EUROPEAN
COMMISSION

Brussels, 22.3.2022
COM(2022) 119 final

2022/0084 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on information security in the institutions, bodies, offices and agencies of the Union

{SWD(2022) 65 final} - {SWD(2022) 66 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

This proposal is part of the EU Security Union Strategy[1] adopted by the Commission on 24 July 2020 and laying down its commitment to bring the European Union's added value to the national efforts in the area of security. Part of this engagement is the initiative to streamline the internal legal frameworks for information security in all Union institutions and bodies.

A key feature of the Strategic Agenda for 2019-2024 adopted by the European Council in June 2019 is to protect our societies from the ever evolving threats targeting the information handled by institutions and bodies. In its conclusions[2], the European Council called in particular on 'the EU institutions, together with the Member States, to work on measures to enhance the resilience and improve the security culture of the European Union against cyber and hybrid threats from outside the EU, and to better protect the EU's information and communication networks, and its decision-making processes, from malicious activities of all kinds'.

In the same line, the General Affairs Council of December 2019[3] concluded that the EU institutions and bodies, supported by Member States, should develop and implement a comprehensive set of measures to ensure their security. This echoes a long standing request from the Council Security Committee to investigate a common core of security rules for the Council, the Commission and the European External Action Service[4].

Currently, the Union institutions and bodies either have their own information security rules, based on their Rules of procedure or founding act, or they do not have information security rules at all. This is mostly the case of some small entities, which lack any formal information security policies.

Due to the ever-increasing amounts of sensitive non-classified and European Union classified information ('EUCI') that the Union institutions and bodies need to share between themselves and considering the dramatic development of the threat landscape, the European administration is exposed to attack in all its areas of activity. The information handled by our institutions and bodies is very attractive for the threat actors and needs to be appropriately protected. This requires swift action aiming at enhancing its protection.

Therefore and in order to increase the protection of the information handled by the European administration, this initiative aims to streamline the different legal frameworks of the Union institutions and bodies in the field by:

- Establishing harmonised and comprehensive categories of information, as well as common handling rules for all Union institutions and bodies,
- Setting up a lean cooperation scheme on information security between Union institutions and bodies able to foster a coherent information security culture across the European administration,

---

1 Communication on the EU Security Union Strategy, COM(2020) 605, 24 July 2020 (Strategic priority 'A future-proof security environment).
2 EUCO 9/19.
3 14972/19.
4 WK 10563/2018 INIT section 9.

- Modernising the information security policies at all levels of classification/categorisation, for all Union institutions and bodies, taking into account the digital transformation and the development of teleworking as a structural practice.

- **Consistency with existing policy provisions in the policy area**

This initiative is in accordance with a wide range of EU policies in the area of security and information security.

Back in 2016, the European Parliament and the Council adopted a Directive[5] concerning measures for a high common level of security of network and information systems across the Union. This Directive was the first EU wide legislative measure meant to increase the cooperation between Member States on cybersecurity. While the Commission has adopted in December 2020 a proposal for the review of this instrument, introducing supervisory measures for the national authorities, the Union administration remains outside its scope.

In the same vein and to complement the efforts of Member States in the area of security, it is of paramount importance that the Union institutions and bodies achieve a high level of protection for their information and their related Information and Communication Systems with a view to safeguarding the information security.

In July 2020, the Commission adopted the Security Union Strategy[6], with a comprehensive commitment from the EU to complement Member States' efforts in all areas of security. This Strategy runs from 2020 to 2025 and outlines four main pillars of action: a future-proof security environment, tackling evolving threats, protecting Europeans from terrorism and organised crime and a strong European security ecosystem. Several of the topics addressed under these pillars focus on security of information, cybersecurity, cooperation and information exchange, and critical infrastructure.

In line with the Security Union Strategy, the European Commission proposes the creation of a minimum set of rules on information security across all the Union institutions and bodies, which will trigger mandatory and high common standards for the secure exchange of information. This initiative represents the engagement of the institutions and bodies to set within the European administration the same level of ambition in the field of security as required from the Member States.

