific themes (e.g. management connections, wireless transmission, remote use and backup procedures) have their particular requirements.

In case the target organisation is aiming at system accreditation by a competent authority, the protection measures have to fulfil the risk assessment findings of both the organisation itself and of the competent authority. The role of risk assessment is essential also on the management of changes. Bringing in new services or interfaces to the existing information handling environment may introduce risks, the mitigation of which leads into changes in some parts of the existing information handling environment and in security procedures.

Assessment use cases for information processing systems have been described more in detail in the Annex II. The role of risk management in Katakri supported use cases has been described more in detail in the Annex III.

In order to stay in control of expenses, it is recommended to pay special attention to correct classification of the information, as well as how to separate or limit the handling environment of the Classified Information to its minimum. For example, when separating the handling environment of CONFIDENTIAL (national classification level III) information from the environment of RESTRICTED (national classification level IV) information, the protection requirements set for CONFIDENTIAL level do not need to be taken into count in the RESTRICTED environment.

When assessing the handling environment of the Classified Information as a whole, it is necessary to take into account all requirements set in the Information Assurance subdivision. When assessing the fulfilment of certain requirements (especially I-12, I-14, I-17 and I-18) the acceptable implementation method is depending on whether the system will be used for handling national or international Classified Information.

Electronic handling of Classified Information includes risks differing from risks of other information set handling, like personal data. In planning and in assessments of the use of Classified Information it is important to pay attention to legislation-derived risks [3]. In Katakri supported use cases the approval of competent authorities typically [4] requires that the entire electronic handling environment is operating under Finnish legislation, thus ensuring the competence of the authority.

When assessing the Classified Information handling environment, it is valuable to understand that part of the environment may rely on cloud based technologies. Cloud based technologies do not - however - change any elementary risks, nor the need or necessity for the binding minimum controls for mitigating them. The relation between cloud-specific risks and minimum controls have been dealt in detail in the Criteria for Assessing the Information Security of Cloud Services (PiTuKri), published by the National Cyber Security Centre in Traficom.

[3] Legislation-derived risks refer to possibilities under 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' Classified Information. In addition to the physical location of Classified 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.

[4] Special cases include, e.g, information system projects related to international cooperation between authorities, where the responsibilities to inspect parts of the system and competences to do so are separately dealt with between security authorities of the member states sharing the project. International cooperation introduces many specific cases. When protecting the electronic handling of information, arrangements made by some EU institutions might be used as a basis when defining common security solutions.

Communications Security

I-01 SECURE INTERCONNECTION OF CIS – SECURITY OF THE NETWORK ARCHITECTURE

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/EU)
Classification level IV (RESTRICTED) 1. **The information processing environment has been separated from other respective environments** 2. **The connection of the information processing environment to the one(s) of another classification level requires the use of a firewall in minimum.** 3. **Data traffic exceeding the perimeter of a controlled physical Security Area has been encrypted using an encryption solution approved by the Crypto Approval Authority (CAA) for the respective level (see I-12 and I-15).** **Classification levels III (CONFIDENTIAL) and II (SECRET):** in addition to points 1 and 3 above 4. **The connection of the information processing environment to the one(s) of another classification level requires the use of a boundary protection service approved by the competent authority for the respective level.**	1. 1101/2019 section 11 (1 and 2) 2. 1101/2019 section 11 (1 and 2) 3. 1101/2019 sections 12 and 11 (7), and 906/2019 section 14 (4). 1101/2019 section 11 (1)	1. Annex IV (32-35) 2. Annex IV (32-35) 3. Art. 9 (4), Annex IV (25 and 35) 4. Annex IV (32-35)

Additional Information

In general: Separation of information processing environments is one of the most influencing factors in the protection of Classified Information. The goal for the separation is to limit the processing environment of Classified Information into a well manageable unity and especially to be able to limit the processing of Classified Information into environments, which can be considered secure enough. It is possible to process lower classification level information on processing environments for higher security level, but bearing in mind that the processing is done completely according to the protection measures for the higher level.

By default the information processing environments are considered to be mutually untrustworthy also in situations where information processing environments administered by different organisations are connected to each other. Information processing environments of the same security level may be connected through an encryption solution approved by the CAA (e.g. interconnection of physically separated information processing environments of the same organisation through a public network).

I-01 SECURE INTERCONNECTION OF CIS – SECURITY OF THE NETWORK ARCHITECTURE

Note: when the classification level of the management traffic (see I-04) gets higher than the classification level a boundary protection service approved by the respective authority for the upper classification level is to be used. In most of the cases, the use of the management traffic is limited to the same classification level. The protection principles of the management traffic are dealt in more detail in I-04. Internet, as well as MPLS networks provided by operators, and e.g. the so-called dark fibers are considered as public networks. Compare to I-12 and I-15.

Examples of implementation: The classification level IV (RESTRICTED) information processing environment may be connected to information processing environments of other classification levels through firewall technology and by limiting the traffic of high risk services (web-browsing, e-mail through internet etc.), which use lower classification level environment, by directing it through separate proxy servers, which filter their content.

It is possible to connect the information processing environments of the classification level IV (RESTRICTED) to Internet or to other untrustworthy networks, as long as the risks of the interconnection can be sufficiently mitigated for classification level IV (RESTRICTED). Risk mitigation for classification level IV (RESTRICTED) requires especially taking care of software updates (see I-19), user rights matching with least privileges (see I-06), system hardening (see I-08) and the capability to incident detection and recovery (see I-11). A typical use of the classification level IV (RESTRICTED) information processing environment is to use it as a part of the office network of the information processing environment, which may consist of e.g. terminal services, application services, and communication network services and of the arrangements used for their protection.

From classification level III (CONFIDENTIAL) onwards the connections to environments of different security level may be done using boundary protection services approved by respective authorities. Design principles for secure boundary protection services is to follow the rules for the Bell-LaPadula model: ”No Read Up” and ”No Write Down”. In other words boundary protection services have to prevent in a reliable way the higher classification level information to be transferred into the lower classification level environment.

Secure design principles and general solution models for boundary protection services which may be approvable have been described in detail in instruction Guidelines for boundary protection services, published by the National Communications Security Authority in the Finnish Cyber Security Centre Regulatory Authority; (www.ncsa.fi > “Ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista”). The document is available in Finnish only.

The classification level III (CONFIDENTIAL) information processing environments are separated from untrustworthy networks or systems using a multi-layer logical or physical separation. The definition “physical separation” stands here for the separation put into effect on the physical layer of the OSI-model. Classification level III (CONFIDENTIAL) information processing environments are normally not connected to other networks/systems. When the end user, based on given duties, has to have access to internet or to systems/networks of other classification levels, the most reasonable way to achieve this tends to be the use of a separate computer, which has not been connected to the classification level III (CONFIDENTIAL) network. The competent authority may, case by case, approve the connection of the classification level III (CONFIDENTIAL) information processing environment to a network or system, which has been inspected and accredited before the interconnection will be done. These separately accredited networks/systems can be roughly divided into four different use cases:

I-01 SECURE INTERCONNECTION OF CIS – SECURITY OF THE NETWORK ARCHITECTURE

A. Data transfer systems

Classification level III (CONFIDENTIAL) system or network may be a data transfer system between two or more physical points. In this case each of these points should fulfil the requirements of the classification level. In most of the cases the network interface is of the form [physically separated network/work station] – [hardware or software firewall] – [crypto device approved to the classification level] – [hardware or software firewall] – [Internet] – [hardware or software firewall]- [crypto device approved to the classification level] – [hardware or software firewall] -[physically separated network/work station]. Similar arrangement may be used for classification level II (SECRET) solutions.

B. Service systems

Classification level III (CONFIDENTIAL) system or network can be e.g. database service used from several physical points. In this case the network level interface follows the case A.

C. Boundary protection services

C1. It is possible to transfer data to level III (CONFIDENTIAL) information processing environment from the one of the lower level through a one-way flow regulator, like a data diode. Similar arrangement may be used for classification level II (SECRET) solutions. In the data transfer between classification levels IV (RESTRICTED) and III (CONFIDENTIAL), a content filtering solution, using element detection may also be used (see point C2 below).

C2. The lower classification level data may be transferred from the classification level III (CONFIDENTIAL) environment to a lower classification level environment using a content filtering solution, based on element detection. The prerequisite for using a content filtering solution is to identify the information content element on the upper classification level environment, in order to let only the lower classification level information elements be transferred from the upper to the lower classification level environment.

D. Other information processing environments

Other level III (CONFIDENTIAL) information processing environments are normally research and development networks of the particular organisation, or other level III (CONFIDENTIAL) information processing environments. Connections to such systems may only be from the ones, which serve this dedicated environment, such as an update server. Update server may be allowed to deliver security updates or fingerprints of malware with certain restrictions. The deliverable updates or fingerprint bases can be imported to the update server through an airgap or, e.g., through a data diode.

Information processing environments for level II (SECRET) are by default physically separated unities, to which the data transfer from other classification levels is only allowed through data diodes or through respective one-way flow regulators, operating on physical layer of the OSI-model.

I-01 SECURE INTERCONNECTION OF CIS – SECURITY OF THE NETWORK ARCHITECTURE

Aggregate of Classified Information: An aggregate of Classified Information in information processing environments may warrant a level of protection corresponding to a higher classification than that of its individual components. Quantity of classified information is not, however, the only reason for elevated classification; sometimes the classification of the information may get higher due to the combination of two different information sources. In the majority of these cases a large amount of classification level IV (RESTRICTED) information in a compiled form creates a protection need equaling the one used to protect level III (CONFIDENTIAL) information.

There is no general formula to evaluate aggregation for all cases. On the national assessments it is important to pay attention to the Act 906/2019 on Information Management in Public Administration , according to which a security classification marking shall be made if the document or the information included 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 and 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 security of Finland. Large amount of Classified Information does not automatically lead into the aggregation effect. Assessment of the possible aggregation requires always an assessment of the existing information content versus the forthcoming one, as well as estimation, whether the aggregated information pool should be classified to, e.g., level III, based on the Act on the Openness of Government Activities 1999/621.

In aggregation cases the protection measures for this elevated information processing environment should then follow the requirements set for the higher classification level information processing environment. According to this procedure the access to the information should be limited, following the need-to-know principle, and 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. When using Katakri as an assessment tool this aggregate effect should be interpreted to require the use of a higher protection level measures for physical security, for I-13 (application layer security), for I-10 and I-11 (traceability and detection capability), as well as for I-06 (separation of duties). It is worth noticing that in cases where the protection level of the pool of information has risen with one level there is no need for an approved boundary protection service between the pool of information (e.g. level III (CONFIDENTIAL)) and the terminal equipment (e.g. level IV (RESTRICTED)). On management solutions for aggregated level III (CONFIDENTIAL) information it is important to bear in mind that terminal devices used for the management have been reliably separated from networks connected to internet.

Other sources of information: Ohje hyväksyttävien yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista (NCSA-FI, in Finnish only); CIS Critical Security Controls (v7.1) / 13; CIS Critical Security Controls (v7.1) / 14; BSI IT-Grundschutz-Compendium Edition 2019; SFS-EN ISO/IEC 27002:2017 13.1.1, 13.1.3; Recommendation of the Information Management Board (2020:19, chapter 6); PiTuKri TT-01

I-02 PRINCIPLE OF LEAST PRIVILEGE - SEGMENTING OF THE COMMUNICATION NETWORK AND FILTERING RULES WITHIN THE CLASSIFICATION LEVEL

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/EU)
The segmenting of the communication network and the filtering rules has to be done following the principles of least privilege and defence-in-depth.	1101/2019 sections 7 and 11 (2 and 3)	Annex IV (16,18,19 and 33-34)

Additional Information

In general: The division of the communications network into separate network areas (zones, segments) may mean, from the information protection point of view, e.g. separating the workstations and servers. This applies also for the separation needs in individual projects. The traffic monitoring and limitation between the network areas may be carried out on the boundary of the classification level IV (RESTRICTED) network by e.g. denying all incoming connections and by limiting the outgoing connections to web-browsing and email traffic through a proxy server. In networks of all classification levels the adequate consideration of the least privilege principle typically requires that within the classification level only the necessary connections between the network areas are allowed (source-target-protocol) and that other connection attempts are detected. Protection measures may be complemented and supported also by using the so called Zero Trust approach, which gives the possibility to limit and control functions of different actors, based especially on the identification and authentication of actors and functions. It is essential to ensure the secure functioning of connections and configurations on regular basis.

Every connected IT system should be considered untrustworthy and one should be prepared for general network attacks. Preparation for general network attacks includes e.g. that only the necessary functions are kept on. This means that each functionality, which is kept on, should be justified by the operation. The functionality should be limited to the narrowest subset, which fulfils the operational requirements (e.g. the limitation of the visibility of functionalities). In addition such things as prevention of spoofing and limitation of visibility of networks should be taken into account. At classification level IV (RESTRICTED) also the possibility of a denial of service should be kept in mind in cases where the system will be connected to an untrustworthy network.

The filtering should be based on the least privilege principle and it should let through only such traffic which has been approved (default-deny). The functionalities of different protocols (e.g. IPv4, IPv6, GRE, IPSec tunnels, routing protocols and protocols of higher layers, like HTTP, SSH, FTP and SMTP) should also be taken into account. Unnecessary protocols should be disabled in all such systems (workstations, servers, network devices etc.) where they have no real operational use. In addition the traffic denial (network, workstation and service levels) should be ensured by filtering rules of the firewalls. In case workstations, servers, network devices and in other similar systems e.g. IPv6 feature is used, the consequences should be taken into account especially in the filtering (firewalls should cover the IPv6 traffic) and routing of traffic. Effects of connecting and multi-use solutions (e.g. IPv4-IPv6 solutions, NAT-64, Teredo) of different protocols should be taken into account in general planning of the network or the system security.

I-02 PRINCIPLE OF LEAST PRIVILEGE - SEGMENTING OF THE COMMUNICATION NETWORK AND FILTERING RULES WITHIN THE CLASSIFICATION LEVEL

Examples of implementation: On classification levels IV (RESTRICTED) to II (SECRET) this requirement may be fulfilled by the carrying out the following:

1. communications network has been divided within the classification level into separate network areas (zones, segments)
2. traffic between network areas is monitored and limited in a manner where only such pre-authorised traffic, which is essential for the operation, is allowed (default-deny).
3. information processing environment has been prepared to stand general level network attacks.

Other sources of information: BSI IT-Grundschutz-Compendium Edition 2019; CIS Critical Security Controls (v7.1) / 12; CIS Critical Security Controls (v7.1)/ 14; SFS-EN ISO/IEC 27002:2017 13.1.1, 13.1.2, 13.1.3; PiTuKri TT-01; PiTuKri TT-02

I-03 SECURITY OF INFORMATION PROCESSING ENVIRONMENT THROUGHOUT THE LIFE CYCLE – MANAGEMENT OF FILTERING AND MONITORING SYSTEMS

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/EU)
The appropriate operation of filtering and monitoring systems will be taken care of throughout the life cycle of the information-processing environment. a) Amendments, changes or removals in the setup of filtering and monitoring systems has been organised and tasked.	1101/2019 section 11 (2), 906/2019 section 13.	Annex IV (8–12).

b) The documentation of the network and the respective filtering and monitoring systems is maintained through its life cycle as an integral part of the process of change and configuration management.

c) The setup and the desirable operation of the systems filtering and monitoring the traffic will be performed periodically during the operation and maintenance of the information-processing environment and when exceptional circumstances arise.

Additional Information

In general: Systems filtering and/or monitoring the traffic are typically firewalls, routers, IDS/IPS-systems and the ones with similar functionalities (network devices/servers/applications).

To set up an adequate documentation usually requires e.g. the description of the network structure, including the network areas (zones and segments) precisely enough, so that the the network is possible to assess against structural requirements set by the competent authority.
In order to ensure the availability and an adequate documentation it is appropriate to back up the filtering and monitoring system configurations and to store these backups according to their classification level.

The frequency of inspections for configurations and the required actions depends especially on the frequency of the amendments and of the scale of the inspected target. For instance, the firewall rules of the organisation using a classification level IV (RESTRICTED) information-processing environment may be vast and the need for changes may be frequent. In such environments a sufficient inspection frequency could be e.g. after every quarter of the year or twice a year. On the other hand, in such small-scale environments where filtering rules does not need constant fine-tuning, a yearly inspection might do. Functionalities of filtering or monitoring software may change or be renewed even in regular software updates. The filtering rules and the correctness of functionality needs to be checked also after regular software updates. Possibilities to take into use new features (like more sensitive filtering) have to be assessed as one part of change management (see I-16).

Other sources of information: CIS Critical Security Controls (v7.1) / 11; BSI IT-Grundschutz-Compendium Edition 2019; SFS-EN ISO/IEC 27002:2017 13.1.2, 18.2.1, 18.2.3;

I-04 SECURE INTERCONNECTION OF CIS – MANAGEMENT CONNECTIONS

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/EU)
1. Management connections have been separated on the basis of the classification level, unless a boundary protection service approved by the competent authority for the particular classification level is used. **2. In case Classified Information is embedded to the management traffic and if the traffic has been routed through a lower classification level environment, the Classified Information has been encrypted using a crypto solution approved by the competent authority.** **3. In case the management traffic flow will stay inside the same classification level, the unencrypted transmission or encryption at a lower level may be used based on the results of the risk management process and subject to the approval by competent authority.** **4. Management connections have been limited according to the least privilege principle.**	1. 1101/2019 section 11(1) 2. 1101/2019 sections 12 and 11 (7), and 906/2019 section 14 3. 1101/2019 section 12 and 906/2019 section 14 4. 906/2019 section 16, 1101/2019 section 11(3)	1. Annex IV (32–35) 2. Art. 9 (4)10, art.10(6), Annex IV (25) 3. Annex IV (31) 4. Annex IV (16 and 18–19)

In general: In examples of implementation below the devices or interfaces mean systems where the management rights should be limited only to the personnel responsible for the maintenance or having similar duties. These include typically the firewalls, routers, switches, wireless base stations, servers, workstations, separate console interfaces (e.g ILO, iDrac) and management interfaces of Blade enclosures.

When assessing the protection of management connections, especially the risk of the disclosure of Classified Information through the management connection should be taken into account. Most of the management connection means make it possible to access Classified Information either directly (e.g. database administrator usually has access to the content of the database) or indirectly (e.g. network device maintenance usually can change the firewall settings), which makes these access possibilities a very attempting target for malicious actors. Especially in situations where the management connection provides a direct or indirect access to Classified Information, the management connection and the terminals connected to it should be kept on the same classification level as the information-processing environment.

The management of a lower classification level environment may, in certain cases, be possible from the upper classification level management environment, if at the boundaries of the classification levels a boundary protection service approved by the competent authority for the respective classification level is used to block the information flow from the upper classification level to the lower level environment. Especially the software vulnerabilities of transfer protocols cause the fact that the management possibilities of lower level environment are typically limited - based on risks - only on the management of lower level environments from environments belonging to classification level IV (RESTRICTED). Due to the security critical nature of the management traffic, by default it is not possible to manage the upper classification level environment from the lower classification level environment. From the upper classification level environment it is possible in some cases, through a boundary protection service approved by competent authorities, to offer a read-only access to the environment, which is one classification level lower.

.

I-04 SECURE INTERCONNECTION OF CIS – MANAGEMENT CONNECTIONS

Additional Information

In order to achieve an adequate traceability within the classification level it is possible to use the so called jump host procedure, in which all management actions are executed through extremely hardened, system and role specific jump hosts, thus enabling the possibility for an extensive traceability (for logging, see I-10). The prerequisites of remote management are described more in detail in the requirement I-18.

Examples of implementation: On national classification levels IV to II the requirement can be fulfilled by putting into force the following:

1) There is no connection to the management connections of the information-processing environment from the environments of other classification levels, unless the boundary protection service has been approved by competent authorities (see I 01).
2) The workstation used for the management is connected to the device or interface through a crypto solution approved by a competent authority (see I-12) to the respective classification level in situations, where the management traffic is routed through a lower classification level environment
3) In situations where the management traffic will stay within the respective classification level (i.e. in encrypted form, encrypted with a crypto solution approved for the respective level by the competent authority and/or in a network physically separated from other environments and located inside a Security Area approved for the storage of Classified Information on the respective level).
   a) the management workstation of the respective classification level is connected to the device or interface physically (with e.g. console cable), or
   b) the traffic channel of the management connection of the respective classification level has been reliably physically protected (e.g. cabling within a Security Area), or
   c) the management workstation of the respective classification level is connected to the device or interface using a lower level crypto solution (e.g. SSH, HTTPS, SCP) to protect the connection
4) Only the management contacts from the sources following the least privilege principle and with defined user rights are allowed to the devices or interfaces.

Other sources of information: Ohje hyväksyttävien yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista (NCSA-FI, in Finnish only); CIS Critical Security Controls (v7.1) / 11; CIS Critical Security Controls (v7.1) / 14; BSI IT-Grundschutz-Compendium Edition 2019; SFS-EN ISO/IEC 27002:2017 13.1.1, 13.1.2, 13.1.3; PiTuKri IP-03; PiTuKri TT-01

I-05 EXCHANGE OF CLASSIFIED INFORMATION OUTSIDE THE PHYSICALLY PROTECTED AREAS - WIRELESS TRANSMISSION

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/EU)
Wireless transmission is encrypted using a crypto solution approved by the competent authority to the respective classification level (see I-12).	1101/2019 section 12 and 906/2019 section 14	Art. 9 (4), Annex IV (33 and 35)

Additional Information

In general: Usage of radio frequency interfaces on wireless transmission (e.g. WLAN, 3-5G, Bluetooth) is interpreted as an exit from a physically protected Security Area. In other words, the use of radio frequency interface is considered as communicating through a public network, which needs to be taken into account especially in encryption solutions (see 1-12) and in the execution of physical security measures. Many wireless interfaces are lacking proper implementation of protocols and software, of which outsiders may take advantage.

Respective protection principle is also applied for wireless peripheral devices (like mice, keyboards, headphones and display sharing systems). Exceptions to this rule are situations where risks for the use of wireless interfaces can be mitigated reliably with the use of physical security measures (e.g. using a wireless mouse in room located in the Security Area, when access to the vicinity is limited only for people authorized for the information handled). Attention must be paid also to such wireless devices like smart phones and other devices of a lower security level, which must not even temporarily be allowed to be connected to the information-processing environment for charging or for other purposes (see I-08, I-09, I-16).

Example of implementation:
in information-processing environments for classification levels IV-II the requirement can be fulfilled by implementing the following:
Wireless transmission is encrypted using a crypto solution approved by the competent authority to the respective classification level (see I-12).

Other sources of information: CIS Critical Security Controls (v7.1) / 15; BSI IT-Grundschutz-Compendium Edition 2019; PiTuKri SA-01

Systems Security

I-06 THE PRINCIPLE OF LEAST PRIVILEGE – MANAGEMENT OF ACCESS RIGHTS

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/EU)
1. User rights to information systems have been defined.	1. 1101/2019 section 8, 906/2019 section 16	1. Art. 7 (1), annex I (2)
2. User rights to information systems may be issued only after verifying that people involved have the right to handle this information (see T-13).	2. 1101/2019 section 8	2. Art. 7 (1 and 5), annex I (2)
3. Users and the automated processes of the information-processing environment shall be given only the access, privileges or authorisations they require to perform their tasks.	3. 906/2019 section 16, 1101/2019 sections 8 and 11(3)	3. Annex IV (19)
4. User rights to have to be maintained updated.	4. 906/2019 section 16	4. Annex IV (8 and 9)

Additional Information

In general: One of the key principles in the managing of user rights is the confidence that only authorised users have access to the information-processing environment and to the information handled through it. It is advisable to base the user rights on an agreement or on some other documented justification which can be verified (e.g. documented personal tasks or a work contract). The life cycle of user identifiers has to be taken care of, in order to make sure that only such identifiers that are needed are valid and active and those user identifiers, which are no longer needed, will be instantly deleted.

User rights have to be limited to the subset needed to perform their tasks. User rights, which are kept too vast, make it possible for users, processes or for the potential attacker getting access to them, to take serious advantage. When following the principle of least privilege in limitation of user rights, risks deriving from intentional or unintentional actions, as well as from, e.g., malware can be mitigated. Special attention has to be paid on the usage of administrator rights only to administrator actions. User account with administrator identifier shall not be used for web browsing or for email.

Verification on the validity of access rights: In order to verify the validity of access rights it is important to audit the user and access rights on a regular basis, like every 6 months. When the characteristics in working positions change - which happens through promotions, resignations etc. - the changes should be taken into account in a clear and well-functioning way. Such a clear manner could be a procedure where the foreman informs people responsible for managing access or user rights in advance. This may mean in practice, that access and user rights are deleted or changed using a centralised managing system or by implementing the changes in several systems one by one.

I-06 THE PRINCIPLE OF LEAST PRIVILEGE – MANAGEMENT OF ACCESS RIGHTS

Separation of duties: An adequate separation of duties is largely depending on the use of the particular system. In most of the systems, an adequate separation of duties may be achieved by separating the maintenance roles of the system (and users) from the ones of log monitoring (and user) . It is quite typical also to require several people for critical maintenance and other respective tasks (two-man rule).

Taking the inspection rights into account in technical solutions: Owners of the Classified Information often reserve a possibility to inspect all such systems, which handle their information. In many cases these inspections require both physical and logical access to the target under inspection, and therefore the inspectors often have a technical possibility to access the information itself. Especially in multi-project networks and in other demanding environments, where there is a need to handle the information belonging to multiple owners, it should be verified that the system has been designed to make these inspections possible in a way where the inspectors don't have access to the information which does not belong to them.

Information belonging to different owners may be separated according to three main classes:
a) For the classification level IV (RESTRICTED) information, a logical level separation (like virtualisation of servers and user right separation of network storage media) is sufficient.
b) For the information belonging to classification levels IV and III, the methods which are based on a reliable logical separation (like virtual machines with approved crypto on a dedicated, customer based physical disks and an approved encryption of the information or data flow on multiuse network devices) are applicable.
c) For the information belonging to classification levels IV, III and II, a solution based on physical separation (dedicated, customer based physical devices) may be used.

Note: the requirement for the separation of information is not valid for the classification level IV (RESTRICTED) in workstations or in other very limited data masses, assuming that there is a reliable method in use to avoid the aggregation. Information belonging to those who have reserved a right to audit the handling procedure of their information may be kept unseparated in cases where all owners of the information have in advance given their written consent to accept the risks cumulating of this inspection right. In the implementation of the above mentioned, a model may be used, where information is accepted only from such owners of information, who bind themselves not to use their right for technical inspection of the respective information-processing environment.

Examples of implementation: on processing environments belonging to classification level IV (RESTRICTED), the requirement can be fulfilled by putting into force the following:

1. User rights management for systems has been individually tasked.
2. Users of the system have been listed.
3. When granting the user rights for the system, the target personnel has been verified to be part of the organisation or is authorised to use the system based on other facts.
4. Administration (management and granting) of user rights has been instructed.
5. There is a clear and well-functioning way to handle the changes in the personnel by immediately informing all relevant players to take action.