On 16 December 2020, the Commission and the High Representative for Foreign Affairs and Security Policy presented a new EU Cybersecurity Strategy[7]. It set out priorities and key actions to build up Europe's resilience, autonomy, leadership and operational capacity in the face of growing and complex threats to its network and information systems, and to advance a global and open cyberspace and its international partnerships thereof. It is equally important that the Union institutions and bodies contribute to the achievement of these priorities by establishing equivalent requirements in the field of both information security and cybersecurity.

---

5 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194/1).

6 C(2020)605.

7 The EU's Cybersecurity Strategy for the Digital Decade | Shaping Europe's digital future (europa.eu) including a Joint Communication with the High Representative of the Union for Foreign Affairs and Security Policy (JOIN(2020)18) and also a revised Network and Information Security (NIS) Directive (COM(2020)823).

This proposal together with the proposal for a Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union, seek to complete the regulatory picture of the Security Union Strategy with dedicated requirements for the European administration. In view of the interlinkages between information security and cybersecurity, a coherent approach to the protection of non-classified information should be ensured between these two proposals.

- **Consistency with other Union policies**

This initiative also takes account of other Union policies that are relevant to the information security.

In the area of data protection and applicable to the European Union and European Atomic Energy Community ('Euratom') administration there is Regulation (EU) 2018/1725[8] on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data. In the same line, we need to mention that for some Union institutions and bodies the EU legislators have adopted specific relevant rules for the protection of personal data.

In the area of transparency, this proposal builds on the principles enshrined in the Regulation (EC) No 1049/2001[9] regarding public access to European Parliament, Council and Commission documents, with respect to other relevant rules.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

- **Legal basis**

Considering the objective and the content of this proposal, its most appropriate legal basis is Article 298 of the Treaty on the Functioning of European Union (TFEU) and Article 106a of the Treaty establishing the European Atomic Energy Community.

Article 298 TFEU was introduced by the Lisbon Treaty and enables the legislators to establish provisions with a view to creating an efficient and independent administration that will support the institutions, bodies, offices and agencies in carrying out their mission.

An efficient and independent administration relies on the security of its information. With a view to achieving their mission, the Union institutions and bodies shall benefit from a secure environment for the information they handle and store on a daily basis. In addition, providing a common baseline of standards mandatory for all would guarantee a high level of security, reduce the risk of weak links in supporting interoperability among institutions and bodies and leverage synergies thus enhancing the administration's resilience facing evolving threats.

Furthermore, with an overall aim to achieve a high common level of security for the EUCI and non-classified information handled and stored by the Union institutions and bodies, this proposal enables the European administration to better protect from external interferences and spying activities.

---

8 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

9 Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

Article 298 TFEU enables the Union to establish common rules for the whole of the European administration to ensure that all Union institutions and bodies treat the EUCI and the non-classified information similarly. As such, this Regulation lays down rules applicable to the administration and may indirectly impose obligations only to the individuals performing tasks on behalf of this administration or on a contractual basis (not including the Commissioners, the Representatives of Member States acting within the Council, the Members of the European Parliament, the Judges of the Union Courts or the Members of the European Court of Auditors).

According to Article 298 TFEU, the European Parliament and the Council shall act by means of a regulation and in accordance with the ordinary legislative procedure.

This proposal needs an additional legal basis as it also covers the information related to some activities of the European Atomic Energy Community. Such information is not Euratom Classified Information, but it is treated by the Union institutions and bodies under the general regime of EUCI.

This additional legal basis is Article 106a of the Treaty establishing the European Atomic Energy Community, which renders Article 298 TFEU applicable to the above mentioned Euratom activities as well.

- **Subsidiarity (for non-exclusive competence)**

According to the principle of subsidiarity laid down in Article 5(3) of the Treaty on European Union, action at EU level should be taken only when the aims envisaged cannot be achieved sufficiently by Member States alone and can therefore, by reason of the scale or effects of the proposed action, be better achieved by the EU.

Since only the Union can adopt rules governing EUCI and sensitive non-classified information handled and stored by the Union institution and bodies, the subsidiary principle does not apply.

- **Proportionality**

The establishment of a common baseline of information security to all Union institutions and bodies is necessary to contribute to an independent and efficient administration.