I-06 THE PRINCIPLE OF LEAST PRIVILEGE – MANAGEMENT OF ACCESS RIGHTS

6. Every user right issuance is documented (electronically or in paper format) (see I-10).
7. User and access rights are regularly audited.
8. Classified Information in the information processing system is separated according to the principle of least privilege by using user right definitions and handling regulation or other respective methods.
9. Within the information processing system Classified Information are kept separated from public information or from the information classified to another classification level, or the entire information mass is handled according to the requirements set for the highest respective classification level.
10. Information which may or will be a target for inspections performed by the originator or the owner of the information are kept separate from each other using the method approved by the competent authority for the respective classification level. For processing environments belonging to classification levels III and II, the requirement can be fulfilled by putting into force the following, in addition to the functions described above (1-10):
11. Tasks and areas of responsibility are separated from each other as well as possible, in order to reduce the risk of unauthorized or accidental alterations or misuse of the protected assets. In case critical working combinations will be probable, there has to be a monitoring procedure in place to avoid negative consequences.
12. The Classified Information used in servers, workstations and in other storage media is stored, using an encryption method approved by a competent authority for the particular technical environment (see I-12) in cases, where the encryption is used to separate the information belonging to different owners, or/and if the storage media will - at some point of their life cycle - be taken out of the perimeter of the Security Area approved for the storage of the information for the respective classification level.

Other sources of information: CIS Critical Security Controls (v7.1) / 4; CIS Critical Security Controls (v7.1) / 14; CIS Critical Security Controls (v7.1) / 16; BSI IT-Grundschutz-Compendium Edition 2019; Instructions for the handling of international classified information (NSA unit of the MFA); NIST National Checklist Program Repository; SFS-EN ISO/IEC 27002:2017 6.1.2, 9.1.1, 9.1.2, 9.2.1, 9.2.2, 9.2.3, 9.2.4, 9.2.5, 9.2.6; PiTuKri IP-01

I-07 DEFENCE-IN-DEPTH - IDENTIFICATION OF ACTORS OF THE INFORMATION PROCESSING ENVIRONMENT WITHIN A PHYSICALLY PROTECTED SECURITY AREA

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/EU)
People, devices and information systems using the information-processing environment are identified reliably enough.	1101/2019 section 11(5)	Annex IV (16 and 19)

Additional Information

Examples of implementation: On classification level IV (RESTRICTED) this requirement may be fulfilled by using the following procedures:

Identification and authentication of persons:

1. Individual user identifiers are in use.
2. All users are identified and authenticated.
3. In identification and in authentication a well-known and reliable technique is used or the requirement has been covered in another reliable way.
4. Too many false attempts in the authentication will result in the locking of the identifier.
5. Maintenance identifiers for systems and applications are personal. In case this is not technically possible in all systems or applications, documented and settled password management procedures which make it possible to identify individual users are required for identifiers used my multiple persons (compare: management connections and especially jump host procedures in I-04 and implementation of traceability in I-10).
6. Authentication is done at least by the use of passwords. In case password authentication is in use, a) users have been notified about good practices in choosing and using the password, b) the application monitoring the usage sets up certain minimum requirements for the password and requires that passwords will be changed with appropriate intervals. The interval between password changes should be adjusted to the operation environment of the organisation and to the classification of the information processed in the device, taking into consideration other security measures in use.

Identification and authentication of devices:

7. Classified Information is processed only in such terminal devices which have been offered and managed by the organisation and which have been approved for the respective classification level. Connection of any other device to the processing environment of Classified Information is simply forbidden. The personnel has been instructed and obligated to follow instructions.

Identification and authentication of information systems:

8. Information systems exchanging information are identified with techniques proportioned for the case, like passwords, keys (e.g. API key), credentials (tokens, like oAuth) or with other respective methods. Identification and authentication is done using encrypted connections.

I-07 DEFENCE-IN-DEPTH - IDENTIFICATION OF ACTORS OF THE INFORMATION PROCESSING ENVIRONMENT WITHIN A PHYSICALLY PROTECTED SECURITY AREA

On classification levels III (CONFIDENTIAL) and II (SECRET) the requirement can be fulfilled by putting into force the following, in addition to the functions 1 to 5 and 7 to 8 described above:

9. Authentication of users is strong, relying on at least two factors.
10. Terminals are technically authenticated (device identification and authentication, 802.1X or equal procedure) before allowing to access the network or the service, unless the access to the network has been limited with physical means (e.g. setting the server in a locked rack cabin inside a Security Area which has been approved by a competent authority for the respective classification level).

To be notified: Classification level IV (RESTRICTED) environments, in which a threat of a Denial of Service is eminent (e.g. locking of identifiers on Internet connected identification and authentication services) the locking of the identifier may be replaced with some other method reducing the risk (e.g. methods of slow reply, filtering or a temporary locking). On classification level IV (RESTRICTED) a technical identification of terminals is normally not required, as long as the users are identified and authenticated.

The methods of strong identification and identification of the device on classification levels III (CONFIDENTIAL) and II (SECRET) may in some cases be implemented by limiting the access to the system only from a physically well-protected area (in most of the cases either a Security Area, a locked rack cabin or equivalent) with a strong access control system, based at least on two authentication factors. In such a case the identification of the user of the information-processing system may be based on user ID and password. In situations where the user identification and authentication relies on physical security procedures, also the procedures for physical security have to fulfil the requirements set for traceability (see I-10), especially with respect to storage time for logging information and other respective records.

Setting up a reliable identification and authentication procedure contains at least the following: i) the authentication method is protected against man-in-the-middle attacks, ii)
no additional information is disclosed in the login phase, before the actual authentication of the user, iii) the authentication credentials are always in an encrypted format if they are sent across the network, iv) the authentication method is protected against replay attacks, v) the authentication method is protected against brute force attacks.

Other sources of information: BSI IT-Grundschutz-Compendium Edition 2019; CIS Critical Security Controls (v7.1) / 1; CIS Critical Security Controls (v7.1) / 4; CIS Critical Security Controls (v7.1) / 11; CIS Critical Security Controls (v7.1) / 16; SFS-EN ISO/IEC 27002:2017 9.1.2, 9.4.1, 9.4.2, 9.4.3; NIST Special Publication 800-63B; PiTuKri IP-02

I-08 PRINCIPLE OF MINIMALITY AND OF LEAST PRIVILEGE - SYSTEMS HARDENING

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/EU)
1. **Only the essential functionalities, devices and services to meet operational requirements shall be implemented in order to avoid unnecessary risks.**	1. 1101/2019 section 11(3 and 6); 906/2019 section 13	1. Annex IV (16,18 and 19)
2. **Organisation uses a procedure through which systems are installed and configured systematically, resulting on a hardened installation.**	2. 1101/2019 section 11(3 and 6); 906/2019 section 13	2. Annex IV (8,16,18 and 19)
3. **Configuration contains only such components, services, user and process rights which are mandatory in order to fulfil the operational as well as the security requirements.**	3. 1101/2019 section 11(3 and 6); 906/2019 section 13	3. Annex IV (16,18 and 19)
4. **Configurations are maintained throughout the life cycle of the information system, including the effectiveness.**	4. 1101/2019 section 11(3 and 6); 906/2019 section 13	4. Annex IV (8,16,18 and 19)

Additional Information

In general:
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 mitigated 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 on by default and easy to take into use. On the other hand, these features are also often run with too vulnerable settings. If unnecessary features are not removed from use, they are available also for a malicious party. If the too vulnerable settings of unnecessary services are not changed, they are also available to malicious parties. 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. 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. Default settings of the system, which may be insecure, and for example unnecessary default user accounts have to be altered or deleted.

I-08 PRINCIPLE OF MINIMALITY AND OF LEAST PRIVILEGE - SYSTEMS HARDENING

The term *system* refers in this context to active components of the network, servers, workstations, mobile devices, printers, peripherals and other devices forming the system. The sufficiently hardened configuration (may be implemented for example by following DISA STIG, CIS or another respective level guidance. In case the handling of Classified Information includes the use of network printers, phone systems etc., the principles mentioned above should be used also to these systems.

Configuration management tools can often also be used for security hardening and its maintenance.

Example of implementation: in the processing environment for classification level IV (RESTRICTED) the requirement may be fulfilled with following procedures:
1. Targets for hardening have been identified.
2. Implementation of the hardening has been defined.
3. Targets have been hardenedaccording to definitions.
4. The hardened configuration is monitored throughout the life cycle of the information system and verified especially after updates.

To be noted in special:
a) Hardening is targeted on all devices in the information-processing environment, including active components of the network, servers, workstations, mobile devices, printers, peripherals and other devices forming the system.
b) In order to reduce the attack surface the devices are actively using only necessary services, interfaces, connections and buses, which all are following the principle of least privilege.
c) The firmware (BIOS and other respective components), the operating system, applications and respective components are hardened at least according to the recommendation by the manufacturer and/or using generally known hardening guidance. In addition to this the reconfigurations are tailored system wise, based on the functional purpose and risks. In case no hardening guidance exists for the component, guidance for respective components are used.

In the processing environments for classification levels III and II the requirements may be fulfilled by adding to the previous points 1 to 4 additional hardening guidance and by using more stringent interpretation on the setup of parameters.

Essential about hardening:
1. Default passwords have been changed to quality ones which fulfil the password policy of the organisation. Passwords are stored in a way that they are under protection and available.
2. Unnecessary services, applications, connections (also on BIOS level) and devices have been removed.
3. Users, interfaces and devices are identified and authenticated (see I-07).
4. Necessary services can be reached only for necessary level, concerning networks, devices and user identification.
5. Software (e.g. firmware, applications) are kept up-to-date (see I-19).

6. Connections to the target, including management connections, are limited, hardened, use user identification and authentication and a time limitation (session time-out).
7. Applications, interfaces and respective elements have been hardened, limited and their features are following the principle of least privilege.
8. Software, like operating systems, applications and firmware are set to collect the necessary logging information in order to detect misuse (see I-10).
9. Booting procedure from unknown, non-primary device has been prevented.

Compensatory methods: When the control of the network device is not technically possible through the individual user ID, the procedure which allows the access to the password shall only be possible after involvement or two persons. When the size of the environment is considered to be large, the use of duplicated AAA-servers (especially TACACS+, RADIUS or Kerberos) is recommended.

Especially on higher classification environments it is reasonable to detach unnecessary components (for example wireless network adapters, cameras, microphones) physically from devices and thus tackle the requirement to prevent usage. In situations where the physical detachment is impossible, some compensative protective measures may be used; for example cameras can be blind taped and devices may be taken out of the configuration through software settings or by changing user settings, settings in the operating system or in firmware. In some operating systems the protective measures can also be complemented by the removal of software elements for the respective device (kernel module).

Other sources of information: CIS Critical Security Controls (v7.1) / 2; CIS Critical Security Controls (v7.1) / 5; CIS Critical Security Controls (v7.1) / 7; CIS Critical Security Controls (v7.1)/ 9; BSI IT-Grundschutz-Compendium Edition 2019; The United States Government Configuration Baseline (USGCB); NATO Best Practice Configuration Guidance; DISA Security Technical Implementation Guides (STIGs); NIST Special Publications (800 Series); NIST National Checklist Program Repository; Microsoft DSC Environment Analyzer; Microsoft Baseline Management; CIS benchmarks; PiTuKri JT-02

I-09 DEFENCE-IN-DEPTH – PROTECTION AGAINST MALWARE

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/EU)
Reliable methods for deterrence, prevention, detection, resilience and recovery measures of malware are used in the information processing environment in order to prevent unauthorised changes and other unauthorised use of the information.	1101/2019 section 11 (2)	Annex IV (8,9,16,18,19,21 and 22)

Additional Information

In general: Set of methods can be used for the protection against malware risks. These methods include systems hardening (see I-08), limitations in user rights (see I-06), maintaining the system's software fully patched (see I-19), capability to detect incidents (see I-11), taking care of the security awareness (see T-12) and also the use of malware protection software (anti-malware). Risks can also be mitigated by separating high-risk environments from production environments, as well as by limiting the use of removable media (like USB sticks). Malware protection software can be left uninstalled on environments where the access for malware has been prevented with other means (e.g. systems without input/output interfaces or where transferrable information is carefully validated or sanitized on strictly controlled interfaces).

Examples of implementation: on processing environments belonging to classification level IV (RESTRICTED), the requirement can be fulfilled by putting into force the following:

1. User rights of systems have been limited according to the principle of least privilege (see I-06).
2. System security updates (patches) are taken care of (see I-19).
3. Systems have been hardened, leaving only necessary functions and software components in use (see I-08).
4. Security awareness of the personnel has been taken care of (see T-12). Users are aware of malware threats and of how to follow security principles of the organisation.
5. Systems where malware protection software (anti-malware) provides added value have been recognized.
6. Malware protection software (anti-malware) has been installed to all such systems which are vulnerable to malware infections. These include typically e.g. gateways of public network (for example email and www traffic) and terminal devices connected to external interfaces (other networks, USB media etc.).
7. Malware protection software (anti-malware) is running and able to act.
8. Malware protection software (anti-malware) produces logs of its functions and gives alarms.
9. Malware fingerprints (and respective) are updated regularly.
10. Malware detection and alarms are monitored regularly and they cause reaction.

I-09 DEFENCE-IN-DEPTH – PROTECTION AGAINST MALWARE

For processing environments belonging to national classification levels III and II, the requirement can be fulfilled by putting into force the following in addition to points 1-10 above:

11. All use cases for the import and export of information have been recognized. Security operating procedures have been defined, instructed and monitored. Security operating procedures include assessment of need for the usage of USB ports and other respective interfaces in the system.
    a) If no essential reason can be found after a critical assessment, the interfaces are removed from use.
    b) In cases where a reason can be found after a critical assessment, the estimation is done case by case to define the prerequisites and conditions for devices and media (like USB sticks) to be connected to the system.

Environments isolated from public networks:
In systems, which are not connected to public networks the updates of malware fingerprints can be arranged by using e.g. a separated, internet connected but managed and protected update server, the fingerprint downloads, keeping the fingerprints up-to-date on the server, and by importing the fingerprints manually (e.g. once a day) or by through an approved boundary protection service (see I-01). Adequacy of the update frequency of fingerprints has to be evaluated in the risk assessment and in relation to the characteristics of the environment, taking especially into account the general traffic density of the environment. Note: there should be a manner to verify the integrity of updates (source, checksums, signatures etc.).

The requirement may be set on a case by case basis to ensure that USB ports (or other respective interfaces) may only be used to connect a dedicated and approved USB stick (or equivalent) to the system, and that they are not connected to any other system. Case by case requirements may, for instance, include an arrangement where only storage media delivered by the ICT management of the organisation may be used, whereas the connection of all other storage media is prohibited and/or technically prevented.

In cases where there is a specific need to import information from untrustworthy sources by using storage media, the permission to use such an exceptional procedure normally sets conditions in order to mitigate the risk. One possible method could be the connection of the storage media to an isolated inspection system, from where the information would then be transferred - after a temporary storage - to a separate storage media, which would be used to import the information into the trusted system. When using such arrangements on level III at least the memory area has to be inspected and from level II on also the controller level tailored threats are to be taken into account.

Other sources of information: CIS Critical Security Controls (v7.1) / 8; BSI IT-Grundschutz-Compendium Edition 2019; SFS-EN ISO/IEC 27002:2017 12.2.1; PiTuKri JT-04

I-10 DEFENCE IN DEPTH – TRACEABILITY OF SECURITY EVENTS

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/EU)
1. In order to detect unauthorised changes or other unauthorised or inappropriate information handling within the information-processing environment, reliable methods have been taken into use for tracing the security events. **2. The use of information systems and disclosure of their information will be logged in case the use of the information system requires identification or other methods of signing in. The idea to collect log information is to follow the use and disclosure of the information and to find out reasons for technical system failures.** **3. The use of Classified Information belonging to national classification levels II and III has to be registered into an electronic log, information system, case register of as a part of information itself (e.g. part of a document).**	1. 906/2019 sections 17, 15, 1101/2019 section 7 2. 906/2019 section 17 3. 1101/2019 section 14	1. Annex IV (16), annex III (18 and 21) 2. – 3. –

Additional Information

In general: 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, log data of workstations, etc. are also very often covered by this.
The coverage requirement can, in most cases, be met by checking that logging is on at least for workstations, servers, network devices (especially firewalls, but also for software firewalls on workstations). 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 who. 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 (or servers), the information content of which is regularly backed up. The logging server(s) must be at environment belonging at least to the same classification level as the log source environment.

Collection and recording of log data needs to be done in a way where the removal of changing of log data can be detected even in situations, where e.g. the log source and the log collector are disconnected. Correspondingly, the collection of log data and their backups from workstations permanently disconnected from the network requires a regular process in place. To support the legal protection of administrators and promote investigation of suspected security breaches, it is recommended to separate tasks so that the logging data maintenance duty is separated from other maintenance duties. In the implementation of traceability also situations, when the individual who has logged in to the system has the possibility to function by using another user account (user impersonation) has to be taken into account. The functioning of logging data storage and analysis software must also be monitored and possible failures have to be detected in a short time frame (e.g. within 24 hours after the log source has stopped to deliver the logs).

I-10 DEFENCE IN DEPTH – TRACEABILITY OF SECURITY EVENTS

The log data storage periods must take into account the needs of the use case in question. For example, for information processing and delivery logs it may be advisable to require storage durations which differ from the storage duration for logs, which are collected to sort out exceptional situations In the activities of the authorities, for example, statutes of limitation in the criminal justice can typically lead to a required storage period of at least five years. As a general practice log data for 6 months is available on a real-time basis and earlier log data will be available within a couple of days, when needed. Different cases for handling log data are covered also in the recommendation of the Information Management Board (2020:21, chapter 7).

In the implementation it should be taken into account that the duration and storage capacity of the logs will be sufficient (normally needs to be increased). Recommendation: to reserve enough capacity, the estimation can be based on the processing environment. Definition of an adequate duration can be done by e.g. calculating the storage capacity sufficient for one month and using this information to determine the storage capacity needed for the storage duration. Note: it is advisable to reserve some buffer capacity, as situations change and because certain type of attacks increase log activities a lot.

Example of implementation: on processing environments belonging to classification level IV (RESTRICTED), the requirement can be fulfilled by putting into force the following:

1. A policy document defining the generation, release, alarm and follow up of the logs has been taken into actual use. This policy has been written taking into account the particular operational requirements.
2. Logs make it possible to detect the security breaches or attempts to such afterwards.
3. Essential recordings are kept for at least six months, unless laws and regulations or separate contracts specify a longer retention period. Processing logs and recordings following the requirements set for, e.g., periods of limitation of the information in criminal justice cases are stored for at least five years.
4. Log files and respective register services are protected against unauthorised access (user rights management, logical access control).) A policy document defining the generation, release, alarm and follow up of the logs have been taken into the actual use. This policy has been written taking into account the particular operational requirements.

On classification levels III and II this requirement may be fulfilled by using the following procedures in addition to the points 1-4 above:

5. Essential recordings are kept at least for five years, unless laws and regulations or separate contracts specify a longer retention period. Recordings with very little value to, e.g., sorting out exceptional situations or to periods of limitation of the information in criminal justice, may be retained a shorter period, for example 2-5 years.
6. Log files are backed up regularly.
7. Clocks of all relevant information processing systems within security domain must be synchronized to a single reference time source.
8. Procedure covering the integrity of the logs has been taken into use.
9. Handling and usage of log files is registered.

Other sources of information: CIS Critical Security Controls (v7.1) / 6; BSI IT-Grundschutz-Compendium Edition 2019; The United States Government Configuration Baseline (US- GCB); SFS-EN ISO/IEC 27002:2017 12.4.1, 12.4.2, 12.4.3, 12.4.4, 18.1.3; VAHTI 3/2009; Recommendation of the Information Management Board (2020:21, chapter 7); PiTuKri JT-01

I-11 DEFENCE-IN-DEPTH - INCIDENT DETECTION AND RECOVERY

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/EU)
Reliable methods are taken into use in the information processing environment in order to detect attacks against the information processing environment, to limit the effect to a minimum amount of the information and to minimum resources of the information processing environment and to prevent other damages, as well as to restore the protected status within the information processing environment.	906/2019 sections 13.1 and 17, 1101/2019 section 7	Annex IV (16)

Additional Information

In general: Ability to detect abnormal events and incidents technically is normally based on three sources: 1) events in the network traffic 2) collected logs and 3) events detected at hosts. A sufficient technical detection capability can normally be achieved by combining the above-mentioned detection sources. The better the information-processing environment and its functions are known, the better also abnormal events can be detected. Detection of abnormal events also supports the detection of such attacks, of which attack indicators are missing (IoC, Indicator of Compromise). The normal functioning of the information-processing environment should be well known from the beginning of the life cycle to the removal from service. Also the change management (I-16) supports the capability to detect abnormal events, e.g. by periodic scrutiny of changes in device and software configurations.
There are numerous solutions on how to solve the detection and how to limit the detected attack, starting from the monitoring on the network node level down to workstation/server sensors and to their combinations. Regardless of the network devices or operators, the actual capability to detect changes on the network level requires understanding of the normal status (baseline) of the network traffic. On classification level IV (RESTRICTED) the detection capability on the network traffic level should cover specifically the outmost border of the network or the target. From the classification level III (CONFIDENTIAL) on the boundary protection services on the outer border, as well as the traffic inside the network/other object should respectively be monitored.

To detect an attack or an intention of misuse in practice, the use of automated detection and alarm tools are required in most of the environments. Manual inspection of logs is possible and even necessary in some situations, where the automated detection has failed in the detection and further investigations are needed. It is essential to remember that information collected on logs has to be the ones needed for information security purposes, and that no such actions, which could limit the freedom of speech or the protection of classified messaging or privacy, are used. In general it is valuable to understand that the detection capability requires a good knowledge of the characteristics of each information-processing environment, definition of critical targets and events to be followed and their customising to match the information-processing environment in case. In addition, the detection capability has to be maintained constantly.

I-11 DEFENCE-IN-DEPTH - INCIDENT DETECTION AND RECOVERY

To restore the protected state of the information-processing environment within reasonable time frame, planned, described, trained and rehearsed processes and technical methods are normally required.

In the development and up keeping of the detection capability it is worth to notice the role of the entire personnel. For example, detection information received from end-users may provide valuable information into the process of detecting attacks or attempts. See T-07 (management of security events) and T-12 (security education and training).

Example of implementation: on processing environments belonging to national classification levels IV-II, the requirement can be fulfilled by putting into force the following:

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 is in use to detect anomalies on logs (see I-10) and on status information (like changes in log pile-up). Especially an unauthorised attempt to use the system has to be detected.
3. A procedure is in use to detect anomalies on hosts (e.g. workstations and servers) of the information-processing environment.
4. A procedure is in use to recover from the detected incidents.

Other sources of information: CIS Critical Security Controls (v7.1) / 6; CIS Critical Security Controls (v7.1) / 19; BSI IT-Grundschutz-Compendium Edition 2019; SFS-EN ISO/IEC 27002:2017 12.4.1, 13.1.1, 16.1.4, 16.1.5; VAHTI 3/2009; PiTuKri JT-01; PiTuKri TJ-05

I-12 EVALUATION AND APPROVAL OF CRYPTOGRAPHIC PRODUCTS - CRYPTO SOLUTIONS

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/EU)
Competent authority has approved crypto solutions or products in the current environment to the respective classification levels in order to safeguard and protect the information against unauthorised disclosure or loss of integrity.	1101/2019 section 11 (7)	Art. 10 (6), annex IV (25)

Additional Information

In general: Especially when communicating through a public network or the network belonging to a lower classification level, crypto solutions are often the only protections for ensuring the confidentiality and integrity of the Classified Information. Shortcomings in encryption solution are very difficult to be replaced with other protection means, resulting to the fact that it is essential to choose a right crypto solution and to use it properly.

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 (public good). On the other hand, 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.

In protecting Classified Information in particular, the need for using encryption solutions with reliable evidence of their sufficient security is emphasized. Several aspects must be taken into account in the evaluation 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 on the secrecy period and integrity of the information.

Crypto approvals of several international security authorities require that the correct functioning of the solution is evaluated, as well as the fulfilment of particular requirements concerning e.g. the delivery and evaluation of the source code, tampering and TEMPEST countermeasures. Pure software crypto solutions may typically be approved for classification level IV (RESTRICTED) and in some cases for level III. For classification level II (SECRET) and usually also for level III (CONFIDENTIAL), reliability requirements for the hardware are set. Approval process has been described in more detail in the Finnish National Cyber Security Centre Instruction for Crypto Evaluations and Approvals. Minimum requirements for crypto solutions are also handled in the Encryption Strength Description and in the Instruction for Secure R&D, both maintained by the Finnish National Cyber Security Centre.

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.

I-12 EVALUATION AND APPROVAL OF CRYPTOGRAPHIC PRODUCTS - CRYPTO SOLUTIONS

The security of the supply chain has to be taken into account in the risk assessment of crypto solutions. Although the crypto solution itself would be secure enough when leaving the manufacturer, deficiencies in the supply chain may expose the crypto solution for tampering and thus lead into an introduction of an insecure crypto solution as a part of the information-processing environment.

Example of implementation: on processing environments belonging to national classification levels IV-II, the requirement can be fulfilled by putting into force the following:

1. Organisation has identified use cases where encryption solutions are needed for the protection of Classified Information. Identified use cases cover all such situations where the protection of Classified Information solely or partly relies on encryption solution. Special attention has been paid to the traffic going through public or lower level network (see I-01), to the transfer of information to another organisation (see I-15 and F-08.1) and to terminal devices which are taken outside of Security Areas (see I-18).
2. The safeguards on a particular classification level have been implemented through a) crypto solutions, which are approved by competent authorities and which are used according to the user policy and respective specifications, or b) case by case approvals and user policies or specifications set by competent authorities for crypto solutions, which have not been approved before.
3. Secret keys can be used by authorised users and processes only. The processes require at least a) cryptographically strong keys, b) secure key distribution, c) secure key storage, d) regular key rollovers, e) changing of outdated or disclosed keys and f) prevention of unauthorised key changes.
4. Security of the supply chain has been verified on a sufficient level. Especially the supply chain from a trustworthy manufacturer to the particular information-processing environment has been ensured.

Other sources of information: List of approved cryptographic products of the Council of the European union; List of approved cryptographic products of NATO; List of approved crypto solutions of Finnish National Cyber Security Centre (NCSC); NCSC Instruction for Crypto Evaluations and Approvals; NCSC Encryption Strength Description; NCSC Instruction for Secure R&D; FI NSA Instruction for the handling of international classified information; CIS Critical Security Controls (v7.1) / 18; BSI IT-Grundschutz-Compendium Edition 2019; SFS-EN ISO/IEC 27002:2017 10.1.1, 10.1.2, 18.1.5; Recommendation of the Information Management Board (2020:19, chapter 7); PiTuKri SA-01

I-13 DEFENCE-IN-DEPTH THROUGHOUT THE LIFE CYCLE - PROTECTION OF SOFTWARE AGAINST NETWORK ATTACS

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/EU)
1. Security of information-processing environment, including their technical and non-technical security measures, shall be subject to security testing during the accreditation process to ensure that the appropriate level of assurance is obtained and to verify that they are correctly implemented, integrated and configured. **2. Protective measures are in place against network attacks. Protective measures and their well-functioning are taken care of throughout the life cycle of the information-processing environment.**	1. 906/2019 section 13 2. 1101/2019 section 11(2)	1. Annex IV (8,9,10,16,19 and 33) 2. Annex IV (10,11 and 19)

In general: Software and purposes for their use in different information-processing environments vary a lot. Consequently, also the needs for secure implementation and introduction of the software are remarkably different in different information-processing environments and purposes. To take an example, the needs for the security of an office application used in a workstation without any physical connections to any networks are radically different than the ones needed in the case management system with multiple users.