In accordance with the principle of proportionality laid down in Article 5(4) TEU, the provisions of the Regulation are not overly prescriptive and leave room for different levels of specific action, in line with the security maturity level of each Union institution and body.

Furthermore, the solution has limited impact on fundamental rights of individuals. Hence, the proposal does not go beyond what is necessary to address the problem of not having a common set of information security rules for all Union institutions and bodies.

- **Choice of the instrument**

A regulation based on Article 298 of the TFEU is considered the appropriate legal instrument.

It is justified by the predominance of elements that require a uniform application that does not leave margins of implementation to the Union institutions and bodies and that creates a minimum horizontal framework.

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- **Ex-post evaluations/fitness checks of existing legislation**

Not Applicable

- **Stakeholder consultations**

The Commission has carried out a broad consultation of the key stakeholders on various aspects related to information security rules of the Union institutions and bodies. The overall aim of the consultation activities was to collect relevant input for the preparation of a legislative initiative on information security rules common to all Union institutions and bodies. The consultations sought to collect inputs on:

- Problems related to the existing framework of information security within the Union institutions and bodies that stakeholders consider should be addressed in the initiative;
- The relevance, effectiveness, efficiency and added value of the initiative;
- The anticipated impacts of the initiative and possible other consequences for the stakeholders.

In preparation of this legislative proposal, the Commission has consulted the following categories of stakeholders:

1. Union institutions, bodies, offices and agencies;
2. National security authorities in the Member States;
3. Research experts from JRC.

Given the particular characteristic of this initiative, which is exclusively applicable to the Union institutions and bodies, with little impact on the European citizens and businesses, Commission services chose to prioritise the collection of viewpoints from the relevant stakeholder groups. As such, **no public consultation was conducted** specifically for this legislative initiative.

Over the course of the consultation process, Commission services used the following **methods and forms of consultation:**

1. An opportunity for all interested parties to provide feedback on the Inception Impact Assessment via the Commission's 'Have your say' platform;
2. A targeted questionnaire addressed to the information security experts within the Union institutions and bodies via online EU survey;
3. A targeted questionnaire addressed to the Member States national security authorities via online EU survey;
4. A request for a tailored risk assessment of the core information security assets and,
5. Numerous meetings and exchanges with counterparts from institutions, bodies, offices and agencies, as well as from the Member States national security authorities.

As main inputs from the consultation activities, the Commission highlights the following:

- The fragmentation of the relevant legal frameworks between our institutions and bodies creates significant duplication of efforts for creating and maintaining internal rules as well as non-interoperable practices in handling information. For the Member States, the diversity of these rules increases the risks of misunderstanding, misinterpreting and non-compliance;
- While establishing a baseline of information security for all Union institutions and bodies would create an ecosystem with standardised security rules and implemented best practices, the diversity and the different business environment of each Union

institution and body shall be taken into account and local solutions should be allowed;

- This initiative needs to respect the autonomy and the different security maturity levels of each Union institution and body, which will remain fully responsible for their organisation of information security;

- **Collection and use of expertise**

The Commission used its own resources to perform the stakeholders' consultation. The Security Directorate of DG HR has done the related work on the surveys, videoconferences and other workshops. This task involved both the selection of participants and the organisation of events and the processing of the input received.

The Joint Research Center (JRC) performed a risk assessment of the main information security assets, used as a basis for the Impact analysis.

- **Impact assessment**

This initiative is exclusively addressed to the Union institutions and bodies and has a limited impact to the Member States and individuals. Therefore, it was not necessary to perform a throughout impact assessment as there were no clearly identifiable or significant impacts on citizens and businesses. A comprehensive Roadmap was published on Europa website and gathered feedback from the relevant stakeholders.

- **Regulatory fitness and simplification**

Not Applicable

- **Fundamental rights**

The EU is committed to ensuring high standards of protection of fundamental rights. This initiative ensures full compliance with the fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union[10], as follows:

- The right to good administration[11]

By enhancing the security of information they handle when treating the affairs of European citizens, the Union institutions and bodies contribute to the achievement of the principle of good administration.

- Protection of personal data[12]

All processing of personal data in the framework of this proposal would be conducted in trusted environments and in full respect of the Regulation (EU) 2018/1725 of the European Parliament and of the Council.