Risks and security needs for software may be assessed, e.g., based on the purpose for the use of software and how it potentially puts security into practice, on the potential attack surfaces and on the nature and classification level of the information processed. In case the role and the purpose for the use of the software is to limit the access to Classified Information, reliable functioning of the software should be ensured. Attack surface may have substantial impact on security needs for the software. Typically, e.g., services belonging to classification level IV (RESTRICTED) may be more accessible and for a heterogenic group of people, unlike e.g. services belonging to classification levels III and II. In fact, the security requirements set for level IV systems may be more stringent than in such compact higher level systems, which have been strictly isolated and in which all users have a need-to-know to all the information within the system. External actors pay potentially more attention to information, which has been classified, resulting in elevated risk and need for protection. For example information under great political interest or the information classified very high may remarkably influence in risks and in security needs also in the preparation for the most advanced cyber-attacks.

When a commercial application is taken into use and when tailored or self-produced software is about to be ordered, the organisation responsible for the order has to pay attention to secure development of the software and the components it will use. Attention has to be payed also to other factors during the life cycle of the software. Such factors can be the requirements for the introduction, contract technique, update procedure and the change control. Software, which has a significant role in the protection of Classified Information, has to be produced based on principles of secure software development, including both the quality of the programming code and the processes for the program development.

I-13 DEFENCE-IN-DEPTH THROUGHOUT THE LIFE CYCLE - PROTECTION OF SOFTWARE AGAINST NETWORK ATTACS

Additional Information

When defining requirements for the software it is important already at the ordering stage to notify the requirements deriving from legislation. Complexes related especially to crypto (I-12), management connections (I-04), user management and identification (I-06, I-07), systems hardening (I-08) and traceability (logging, I-10) have to be noticed in the implementation of software. Implementations of software may not put the principle of need-to-know in danger or to offer access for external actors to information-processing environment or parts of it, which need to be protected. In phases of life cycle, it is important to verify especially the responsibilities of software patching and to enable software security maintenance also when new attack techniques appear. It is also recommended to try to ensure the quality of commercial of-the-self software following the same principles.

Sometimes a need may arise to use services, where the program code and the visibility to development procedures of it may be weak or may even not exist. The reliability of such software may be assessed by studying update frequencies, documentation and other findings, like the existing test reports. In such cases compensative protection methods may be used in addition to secure configuration. In secure configuration and as compensative protection methods such measures like enhanced detection capability, systems hardening, run-time limitations for software code (e.g. AppLocker, SELinux, AppArmor), application firewalls (WAF) and logical separation of the entire program through, e.g. virtualization.

In order to ensure the security of software it is essential to take advantage of instructions and standards dealing with the issue. These include, e.g.,
VAHTI Software Development Security Guide (VAHTI 1/2013), OWASP Application Security Verification Standard (ASVS) and the instruction of National Cyber Security Centre "Instruction for Secure R&D; on the way to approval".

Examples of implementation:

1. Purposes for software (applications, services, systems) and roles possibly carrying out security of software have been identified.
2. Security needs for software (applications, services, systems) have been assessed, paying special attention to the purpose for the use of software and how it potentially puts security into practice, on the potential attack surface and on the nature and classification level of the information processed.
3. Dependencies and interfaces of software (applications, services and systems) have been detected. Dependencies and interfaces have been a target for the same requirements as for the software, bearing in mind e.g. the used libraries, interfaces (APIs) and device engagements. Requirements cover both server and client parts.
4. Critical software (applications, services, systems) are implemented or the implementation is verified against a reliable standard or/and using the instruction for secure programming, if possible.
5. It has been ensured that the software code quality maintenance, development and change control of the software (applications, services and systems) match with the need for the entire life cycle.
6. It has been ensured that software (applications, services, systems) fulfil the requirements derived from legislation. Special attention has to be payed to complexes dealing with crypto (I-12), management connections (I-04), user management and identification (I-06, I-07), systems hardening (I-08) and traceability (logging, I-10).

Other sources of information: CIS Critical Security Controls (v7.1) / 2; CIS Critical Security Controls (v7.1) / 18; BSI IT-Grundschutz-Compendium Edition 2019; CPNI - Development and Implementation of Secure Web Applications; OWASP Application Security Verification Standard Project (ASVS); CWE TOP 25 Most Dangerous Software Errors; The Building Security In Maturity Model; Software Assurance Maturity Model; SFS-EN ISO/IEC 27002:2017 14.1.1, 14.1.2, 14.1.3, 14.2.8, 14.2.9; VAHTI 1/2013; NCSC Instruction for Secure R&D; on the way to approval; PiTuKri MH-02

I-14 DEFENCE-IN-DEPTH – ELECTROMAGNETIC EMANATIONS (TEMPEST) AND ELECTRONIC INTELLIGENCE

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/EU)
1. Security measures shall be implemented to protect information-processing environment handling Classified Information against compromise of such information through unintentional electromagnetic emanations (TEMPEST security measures). **2. When handling information classified to Levels III (CONFIDENTIAL) or II (SECRET) the risks of electronic intelligence have to be mitigated sufficiently.** **3. Such security measures shall be commensurate with the risk of exploitation and the level of classification of the information.**	1. 1101/2019: section 11 2. 1101/2019: section 11 3. 1101/2019: section 11	1. Art.10 (5) 2. Art.10 (5) 3. Art.10 (5)

Additional Information

In general: On classification level IV (RESTRICTED) there are no defined TEMPEST requirements for the information-processing environment. On classification levels III and II the electromagnetic radiation which exceeds the set limits will be controlled using the respective protection methods approved by the competent security authority.
In cases where international Classified Information is concerned, the National TEMPEST Authority (NTA) is the NCSA of Finnish Transport and Communications Agency. On classification level III (CONFIDENTIAL) compensative protection measures may be more widely approved.

The adequacy of counter measures may be verified by facility zoning measurement or by shielded enclosure measurement.

Other sources of information: Sähkömagneettisen hajasäteilyn aiheuttamien tietoturvariskien ehkäisyn periaatteet (in Finnish only); BSI IT-Grundschutz-Compendium Edition 2019; SFS-EN ISO/ IEC 27002:2017 11.2.3

Operations Security

I-15 EXCHANGE OF CLASSIFIED INFORMATION BETWEEN PHYSICALLY PROTECTED AREAS - ELECTRONIC TRANSFER OF THE INFORMATION

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/EU)
1. When Classified Information is transferred outside physically protected areas, the information or the traffic is encrypted with a method approved by the competent authority to the respective classification level. In addition to this, the information transfer procedure has to include the identification and authentication of the recipient in a sufficiently secure way before the recipient is getting access to the transferred Classified Information. **2. When transmission of Classified Information is confined within physically protected areas, unencrypted transmission or encryption at a lower level may be used, based on the outcome of a risk management process and subject to the approval of the competent authority.**	1. 1101/2019 sections 12 and 11(7), and 906/2019 section 14 2. 1101/2019 sections 12 and 11(7), and 906/2019 section 14	1. Art. 9 (4) 2. Annex IV (31)

Additional Information

In general: Electronic transfer of Classified Information includes numerous risks. The mitigation of risks to an acceptable level requires some notifications concerning the personnel, as well as the technological implementation. In situations where it is necessary to transfer Classified Information between two organisations through a public network, secure transfer requires secure encryption solutions, key management and trained personnel. In situations when the use of a crypto solution requires action from the personnel (e.g. transfer of a document belonging to classification level IV (RESTRICTED) to another organisation as an attachment to email), special attention has to be paid for security of the procedure through training. Technically secure crypto solution does not provide the protection needed in situations, where management of keys is inadequate or when the personnel is not following the secure principles for the usage of the crypto solution.

Sufficiently reliable recipient identification and authentication is largely depending on the crypto solution used. Finnish NCSC operative policies for approved crypto solutions take often stands on the identification and authentication of recipients in cases when the crypto solution is used for communicating to a person working on another organisation. On the other hand, in many crypto solutions the identification and authentication of the recipient relies on the reliability of the key management (e.g. encryption based on a shared secret, between facilities of the organisation or between networks (LAN-2-LAN) of two organisations or a file encryption based on a shared secret). Secure encryption solutions and key management procedures are handled more in detail in 1-12.

I-15 EXCHANGE OF CLASSIFIED INFORMATION BETWEEN PHYSICALLY PROTECTED AREAS - ELECTRONIC TRANSFER OF THE INFORMATION

Internet, as well as the MPLS networks offered by operators and e.g. so called dark fibers are considered as public networks. This requirement covers telephones, facsimiles, email, instant messaging and other similar network based transfer methods. Protection principles for the storage media (hard drives, USB-memories etc.) containing Classified Information are described on requirement I-18.

The use of radio-interface on wireless network connections (e.g. WLAN, 3-5G, Bluetooth) is understood as a dismissal from the physically protected area. This means that the radio-interface of wireless networks should be handled in a similar manner as a public network. See I-05.

Example of implementation: on processing environments belonging to national classification levels IV-II, the requirement can be fulfilled by putting into force the following:

1. When transferring Classified Information through a network outside physically protected areas approved for the level, the role of encryption has to be taken into account as a focal protection element (see I-01, I-12 and I-18).
   a) Personnel have tools and methods to protect Classified Information with a crypto solution approved by a competent authority.
   b) Ability of the personnel to use a crypto solution approved by a competent authority has been verified (e.g. instructions, training and control).
2. In situations, where Classified Information is transferred within physically protected areas,
   a) traffic channel of respective security level has been physically protected (e.g. cabling which stays inside a physically protected area, perhaps within a single room, approved for the respective classification level) or
   b) information is encrypted with a lower level encryption product, based on a separate approval by the competent authority (e.g. HTTPS in the traffic within the network for the respective classification level).

Other sources of information: CIS Critical Security Controls (v7.1) / 13; CIS Critical Security Controls (v7.1) / 14; BSI IT-Grundschutz-Compendium Edition 2019; FI NSA Instruction for the handling of international classified information; SFS-EN ISO/IEC 27002:2017 10.1.1, 13.2.1, 13.2.3; PiTuKri JT-05; PiTuKri SA-02; PiTuKri SA-03

I-16 SECURITY THROUGHOUT THE INFORMATION PROCESSING ENVIRONMENT LIFE CYCLE - CHANGE MANAGEMENT

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/EU)
1. Ensuring security shall be a requirement throughout the information-processing environment life cycle, from initiation to withdrawal from service. **2. Security assessments, inspections and reviews shall be performed periodically during the operation and maintenance of an information-processing environment and when exceptional circumstances arise.** **3. Security documentation for an information-processing environment shall evolve over its life cycle as an integral part of the process of change and configuration management.**	906/2019 sections 13 and15	1. Annex IV (8) 2. Annex IV (11 and 16) 3. Annex IV (12)

Additional Information

In general: Reliable management of information security and changes in the information-processing environment requires that the technical structure and, e.g., all devices and programs belonging to it are known. Changes in settings and functions have to be monitored and they must lead into the verification of their justification (see also I-03). When inventory is up-to-date, the needed changes can be focused precisely throughout the life cycle, changes are easier to predict and the security monitoring of the environment is possible. Inventory procedure may take good use of, e.g. network diagrams, device and software component listings and configuration data bases.

It has to be possible to be confirmed about the information security of the information-processing environment throughout the life cycle. This requires constant monitoring for the need of changes and also a procedure for regular changes. Needs for changes may be resulted from, e.g., end of the life cycle of information-processing systems or the incapability of current protection structures to meet challenges in new attack methods. For example software updates may cause unexpected consequences, like changes in security settings and in user rights or introduction of new, insecure services into the information-processing environment. Harmful consequences may be prevented e.g. by comprehensive testing and monitoring of change logs (typically e.g. changelog, readme). Harmful consequences may be possible to observe, e.g., by examining configurations after updates (installed to test environment) and, among other means, by automated scanning and configuration comparisons.

In the protection of the system against connection of unauthorised devices, the following means may be used:
a) Placing of devices on a security rack which is sealed and/or equipped with alarm,
b) Use of devices which have been protected against tampering, or
c) Use of some other respective method (e.g. sealing of devices). When using the sealing method, inspection of the seals should be a regular process.

I-16 SECURITY THROUGHOUT THE INFORMATION PROCESSING ENVIRONMENT LIFE CYCLE - CHANGE MANAGEMENT

Inspection interval, which can be accepted for verifying unauthorised modifications or devices, depends on procedures implemented to limit and to supervise the access to the target (system, physical area). In most of the environments a yearly or biannual inspection might be sufficient.

Also instructions to personnel (T-04) and their training (T-12) need to be taken into account in the procedure for protecting the system against connection of unauthorised devices. One has to pay attention to the fact that only such peripherals (e.g. display, keyboard and mouse) and media (e.g. USB memory approved only for the environment at stake) may be connected to terminal devices, which have been approved to be used in the respective information-processing environment. Especially in situations where the terminal device is used in the physical area belonging to lower classification level (se I-17and I-18), it is normally not possible to use peripherals or media stored in the above mentioned space. See also I-05.

Examples of implementation: on processing environments belonging to national classification levels IV-III, the requirement can be fulfilled by putting into force the following:

1. Up-to-date inventory can be found concerning the configuration of the information-processing environment. The term inventory refers to hardware and software inventory and to information about configurations and procedures which have influence to security aspects.
2. Changes having effect on information processing should be handled through a change management process. Changes should be traceable.
3. Methods have been put in place to ensure the continuance of the security level after changes.
4. Inventory is kept on a level, which makes it possible to determine hardware and software and their versions (device, operating system and applications) used in the information-processing environment, and which supports the vulnerability management (see I-19).
5. Information-processing environments are monitored in order to detect unauthorised changes or devices. The inventory of the information-processing environment is kept up-to-date throughout the life cycle.
6. Classification and protection needs for the material (documents, inventory in electronic form etc.) dealing with the implementation of the information-processing environment are defined.