- Right of access to documents[13]

Public access to EUCI and sensitive non-classified documents remains fully governed by Regulation (EC) 1049/2001 of the European Parliament and of the Council.

- Right to intellectual property[14]

---

10 Charter of Fundamental Rights of the European Union (OJ C 326, 26.10.2012, p. 391–407).
11 Article 41 of the Charter of Fundamental Rights of the European Union.
12 Article 8 of the Charter of the Fundamental Rights of the European Union.
13 Article 42 in the Charter of Fundamental Rights of the European Union.
14 Article 17 of the Charter of Fundamental rights of the European Union.

While handling and storing non-classified information and EUCI, the Union institutions and bodies protect the intellectual property in accordance with Directive 2001/29/EC of the European Parliament and of the Council[15].

- Freedom of expression and information[16]

While everybody has the freedom to receive and share information and ideas without interference by public authority, this shall not prevent the Union from establishing the conditions for accessing, handling and storing certain types of information, based on their confidentiality level.

The exercise of these freedoms may be subject to conditions and restrictions provided by law and necessary in a democratic society, in order to prevent the disclosure of information received in confidence and in the interest of EU security.

4. BUDGETARY IMPLICATIONS

This proposal requires the assignment of one AD official and one AST assistant for the permanent Secretariat of the Coordination Group which is provided by the Commission, in the Security Directorate of the Directorate-General for Human Resources and Security.

For the institutions and bodies there are cost savings expected in terms of the shared and collaborative tasks as well as from preventing potential economic damages resulted from security incidents, due to improvements in information security. On the other side, the financial efforts required for the implementation of the new legislation can be covered as part of the existing information security improvement programmes in each Union institution and body.

5. OTHER ELEMENTS

- **Implementation plans and monitoring, evaluation and reporting arrangements**

The proposal provides for the obligation of the Commission to report each 3 years to the European Parliament and to the Council on the implementation of this Regulation, including the functioning of the governance set up by this Regulation.

Moreover and every 5 years, the Commission shall evaluate this Regulation with a view to assessing its actual performance and based on this, whether any modification to the legislation is necessary.

- **Detailed explanation of the specific provisions of the proposal**

This proposal is structured around the requirements for handling and storing non-classified information and EUCI, which are the main subjects of the initiative and whose enhanced protection represents its underlying purpose.

Subject and scope (Article 1 and Article 2)

This Regulation is set to create a minimum set of information security rules applicable to all Union institutions and bodies.

It applies to all information handled and stored by the Union institutions and bodies, including the information related to European Atomic Energy Community activities, other than Euratom

[15] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ L 167, 22.6.2001, p. 10–19).

[16] Article 11 in the Charter of the Fundamental Rights of the European Union.

Classified Information. Both the non-classified information and the EUCI are covered by this Regulation.

Definitions and general principles (Articles 3 to 5)

The definitions provided under Article 3 are based on the current rules on information security adopted separately by the Union institutions and bodies.

Besides the general principles of the Union legislation: transparency, proportionality, efficiency and accountability, this Regulation provides for the main binding guiding lines, such as separate information security risk management process carried out by each Union institution and body and the assessment of their information in order to be properly categorised.

Governance and organisation of security (Articles 6 to 8)

All Union institutions and bodies shall cooperate in an Interinstitutional Information Security Coordination Group, which acts by consensus and in the common interest of the Union institutions and bodies.

The Coordination Group gathers the Security Authorities of all institutions and bodies and establishes guidance documents on the implementation of this Regulation. It liaises regularly with the National Security Authorities of the Member States, gathered in an Information Security Committee.

Five sub-groups composed by experts representing different institutions and bodies are set up with a view to streamlining the procedures and other practical aspects related to the information security.

Each Union institution and body is required to designate a Security Authority, which is responsible for defining internal policies on the Information security and for implementing them. The Security Authority establishes specific functions such as the Information Assurance Authority, the Information Assurance Operational Authority, the Security Accreditation Authority, the TEMPEST Authority, the Crypto Approval Authority and the Crypto Distribution Authority, which may be delegated to another institution or body for efficiency or resources reasons.