On processing environments belonging to national classification level II, the requirement can be fulfilled by putting into force the following in addition to points 1-6 above:

7. Systems are protected against the connection of unauthorised devices (key loggers, wireless transmitters incl. mobile devices etc.)

Other sources of information: CIS Critical Security Controls (v7.1) / 1; CIS Critical Security Controls (v7.1) / 2; BSI IT-Grundschutz-Compendium Edition 2019; FI NSA Instruction for the handling of international classified information; SFS-EN ISO/IEC 27002:2017 8.1.1, 12.1.1, 12.1.2, 12.5.1, 14.2.2, 14.2.8, 14.2.9, 18.2.3; Recommendation of Information Management Board (2020:21, chapter 5); PiTuKri MH-01

I-17 HANDLING OF CLASSIFIED INFORMATION WITHIN PHYSICALLY PROTECTED AREAS - PHYSICAL SECURITY

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/EU)
Classification level IV (RESTRICTED)		
1. Classified Information has to be handled in Security Areas and outside of them in a way, which prevents unauthorised access to Classified Information (see F-04 and I-18).	1. 1101/2019 section 10	1. Art.8 (3)
2. Handling of information is possible inside the perimeter of a Security Area approved by a competent authority (see F-04) and outside Security Areas when procedures approved by competent authority are used (see I-18).	2. 1101/2019 section 10	2. Annex II (23), art. 8 (3)
3. Storage of information is possible inside the perimeter of a Security Area approved by a competent authority (see F-04) and outside Security Areas when procedures approved by competent authority are used (see I-18).	3. 1101/2019 section 10	3. Annex II (24), art. 8 (3), art. 9 (4)
4. Data pools containing information belonging to classification level IV (RESTRICTED) and information systems used to process this information have to be placed inside the perimeter of a Security Area approved by a competent authority (see F-04).	4. 1101/2019 section 10	4. Annex II (24)
Classification levels III (CONFIDENTIAL) and II (SECRET): in addition to points 1 and 2 above:		
5. Storage of information is possible inside the perimeter of a Secured Area approved by a competent authority (see F-04). Note exceptions valid only for national information in point 6 and for remote use in I-18.	5. 1101/2019 section 10	5. Annex II (22 and 26), art.8 (4)
6. Only for national classification level III information, the storage of information in electronic format is possible outside the perimeter of a Secured Area using a terminal device approved for the respective level and taking into account that a) information has been protected using an encryption solution approved for the respective classification level by a competent authority (see I-12), and b) information security of the terminal device has been taken care of, paying special attention to the sufficient confidentiality and integrity using a method approved by a competent authority (see F-04). Note remote working in I-18.	6. 1101/2019 section 10	6. –

Additional Information

In general: Requirements for Administrative Area, Secured Areas and e.g. safes have been described in subdivision F of KATAKRI (see F-02, F-03 and F-04). On the other hand, the subdivision I describe the relation of electronic handling of information inside Security Areas, following the requirements set in subdivision F, and also outside of them in remote working conditions (see I-18).

In situations where Classified Information belonging to levels III or II is temporarily used in the area which is of one level lower, protection against electromagnetic emanations (see I-14) should be taken into account according to the classification of the information. In the implementation it is worth noticing procedures while working pauses (e.g. taking the piece of information into the safe within a Secured Area), preventing visibility to the working space (e.g. covering windows) and limiting the access to the area only for those approved. In the handling of NATO Classified Information one has to bear in mind that protection principles partly differ from those used to protect national or EU Classified Information.

I-17 HANDLING OF CLASSIFIED INFORMATION WITHIN PHYSICALLY PROTECTED AREAS - PHYSICAL SECURITY

Electronic handling inside an Administrative Area: Information processing system or communication arrangement has to be protected according to the respective classification level. For example terminal device, which has been protected following the requirements set for classification level III (CONFIDENTIAL), may be taken to the Administrative Area or outside it, from where the terminal device establishes an encrypted connection approved for classification level III (CONFIDENTIAL) to the data pool located inside a Secured Area in order to process information. Terminal device cannot be left unattended to the Administrative Area; it has to be returned to Secured Area for storage, unless it is possible to guarantee the confidentiality, integrity and availability of the terminal device in some other way (F-04). Fixed network for classification levels III or II cannot be stretched to an Administrative Area.

Handling and storage of national information on classification levels IV or III in a terminal device: In situations, where information belonging to national classification levels IV or III is handled and stored in a terminal device outside Security Areas or information belonging to national classification level III in an Administrative Area, information in terminal devices has to be protected with an encryption solution approved for the respective level by a competent authority (see I-12). It is especially important to take care of integrity of the terminal device for the respective level using a method approved by a competent authority (see F-04).

Integrity of a terminal device has to be maintained on a sufficient level in order to guarantee that the confidentiality of the information is not put in danger as a result of a loss of the integrity of the terminal device. The most typical way to ensure the integrity of the information system is to protect it by means of physical access control to Security Areas, including e.g. all physical servers, network devices, terminal devices and cablings of the information system. For example, when protecting the integrity of an information system in classification level IV against general risks for Classified Information, it may be sufficient to place data pools of the information system to Administrative Area or to Secured Area. When terminal devices are equipped with sufficient encryption capability, also a limited storage in a locked space, e.g. at home of the official may be possible.

Information systems belonging to classification level III should be placed in total to a Secured Area. In case terminal device handling level III Classified Information has to be stored in an Administrative Area (see F-04) or even outside Security Areas, the lack of integrity protection offered by physical access control may be compensated on risk assessment basis, e.g., by placing the terminal device inside a housing or package which reveals unauthorized access. For example so called security briefcases are available and will detect unauthorized attempts to access by informing the owner or the using organisation of the access attempts, or/and will indicate the unauthorized access by a mark in the housing or package.

In the risk assessment it is vital to bear in mind that the threat against Classified Information and terminal devices used to handle information outside Security Areas may be hard or even impossible to mitigate enough, especially from level III on. In the handling of Classified Information also unauthorized visual observation and eavesdropping have to be taken into account when choosing protection measures. This same applies - based on risk assessment - to the protection against effects of electromagnetic emanations. When storing terminal devices handling level III information also international information security requirements have to be taken into account. In them the storage outside Secured Areas may be completely forbidden.

Other sources of information: BSI IT-Grundschutz-Compendium Edition 2019; CPNI Security Advice Physical Security; SFS-EN ISO/IEC 27002:2017 11.1.1, 11.1.3, 11.1.5, 11.2.1; Recommendation of Information Management Board (2020:19, chapter 5); PiTuKri FT-02

I-18 HANDLING AND TRANSFER OF CLASSIFIED INFORMATION BETWEEN PHYSICALLY PROTECTED AREAS - REMOTE USE AND REMOTE MANAGEMENT

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/EU)
Classification level IV (RESTRICTED) 1. Users and terminal devices are identified and authenticated sufficiently reliably. Transferring and handling of Classified Information between Security Areas (see F-04) is possible only by using compensative arrangements approved by competent authorities. 2. Classified Information has to be handled outside Security Areas in a way where unauthorised access to Classified Information is prevented. Personnel has been trained and instructed on secure remote use and management. 3. Unless the classification level IV (RESTRICTED) Classified Information stored on electronic media (hard drives, USB-sticks etc.) has been encrypted using a method approved by competent authority, storage media has to stay under constant supervision. 4. Remote use or management requires that the traffic will be encrypted by using a crypto solution approved by a competent authority to the respective classification level. 5. Information stored inside the terminal device has to be protected with an encryption solution, which is secure enough for the respective classification level and approved by a competent authority. Integrity of the terminal device has to be taken care of on an appropriate level. **Classification levels III and II:** in addition to the points 1 to 5 above 6. Classified Information may not be decrypted or read while travelling or on public place. 7. Remote use or management of systems is limited to Security Areas approved by competent authorities (see F-04). Note: exception valid only for national information in point 8: 8. Only for national information classified on level III, remote use (handling) and storage is possible outside Security Areas with a terminal device dedicated for the respective level, by taking into account that a) information has been encrypted with a crypto solution approved by a competent authority to the respective level and b) information security aspects concerning the terminal device have been taken care of, bearing especially in mind that the sufficient confidentiality and integrity have been ensured with a method approved by a competent authority.	1. 1101/2019 section 11(5) 2. 906/2019 section 4 3. 1101/2019 sections 10 and 13 4. 1101/2019 sections 12 and 11(7), and 906/2019 section 14 5. 1101/2019 sections 10, 11 and 12 6. 1101/2019 section 13 7. 1101/2019 section 10 (CL II) 8. 1101/2019 section 10 (CL III)	1. Art. 8(3), art. 9(4) 2. Annex IV (22) 3. Art. 9(4), annex III (28, 30 and 33) 4. Art. 10(6) 5. Art. 1(2) 6. Art. 9(4), annex III (28, 30 and 33) 7. Annex II (25–26), art.8(4) 8. –

I-18 HANDLING AND TRANSFER OF CLASSIFIED INFORMATION BETWEEN PHYSICALLY PROTECTED AREAS - REMOTE USE AND REMOTE MANAGEMENT

Additional Information

In general: Remote use and management usually means that information processing systems are used or managed outside the office facilities of the organisation with a terminal device dedicated for the use. In most of the cases the terminal device used is a laptop computer, assigned to this use by the organisation. Remote use and management of Classified Information is nominally suitable only for classification level IV (RESTRICTED).

From classification level III (CONFIDENTIAL) the handling of Classified Information requires a physically protected Security Area, approved by a competent authority for this particular use. In special cases this requirement may be compensated by the use of additional physical security measures (e.g. in an operational work carried out by authorities). An exception to this rule is the remote use and storage of only national information classified on level III with a terminal device approved for this level (see I-17, field Additional Information "Handling and storage of national information on classification levels IV or III in a terminal device"). The remote management of both national and international classification level III (CONFIDENTIAL) information-processing environments shall be limited to Security Areas approved by a competent authority.

Compensative arrangements on the requirement 1 include on classification level IV (RESTRICTED) the following:
a. remote use or management of systems requires a strong authentication based on at least two factors
b. only devices and remote connections approved by competent authorities for this particular environment are used.

On classification levels III and II the use of technical binding to approved remote terminals (device authentication) is required as an additional compensative control.

When training and instructing the personnel special attention has to be paid on the safeguarding of the Classified Information from unauthorised people. This includes e.g. how to choose correct handling places and what kind of limitations can be foreseen for the handling (unauthorized visual observation and eavesdropping), how to protect terminal devices and other working material from thefts and tampering (storage only in a locked space and memory area encryption activated and, e.g., usage of housings and packages (see Additional Information field in I-17) and other methods for secure usage of terminal devices and working material involved.

Protection of management connections is one of the most critical factors in the security of information processing systems (see I-04). However, especially systems belonging to classification level IV (RESTRICTED) may be considered as subject to remote management. In cases where remote management is considered to be justified, the security measures are recommended to be stricter than in the pure remote use of the system. For instance, remote management connections for classification level IV (RESTRICTED) may be limited to dedicated physical and logical locations.

Other sources of information: CPNI - Personnel Security in Remote Working; CPNI - Configuring and managing Remote Access for Industrial Control Systems; BSI IT-Grundschutz-Compendium Edition 2019; CPNI - Security Advice - Physical Security; SFS-EN ISO/IEC 27002:2017 6.2.1, 6.2.2, 7.2.2, 8.3.1, 8.3.3, 11.1.1, 11.1.3, 11.1.5, 11.2.1, 11.2.3, 11.2.5, 11.2.6, 12.1.1; PiTuKri IP-03; PiTuKri JT-05; PiTuKri SA-02

I-19 SECURITY THROUGHOUT THE INFORMATION PROCESSING ENVIRONMENT LIFECYCLE - MANAGEMENT OF SOFTWARE VULNERABILITIES

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/EU)
Reliable arrangements are established for the entire life cycle of the information processing environment to manage software vulnerabilities.	906/2019 section 13	Annex IV (8,11 and 16)

Additional Information

In general: Many types of attacks exploit software failures, or vulnerabilities, to some extent. Vulnerable source code is embedded into operation systems software, server applications, end-user applications, as well as in firmware applications and drivers, in BIOS and in separated management connections (e.g. iLo, iDrac). In addition to errors in the software, configuration errors and outdated practices - like outdated encryption algorithms - create vulnerabilities. Responsible suppliers fix vulnerabilities found in their software products. Risks can be reduced by installing patches. On the implementation of vulnerability management measures, the up-to-dateness and security of vulnerability scanners, CMDB and other systems has to be taken care of.

Precise situation picture should be one of the goals for vulnerability management, involving continuous monitoring and development of the system environment. As one part of maintaining the situation picture, risks deriving from vulnerabilities and detected deficiencies should be assessed in comparison to the processing environment in order to set corrective actions on par with assessed criticalities. Corrective actions may include vulnerability patches from suppliers, software updates and configuration changes aiming at limiting or removing the risk. In addition to this, it is important to follow supplier support for software versions. Updates are not necessarily actively received to outdated software, which makes it sometimes impossible to fix software vulnerabilities. Effective and process driven management of vulnerabilities requires an organised procedure with set responsibilities, and typically also cooperation between internal and external counterparts.

Management of software vulnerabilities may be implemented by

1. information updates from CERT-community and from suppliers are subscribed as e-mail. From these updates such information is picked up, which has impact to the security of the systems of the organisation. For picking up, up-to-date inventory is put in place for the software for its versions (see system inventory in I-16). The integrity of software downloads and updates (checksums, malware detection) is tested before delivering them to the production environment. Effects of updates should be tested before installing them to the production environment. Testing can be done in an isolated test environment or by a small user group.
2. Successful installation of updates is monitored on a regular basis, at least monthly. For monitoring, e.g. centralized patch management processes may be used.
3. The network and its services, servers and workstations connected to the network, as well as laptops, printers, mobile devices and other devices are inspected (vulnerability scan, CMDB etc.) regularly and after every significant change or modification in order to detect such objects in the update process which need to be fixed.

I-19 SECURITY THROUGHOUT THE INFORMATION PROCESSING ENVIRONMENT LIFECYCLE - MANAGEMENT OF SOFTWARE VULNERABILITIES

4. Inventory of software and hardware (see I-16), as well as the security and up-to-dateness of scanning application have been taken care of. Especially scanning applications may require extensive access rights to different parts of the information-processing environment in order to produce reliable findings. This has to be taken into consideration in the protection of scanning software (access rights, traceability).
5. Handling of detected vulnerabilities and deficiencies in updates are managed by following a procedure, where weak spots clearly effecting on the protection of the information-processing environment are removed, mended or otherwise limited to ensure that handling of Classified Information will not unnecessarily be endangered. When estimating the gravity of vulnerabilities, e.g. CVE classification may be used, by proportioning it to the protections in use in the information-processing environment for preventing, limiting and detecting the use of vulnerabilities.

Example of implementation: on processing environments belonging to classification level IV (RESTRICTED), the requirement can be fulfilled by putting into force a vulnerability management process, which includes at least the followin:

1. Security bulletins of the authorities, equipment manufacturers, software suppliers and other similar parties are followed, in order to estimate the need of security updates. Updates are installed in a controlled manner.
2. Successful installation of updates is monitored on a regular basis, at least monthly.
3. The network and its services, servers and workstations connected to the network, as well as laptops, printers, mobile and other devices are inspected (vulnerability scan, CMDB etc.) at least annually and after every significant change or modification, in order to detect such objects in the update process which need to be fixed.
4. Inventory of software and hardware (incl. CMDB), as well as the security and up-to-dateness of scanning software have been taken care of.
5. Handling of detected vulnerabilities and deficiencies in updates are managed by following a procedure, where weak spots clearly effecting on the protection of the information-processing environment are removed, mended or otherwise limited to ensure that handling of Classified Information will not unnecessarily be endangered.

On processing environments belonging to national classification levels III and II, the requirement can be fulfilled by putting into force the following in addition to points 1, 2, 4 and 5 above:

6. The network and its services, servers and workstations connected to the network, as well as laptops, printers, mobile and other devices are inspected (vulnerability scan, CMDB etc.) at least twice a year and after every significant change or modification in order to detect such objects in the update process which need to be fixed.

Significant change refers here to, e.g, changes in network topology, introduction of new systems and/or service pack level updates to the existing ones, notable changes in filtering rules of firewalls and respective elements, etc.

Other sources of information: CIS Critical Security Controls (v7.1) / 3; BSI IT-Grundschutz-Compendium Edition 2019; SFS-EN ISO/IEC 27002:2017 12.6.1; Recommendation of Information Management Board (2020:21, chapter 5); PiTuKri KT-04

I-20 SECURITY THROUGHOUT THE INFORMATION PROCESSING ENVIRONMENT LIFECYCLE - BACKUP COPIES

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/EU)
Backup copies containing Classified Information are kept under protection throughout their life cycle, using protection measures of at least equal level as what is used for safeguarding the original information.	906/2019 sections 13 and 15, 1101/2019 sections 7,11 and 14	Annex III (18 and 27), annex IV (8 and 16)

Additional Information

In general: It is recommended that backup copying is always done according to the operational requirements. Backup copying that is considered adequate for the operational requirements takes into account at least the following:

1. Backup frequency is adequate considering the criticality of the data being backed up. Requires determining how much data may be lost (recovery point objective, RPO).
2. The speed of the recovery process is adequate for the operational requirements. Requires determining how long recovery may take (recovery time objective, RTO).
3. Correct functioning of the backup and recovery process is regularly ensured through testing.
4. The documentation of the recovery process is on an adequate level.
5. The physical location where backups are stored, is separated from the actual system (in a separate sag/fire space, sufficient distance between backups and the system room, etc.). Note: backup copies should be protected with physical and logical access control methods following at least the requirements set for the respective classification level (taking into account the possible aggregate effect).
6. When the same backup system is used for handling information belonging to different owners, separation methods (see I-06) have to be implemented in backup system interfaces and in storage media (e.g. dedicated and encrypted backup tapes which are stored in separate safes or closets) to enable utilization of inspection rights.

Example of implementation: on processing environments belonging to classification level IV (RESTRICTED), the requirement can be fulfilled by putting into force the following:

1. Backup copies are handled and stored throughout their life cycle on systems, which fulfil at least requirements set for the classification level.
2. When the same backup system is used for handling information belonging for different owners, who reserve the inspection rights (see I-06) to the handling of their particular information, separation methods making this possible in backup system interfaces and storage media have to be implemented following the requirements set for the classification level.
3. In case there is a need to transfer backup copies outside the physically protected security area of the particular classification level, procedures described in I-15 (electronic transfer) and/or in F-08.1 (mail/courier) and I-18 (transfer outside physically protected security area) have to be taken into account.
4. Backup media are destroyed according to the requirements set for the particular classification level (I-21).
5. Recovery of the system and information is regularly, e.g., automatically tested, in order to be able to recover information in right status and thus ensure the integrity.
6. On processing environments belonging to national classification levels III and II, the requirement can be fulfilled by putting into force the following in addition to points 1 to 5 above: Registers of backup copies are maintained and the handling of backups is documented on electronic log, on information system, on document management system, or on manual diary or document (see F-08.3).

Other sources of information: CIS Critical Security Controls (v7.1) / 10; BSI IT-Grundschutz-Compendium Edition 2019; SFS-EN ISO/IEC 27002:2017 12.3.1; Tiedonhallintalautakunnan suositus (2020:21, luku 5); PiTuKri KT-03

I-21 SECURITY THROUGHOUT THE INFORMATION PROCESSING ENVIRONMENT LIFECYCLE – DISPOSAL OF CLASSIFIED INFORMATION IN ELECTRONIC FORMAT

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/EU)
Classification level IV (RESTRICTED) 1. **Classified material that is in the electronic format is destroyed securely. The destruction is carried out with methods which are secure enough to prevent reconstruction in whole or in part of destroyed information. Concerning non-electronic information, see F-08.4.** Classification level III (CONFIDENTIAL): in addition to point 1 2. **When international CONFIDENTIAL information is concerned, a destruction certificate has to be signed by the registrar and stored in the registry. Registry information has to be updated accordingly. The destruction certificates will be stored in the registry for at least five years. (see F-08.3).** Classification level II (SECRET): in addition to points 1 and 2 above 3. **In case the originator of the information is another authority, the authority destructing information shall inform the originator about the destruction, unless the information is returned to the originating authority.** 4. **Information may be only destructed by a person who has been nominated for the task by an authority. Draft documents may be destroyed by the originator.** 5. **International information belonging to classification level SECRET has to be destroyed in the presence of a witness. The witness has to be security cleared at least to the level the information to be destroyed.**	1. 906/2019 section 21, 1101/2019 section 15 2. – 3. 1101/2019 section 15 4. 1101/2019 section 15 5. –	1. Annex II (8), annex III (46), annex IV (8) and (37,38) 2. Annex III (43 and 45) 3. – 4. – 5. Annex III (44).

In general: Technological development is effecting also to the reliable destruction of information. For example, the ever increasing calculation capacity makes it easier to reassemble shredded paper format information by technical means. On the other hand, destruction of electronic storage media (hard drives, USB sticks and others) in a reliable manner may more often require the use of melting instead of shredding.

Information needs to be protected until the end of its life cycle. This is important to be kept in mind especially in situations where third party services are used for the destruction of the information, like melting hard drives. The practical way to handle this requirement is to use a method, where the organisation responsible for the information will observe the destruction process until the end of the life cycle of the information.

The role of personnel has to be taken into account in the destruction process. The organisation is responsible for arranging a simple and solid way to destroy Classified Information. This may, in practice, mean the possibility to use appropriate paper shredders and also the security training of the personnel (see T-12).

Additional Information

Destruction using a shredder: On classification level IV (RESTRICTED) the material may be shredded following, for instance, requirements below

- the remaining magnetic hard disk particles are not larger than 320 mm2 (DIN 66399 / H-5),
- the remaining SSD-disk or USB-memory particles are not larger than 10 mm2 (DIN 66399 / E-5), and
- the remaining optical media particles are not larger than 10 mm2 (DIN 66399 / O-5).

On classification level III (CONFIDENTIAL) the material may be shredded following, for instance, requirements below:

- the remaining magnetic hard disk particles are not larger than 10 mm2 (DIN 66399 / H-6),
- the remaining SSD-disk or USB-memory particles are not larger than 10 mm2 (DIN 66399 / E-5), and
- the remaining optical media particles are not larger than 5 mm2 (DIN 66399 / O-6).

On classification level II (SECRET) the material may be shredded following, for instance, requirements below:

- the remaining magnetic hard disk particles are not larger than 10 mm2 (DIN 66399 / H-6),
- the remaining SSD-disk or USB-memory particles are not larger than 1 mm2 (DIN 66399 / E-6), and
- the remaining optical media particles are not larger than 5 mm2 (DIN 66399 / O-6).

When using particle sizes described above the remaining waste may be disposed in a similar manner as the normal office waste. This means, for instance, that particles resulting from the destruction of optical media when using DIN 66399 / O-6 shredders for level III (CONFIDENTIAL) material there is no need to use, e.g., a controlled melting process.

Destruction using combined methods: Destruction may be done instead or in addition to shredding by using various other methods, which are secure enough to prevent the reconstruction of destroyed information (like melting shredded hard disks). Encrypting the data in different parts of its life cycle also mitigates the risks. Destruction of electronic media has been covered more in detail in NCSC instructions (www.ncsa.fi > Asiakirjat > Ylikirjoitusohje; in Finnish only).

Details to be taken into account on the destruction of electronic media: Reliable destruction of electronic material should cover all devices which have been used to store Classified Information at some part of their life cycle. One has to make it sure that individual components of devices (hard drives, memory components, memory cards etc.) containing Classified Information are 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 competent authorities) 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, the service should be carried out under supervision in order to ensure that classified information is not disclosed during the service.

Additional information concerning the documentation of the destruction procedure can be found at F-08.3 (registering).

Other sources of information: NCSC overwriting instruction "Kyberturvallisuuskeskuksen ylikirjoitusohje" in Finnish only; Secure destruction of sensitive items CPNI standard 2014; BSI IT-Grundschutz-Compendium Edition 2019; SFS-EN ISO/IEC 27002:2017 8.3.2, 11.2.4, 11.2.7; Recommendation of Information Managent Board (2020:21, chapter 4); PiTuKri SI-02

ANNEX I: Facility Security Clearance

Using Katakri in the Facility Security Clearance procedure

Finnish national procedure for Facility Security Clearances has been set at the Act on Security Clearances (726/2014). Using the Facility Security Clearance (FSC) procedure the competent authority is able to assess the capability of the company for taking care of given security responsibilities. This is achieved through the use of information sources listed in the Act, through vettings of personnel and through audits of security management and premises of the company. Security arrangements, which are audited, are among others the safeguarding procedure of Classified Information, physical access control mechanisms and the security training of the personnel. Katakri can be used as a tool on the above mentioned assessment process.

The assessment process for the Facility Security Clearance can be seen in figure 1. This process scheme describes the tasks of the assessing security authority and the ones of the company at different stages of the assessment process. The process includes an audit to company's information systems in cases where this particular audit is part of the Facility Security Clearance process.

It is possible to carry out the Facility Security Clearance procedure partially. In case there is an indication on the FSC application that the company should be capable to safeguard Classified Information of authorities within the premises of the company (”FSC without safeguards”), subdivision T for Security Management and subdivision F for Physical Security of Katakri may be used. In case there is an indication on the FSC application that the company should be able to handle Classified Information belonging to authorities in communication and information systems of the company (”FSC with safeguards including CIS”), assessment will be done using – in addition to the previous subdivisions - the Information Assurance subdivision I. Evaluation of electronic handling of information as a part of the FSC procedure has been described more in detail in Annex II.