Information assurance and communication and information systems (Articles 9 to 11)

The Regulation establishes a sub-group on information assurance with the objective of enhancing the coherence across the Union institutions and bodies between the information security rules and the cybersecurity baseline as defined by the Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union.

The Union institutions and bodies are required to comply with the principles mentioned under these articles and adopt separate internal rules for specific security measures, adjusted to their own security environment.

Non-classified information (Articles 12 to 17 and Annex I)

The Regulation provides for 3 categories of non-classified information: information for public use, normal information and sensitive non-classified information. All categories are defined, while markings and handling conditions are stipulated for protecting such information.

With a view to coordinating the work on equivalence between particular categories established by some Union institutions and bodies and common categories provided by the Regulation, the proposal sets up a sub-group on non-classified information.

EUCI (Articles 18 to 58 and Annexes II to VI)

As the most voluminous of the proposal, this chapter is structured in seven sections, as follows: General provisions, Personnel security, Physical security, Management of EUCI, Protection in communication and information systems, Industrial security and Sharing EUCI and exchanging classified information.

The section on general provisions provides for four levels of EUCI: TRES SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET, CONFIDENTIEL UE/EU CONFIDENTIAL, RESTREINT UE/EU RESTRICTED and provides for an obligation of Union institutions and bodies to take the necessary security measures in accordance with the results of an information security risk management process.

Each of the remaining sections focus on the standards of EUCI protection, related to their specific area. The details for this protection of EUCI are specified in the Annexes II to V. Annex VI provides for the table of equivalence of EUCI with the security classifications of Member States and European Atomic Energy Community.

With the aim to streamline the relevant processes in the field and to avoid duplication of effort, the Regulation sets up sub-groups on information assurance, on non-classified information, on physical security, on accreditation of communication and information systems handling and storing EUCI and on EUCI sharing and exchange of classified information.

Final provisions (Articles 59 to 62)

The final provisions ensure the transition from the current rules and procedures to the new legal framework set by this Regulation. They concern the internal rules on information security currently applicable in the Union institutions and bodies, the recognition of assessment visits carried out before the start of application of the Regulation, the treatment of previously concluded administrative arrangements and the continuation of specific security frameworks applicable to grant agreements.

This Regulation is set to apply after 2 years from the date of its entry into force.

2022/0084 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on information security in the institutions, bodies, offices and agencies of the Union

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 298 thereof,

Having regard to the Treaty establishing the European Atomic Energy Community, and in particular Article 106a thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national Parliaments,

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) Union institutions and bodies currently have their own information security rules, based on their rules of procedure or their founding act, or do not have such rules at all. In that context, each Union institution and body invests significant efforts in adopting different approaches, leading to a situation where exchange of information is not always reliable. The lack of a common approach hinders the deployment of common tools building on an agreed set of rules depending on the security needs of the information to be protected.

(2) While progress has been made towards more consistent rules for the protection of European Union classified information ('EUCI') and non-classified information, the interoperability of the relevant systems remains limited, preventing a seamless transfer of information between the different Union institutions and bodies. Further efforts should therefore be made to enable an interinstitutional approach to the sharing of EUCI and sensitive non-classified information, with common categories of information and common key handling principles. A baseline should also be envisaged to simplify procedures for sharing EUCI and sensitive non-classified information between Union institutions and bodies and with Member States.

(3) Therefore, relevant rules ensuring a common level of information security in all Union institutions and bodies should be laid down. They should constitute a comprehensive and coherent general framework for protecting EUCI and non-classified information, and should ensure equivalence of basic principles and minimum standards.

(4) The recent pandemic caused a significant change in working practices with remote communication tools becoming the rule. Therefore, many procedures that were still at least partly paper-based were rapidly adjusted to enable electronic processing and exchanges of information. These developments require changes in the handling and protection of information. This Regulation takes account of the new working practices.

(5) By creating a minimum common level of protection for EUCI and non-classified information, this Regulation contributes to ensuring that the Union institutions and bodies have the support of an efficient and independent administration in carrying out their missions. At the same time, each Union institution and body retains its autonomy in determining how to implement the rules laid down in this Regulation, in line with its own security needs. This Regulation shall in no case prevent Union institutions and bodies to fulfil their mission, as entrusted by the EU legislation, or encroach on their institutional autonomy.

(6) This Regulation is without prejudice to Regulation (Euratom) No 3/1958[17], Regulation No 31 (EEC), 11 (EAEC), laying down the Staff Regulations of Officials and the Conditions of Employment of other servants of the European Economic Community and the European Atomic Energy Community[18], Regulation (EC) 1049/2001 of the European Parliament and of the Council[19], Regulation (EU) 2018/1725 of the European Parliament and of the Council[20], Council Regulation (EEC, EURATOM) No 354/83[21], Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council[22], Regulation (EU) 2021/697 of the European Parliament and of the Council[23], Regulation (EU) [...] of the European Parliament and of the Council[24] laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union.

(7) In order to preserve the specific nature of the European Atomic Energy Community activities regulated by Regulation 3/1958 of the Council of the European Atomic Energy Community[25], this Regulation should not apply to Euratom Classified Information. However, all information related to other Euratom activities not covered by Regulation 3/1958 should fall within the scope of this Regulation.

(8) With a view to establishing a formal structure for cooperation between Union institutions and bodies in the field of information security, it is necessary to set up an Interinstitutional Coordination Group (the 'Coordination Group') in which all

---

17 Regulation (Euratom) No 3/1958 implementing Article 24 of the Treaty establishing the European Atomic Energy Community (OJ 17, 6.10.1958, p. 406).

18 OJ 45, 14.6.1962, p. 1385.

19 Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

20 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

21 Council Regulation (EEC, EURATOM) No 354/83 of 1 February 1983 concerning the opening to the public of the historical archives of the European Economic Community and the European Atomic Energy Community (OJ L 43, 15.2.1983, p. 1).

22 Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012 (OJ L 193, 30.7.2018, p. 1).

23 Regulation (EU) 2021/697 of the European Parliament and of the Council of 29 April 2021 establishing the European Defence Fund and repealing Regulation (EU) 2018/1092 (OJ L 170, 12.5.2021, p. 149).

24 Regulation […] of the European Parliament and of the Council laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union, to be adopted

25 EAEC Council: Regulation No 3 implementing Article 24 of the Treaty establishing the European Atomic Energy Community (OJ 17, 6.10.1958, p. 406).

Union institutions' and bodies' Security Authorities are represented. Without having decision-making powers, the Cordination Group should enhance the coherence of policies in the field of information security and should contribute to the harmonisation of the information security procedures and tools across the Union institutions and bodies.

(9) The Coordination Group's work needs the support of experts in different areas of information security: categorisation and marking, communication and information systems, accreditation, physical security and sharing EUCI and exchanging classified information. In order to prevent duplication of effort across the Union institutions and bodies, thematic sub-groups should be therefore established. Moreover, where needed, the Coordination Group should be able to set up other subgroups with specific tasks.

(10) The Coordination Group should closely cooperate with the National Security Authorities of the Member States with a view to enhancing information security in the Union. An Information Security Committee of the Member States should therefore be set up to provide advice to the Coordination Group.

(11) While the common bodies representing all Union institutions and bodies are set up based on the cooperation principle, each institution and body should remain fully responsible for the security of information within its organisation. Each Union institution and body should have a Security Authority and where necessary, other authorities in charge of specific responsibilities related to information security.

(12) The principle of information security risk management should be at the core of the policy to be developed in the field by each Union institution and body. While the minimum requirements laid down in this Regulation must be met, each Union institution and body should adopt specific security measures for protecting information in accordance with the results of an internal risk assessment. In the same way, the technical means to protect the information should be adapted to the specific situation of each institution and body.

(13) Given the diversity of categories of non-classified information that the Union institutions and bodies have developed based on their own security information rules and in order to avoid delay in the implementation of this Regulation, Union institutions or bodies should be able to maintain their own marking system for internal purposes or in the exchange of information with their particular counterparts from other institutions and bodies or from the Member States.

(14) With the purpose of adjusting to the new teleworking practices, the networks used for connecting to the Union institution's or body's remote access services should be protected by adequate security measures.