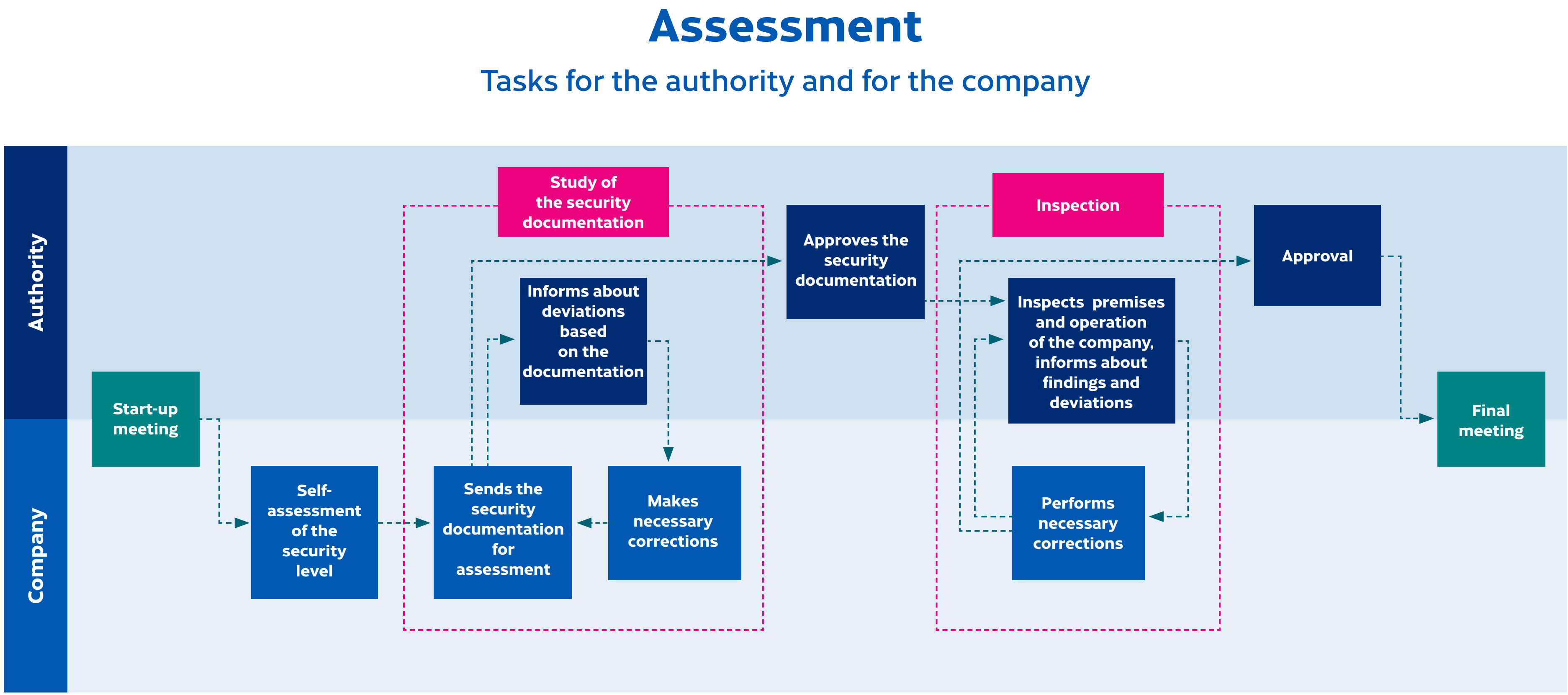

Assessment
Tasks for the authority and for the company
Authority
Company
Start-up meeting
Self-assessment of the security level
Study of the security documentation
Informs about deviations based on the documentation
Sends the security documentation for assessment
Makes necessary corrections
Approves the security documentation
Inspection
Inspects premises and operation of the company, informs about findings and deviations
Performs necessary corrections
Approval
Final meeting

Figure 1. Assessment process.

ANNEX II: Assessment of information systems

According to the Act on the Assessment of the Information Security of Public Authorities' Information Systems and Telecommunications Arrangements [5] it is possible to give the assessment task to the Finnish Transport and Communications Agency or to one of the Information Security Inspection Bodies approved by it [6]. Katakri can be used as a tool when assessing how the information system used or planned for the use of the government fulfils the national or international security requirements. Also when used to assess the government information systems

Katakri has to be used following the findings of systematic risk assessment, resulting in the selection of safeguarding requirements chosen for the particular use and in the assessment of their realisation based on given examples.

This annex describes different use cases of Katakri when inspecting information systems. The description concentrates on cases where the topic is either a FSC or an assessment of information system used (or to be used) by the government. In these cases the relevant competent authority is the Finnish Transport and Communications Agency. This description has been divided into presentations of use cases, assessment and accreditation processes and of the accreditation and certificate for conformity issuance. The description leaves out other user cases, like the use as a part of the internal security work of the organisation.

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

[6] Act on Information Security Inspection Bodies (1405/2011).

Use cases

Katakri use cases on information system inspections performed by the NCSA function of the Finnish Transport and Communications Agency can be divided in five categories:

1. Systems which are in possession of the government or are intended to be purchased, and of which the governmental authority has issued an assessment request for the Finnish Transport and Communications Agency (Act 1406/2011, Act 10/2015 [7]).
    - system assessment is based on the interest specified on the request; national interest, international interest or both, concerning the protection of Classified Information.

2. Requests of the Ministry of Finance concentrating on general information security level of information systems or Telecommunications Arrangements owned by government authorities (Act 1406/2011, Act 10/2015).
    - system assessment is based on the interest specified by the Ministry of Finance on the request; national interest, international interest or both, concerning the protection of Classified Information.

3. Systems owned by governmental authorities as long as they are part of fulfilling the international information security obligations (Act 588/2004 [8]).
    - system assessment is based on the interest concerning the protection of international Classified Information.

4. Systems owned by companies when systems are part of the assessment package, based on the request for a Facility Security Clearance and when the accreditation given by the competent NCSA authority is needed (Act 588/2004) and/or assessment of conformity (726/2014 [9]).
    - system assessment is based on the interest concerning the protection of national or international Classified Information.

5. Information systems belonging to authorities, for which the authority is seeking a certificate for conformity, issued by the Finnish Transport and Communications Agency (Act 1406/2011).
    - system assessment is based on the interest concerning the protection of national Classified Information.

Use cases of information system inspections can be combined according to the wishes expressed by the organisation ordering the assessment.

[7] Act on Security network functions of Governmental Authorities (10/2015).

[8] Act on International Information Security Obligations (588/2004).

[9] Act on Security Clearances (726/2014).

Assessment process

Assessment process for the security of information systems begins when the target of the assessment sends an assessment request to the Finnish Transport and Communications Agency (competent authority). Other phases in the assessment process are the planning of the inspections, the inspections and the reporting. An assessment process has been visualised in figure 2. An assessment process may be used, e.g., as a part of the internal security work of the target organisation, perhaps in a way where, for instance, residual risks are left completely on the responsibility of the target organisation. The assessment process has been described more in detail in the Finnish Transport and Communications Agency instruction "Information Security Inspections of NCSA – View of the ordering organisation" [10].

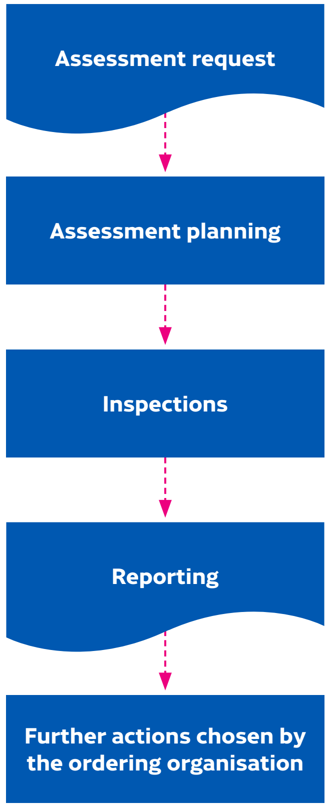


Figure 2. Simplified assessment process.

[10] NCSA 2019.

Accreditation process

Accreditation process (Act 588/2004 or Act 1406/2011), aiming at the accreditation issued by the Finnish Transport and Communications Agency begins, when the target organisation for the assessment sends an accreditation or certification request to the Finnish Transport and Communications Agency. The accreditation process is similar to the assessment process with the exception that deviated findings of the inspection have to be corrected and further verified before the accreditation or the certification can be issued. Accreditation process has been visualised in a simplified form in figure 3. Accreditation process may be used, e.g., when the target organisation wishes to proof the conformity of the protection of the information system by the accreditation or certificate issued by the Finnish Transport and Communications Agency. In the accreditation process, the risk assessment is be done using the assessments made by both the organisation itself, as well as the one of the competent authority (Finnish Transport and Communications Agency). The accreditation process is described more in detail in the NCSA instruction "Information Security Inspections of NCSA – View of the ordering organisation" (in Finnish only).

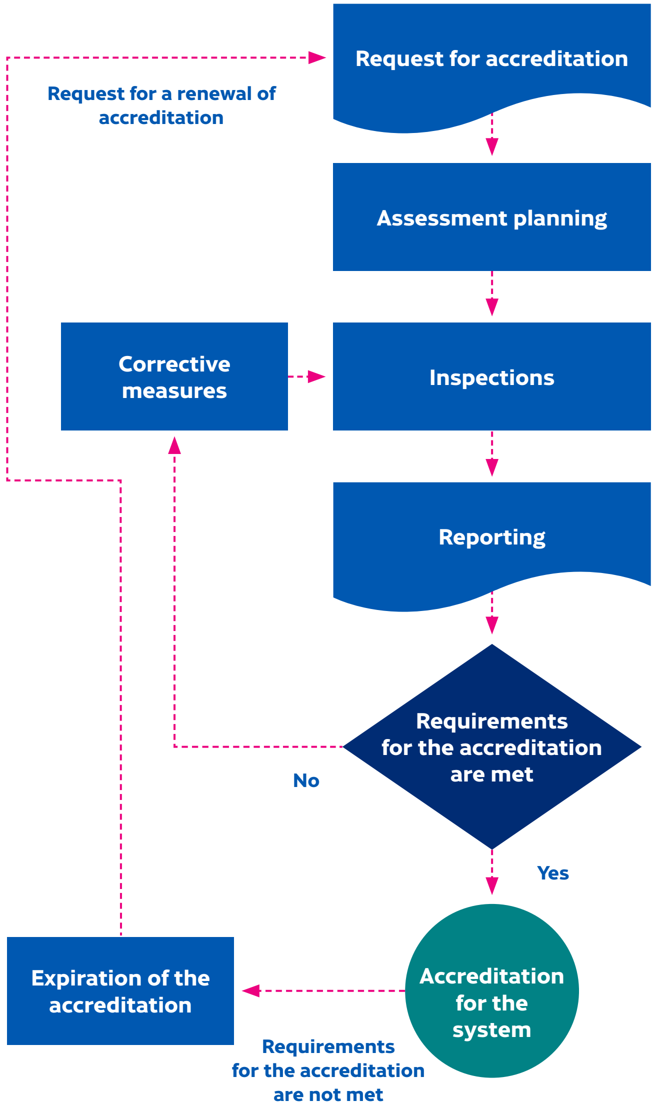

Request for accreditation
Request for a renewal of accreditation
Assessment planning
Corrective measures
Inspections
Reporting
Requirements for the accreditation are met
No
Yes
Expiration of the accreditation
Accreditation for the system
Requirements for the accreditation are not met

Figure 3. Simplified accreditation process.

Accreditation by competent authority

The Finnish Transport and Communications Agency Traficom may issue an accreditation for the system which handles national or international Classified Information and fulfils the requirements. Prerequisite for issuing the accreditation is the commitment of the target organisation to maintain the approved security level. One of the typical requirements for the accreditation is that the information system as a whole can be considered to be subject to Finnish legislation and within the competence of national authorities [11]

The validity of the accreditation will expire in case a significant change affecting the security of the inspected target will occur. Such changes could be, for instance, significant changes in the network architecture, personnel, security measures or premises. Changes resulting from normal maintenance procedures, such as software security patching, will not cause revoking of the accreditation. Conditions for revoking the accreditation will be defined at their issuance. Approvals for major changes should be requested in advance from the competent authority (Finnish Transport and Communications Agency).

The Finnish Transport and Communications Agency is able to issue an accreditation for the system which has been inspected by an approved Information Security Inspection Body (Act 1405/2011). Prerequisite for the issuance is that the target for the inspection has been confined to match with the definitions of the request for the accreditation, as well as the adequacy of the information in audit reports. The potential use of approved Information Security Inspection Bodies is limited to Finnish national classification level IV and with certain limitations also to classification level III information systems and information-processing environments. The Finnish Transport and Communications Agency may carry out additional inspections or may ask for further information from the ordering organisation in order to ensure that the target fulfils applicable information security requirements.

[11] As an exception, e.g. systems used in international cooperation between governmental authorities, when responsibility and competency roles for inspections and accreditations of system components have been settled between security authorities of participating countries.

ANNEX III: Security assessment using Katakri Security Model

The assessment of sufficient security arrangements shall be based on systematic risk assessment. By managing security risks, such a combination of security measures should be reached, where an acceptable balance between requirements, costs and residual risks is achieved. This annex describes a security model which has been a basis for Katakri, as well as the role for risk management in use cases supported by Katakri.

Katakri Security Model

Katakri security model is a hybrid model, consisting of minimum control requirements and their risk based adjustment and management in handling environments concerned. Goal for minimum control requirements is to mitigate common Classified Information related risks to an acceptable level and to also cover regulation and Classified Information owner/originator related minimum control requirements for the entire life cycle of Classified Information.

Risk-based control adjustment supports the mitigation of common Classified Information related risks, but also the mitigation of risks specific for the handling environment. Risk-based management targets at reinforcing minimum controls for risks specific in the corresponding handling environment and to adapt the controls according to changes in the risk environment.

Role of the risk management in supported use cases

Residual risks are a reality in all handling environments of Classified Information. Information owners have different risk appetites. In addition to this, risk management procedures of organisations have partly different driving factors. The goal for Katakri is not a complete streamlining of risk management procedures of different organisations, but to provide a process resulting into acceptable residual risks for Classified Information handling in the corresponding use case.

On Katakri's supported use cases aiming at approval (Act 726/2014, Act 588/2004), a two-phased risk management model is used. On the two-phased risk management the target organisation has to achieve an acceptable level of residual risks, judged by both the target organisation itself and by an external assessor. The risk management of the target organisation can mitigate environment specific risks. The role of the external assessor is to ensure general Classified Information related risks are mitigated to an acceptable level.

Assessment use of Katakri (Act 1406/2011) in supported use cases benefits from a risk management model which compares controls of the organisation to the risks assessed by an external assessor. In both supported use cases – targeting for approval or assessment – the assessment of an external assessor is based on the threat intelligence of the competent security authority. The role of risk assessment is high, especially when evaluating the adequacy of compensative controls. Katakri may also be used in use cases which differ from the supported use cases (Act 726/2014, Act 588/2004, Act 1406/2011) and which may also have a different risk management model. For example when using Katakri in the internal security work of an organisation to support the protection of information owned by the organisation, it is often advisable to take advantage of the internal risk management procedures used by the organisation.

National security authority
PO BOX 176
FI-00023 GOVERNMENT FINLAND
NSA@formin.fi
https://um.fi/national-security-authority-nsa