(15) Since Union institutions and bodies frequently make use of contractors and outsourcing, it is important to establish common provisions relating to contractors' personnel carrying out tasks related to information security.

(16) The substantive rules regarding access to EUCI in the internal rules of various Union institutions and bodies are currently aligned, but there are significant differences as regards denominations and required procedures. This creates a burden for the National Security Authorities of the Member States who need to adjust to different requirements. Thus it is necessary to provide for a common glossary and common procedures in the area of personnel security, thereby simplifying cooperation with the National Security Authorities of the Member States and limiting the risk of compromising EUCI.

(17) Given the disparity of resources amongst Union institutions and bodies and in order to streamline their relevant procedures and practices, the security clearance tasks can be entrusted to the Commission in order to provide a continuation of a long-standing practice in the field of security clearance and contribute to the centralisation of the tasks assigned to each Security Authority.

(18) The protection of EUCI is also ensured by technical and organisational measures which apply to the premises, buildings, rooms, offices or facilities of the Union institutions and bodies where EUCI is discussed, handled or stored. This Regulation provides for the implementation of an information security management process in the area of physical security which would allow Union institutions and bodies to select the appropriate security measures for their sites.

(19) All Union institutions and bodies handling and storing EUCI should establish physically protected areas in their sites, in order to ensure the same level of protection for the relevant levels of EUCI classification handled and stored within. Those areas should be designated as Administrative Areas and Secured Areas and respect common minimum standards for the protection of EUCI.

(20) Originator control is an important principle in the EUCI management, therefore it needs to be clearly stipulated and developed. In that regard, the creation of EUCI confers to the originator a responsibility which should cover the entire life cycle of the relevant EUCI document.

(21) Union institutions and bodies have been traditionally developed their communication and information systems autonomously, with insufficient attention to their interoperability across all Union institutions and bodies. It is therefore necessary to establish minimum security requirements concerning the Communication and Information Systems (CISs) handling and storing both EUCI and non-classified information with the aim to guarantee a seamless exchange of information with the relevant stakeholders.

(22) With the objective of achieving a single standard of accreditation of CISs handling and storing EUCI, the Union institutions and bodies should work together in a group set up for that purpose. It is recommended that all of them use that standard in order to contribute to a general level of EUCI protection. However, as regards organisational autonomy, the decision remains with the competent authority of each institution or body.

(23) All Union institutions and bodies should follow the same procedures and apply the same measures when awarding and implementing classified contracts or grant agreements. Thus it is necessary to clearly stipulate both the mandatory and the optional elements of a classified contracts and grant agreements. However, the measures for the protection of EUCI in relation with classified contracts and grant agreements should take into account the rules already developed separately in the area by the Union institutions and bodies together with the Member States.

(24) The close cooperation between Union institutions and bodies as well as the multitude of synergies developed among them involve the sharing of a large amount of information. For the sake of the classified information security, the trustworthiness of a Union institution or body should be assessed before they handle and store a specified level of EUCI.

(25) Furthermore, the sharing of EUCI between the Union institutions and bodies and the exchange of classified information with international organisations and third

countries should also be regulated by appropriate security measures for the protection of that information. Where agreements on security of information are envisaged, the provisions of Article 218 of the Treaty should apply.

(26) The agreements on security of information are meant to ensure the overall legal framework for the exchange of classified information of the Union with the third countries and international organisations, it is also necessary to provide for the possibility of Union institutions and bodies to enter into administrative arrangements with a specific counterpart of a third country or of an international organisation for the purpose of exchanging EUCI.

(27) This Regulation establishes a framework common to all Union institutions and bodies. In order to avoid imposing an excesive administrative burden on the Union institutions and bodies in the process of adapting their internal security rules to the rules laid down in this Regulation, this Regulation should apply from 2 years after its entry into force.

(28) In accordance with paragraphs 22 and 23 of the Interinstitutional Agreement of 13 April 2016 on Better Law-Making[26], the Commission should evaluate this Regulation in order to assess its actual effects and the need for any further action. The Commission should submit to the European Parliament and to the Council a report on the implementation of this Regulation, at the latest 3 years from the date of application.

(29) The European Data Protection Supervisor was consulted in accordance with Article 42 of Regulation (EU) 2018/1725 of the European Parliament and of the Council[27] and delivered an opinion on ...

HAVE ADOPTED THIS REGULATION:

Chapter 1
General provisions

Article 1

Subject matter

1. This Regulation lays down information security rules for all Union institutions and bodies.

Article 2

Scope

1. This Regulation shall apply to all information handled and stored by the Union institutions and bodies, including information related to activities of the European Atomic Energy Community, other than Euratom Classified Information.

2. It shall apply to the following confidentiality levels of information:

[26] Interinstitutional Agreement between the European Parliament, the Council of the European Union and the European Commission on Better Law-Making (OJ L 123, 12.5.2016, p. 1–14).

[27] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018).

(a) three levels of non-classified information: public use, normal and sensitive non-classified;

(b) four levels of EU classified information: RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, TRES SECRET UE/EU TOP SECRET.

3. These levels are based on the damage that unauthorised disclosure may cause to the legitimate private and public interests, including those of the Union, Union institutions and bodies and Member States or other stakeholders, so that the appropriate protective measures can be applied.

Article 3

Definitions

For the purpose of this Regulation, the following definitions apply:

(a) 'information' means any data in oral, visual, electronic, magnetic, or physical form, or in the form of material, equipment or technology and includes reproductions, translations and material in the process of development;

(b) 'information security' means ensuring the authenticity, availability, confidentiality, integrity and non-repudiation of information;

(c) 'handling' of information means all possible actions to which the information can be subject throughout its life cycle; it comprises its creation, collection, registration, assignment of a confidentiality level, processing, display, consultation, carriage, transmission, downgrading, declassification, archiving and destruction;

(d) 'storing' means the act of keeping information on any medium to ensure its availability for future use;

(e) 'Union institutions and bodies' means the Union institutions, bodies, offices and agencies set up by, or on the basis of, the Treaty on European Union, the Treaty on the functioning of European Union, the Treaty establishing the European Atomic Energy Community or a legislative act;

(f) 'Euratom classified information' means information within the meaning of Regulation No 3/1958 of the Council of the European Atomic Energy Community;

(g) 'Security Authority' means the security function of each Union institution and body, designated in accordance with its rules of procedure or founding act;

(h) 'information security risk management process' means the entire process of identifying, controlling and minimising uncertain events that may affect the security of an organisation or of the systems it uses; it covers the entirety of risk-related activities, including assessment, treatment, acceptance and communication;

(i) 'asset' means anything that is of value to a Union institution or body, its operations and their continuity, including information resources that support their mission;

(j) ‘security operating procedures’ means a set of documented procedures, as referred to in Annex III, for the operation of a Secured Area, a communication and information system or other security-related asset or service to ensure its effectiveness;

(k) ‘communication and information system’ or ‘CIS’ means any system enabling the handling and the storage of information in electronic form, including all assets required for its operation;

(l) ‘information assurance’ means the certainty that the communication and information systems will protect the information they handle and store and will function as they need to, when they need to, under the control of legitimate users, while ensuring appropriate levels of authenticity, availability, confidentiality, integrity and non-repudiation;

(m) ‘accreditation’ means the formal authorisation from the Security Accreditation Authority for a communication and information system to process, or a Secured Area to store a pre-defined level of EUCI;

(n) ‘accreditation process’ means the steps and tasks required prior to accreditation;

(o) ‘TEMPEST security measures’ means measures to protect any CIS handling and storing information classified CONFIDENTIEL UE/EU CONFIDENTIAL or higher against compromise of such information through unintentional electromagnetic emanations;

(p) ‘CERT-EU’ means the Cybersecurity Centre for the Union institutions and bodies within the meaning of Regulation (EU) [...] of the European Parliament and of the Council laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union;

(q) ‘information security incident’ means any event potentially compromising the authenticity, availability, confidentiality, integrity or non-repudiation of stored, transmitted or processed information;

(r) ‘need-to-know’ means the necessity for an individual to access specified information handled or stored by an Union institution or body in order to fulfil the tasks of that particular Union institution or body;

(s) ‘zero trust’ means a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement of the existence of threats inside and outside traditional network boundaries;

(t) ‘marking’ means a label that is applied to information to ensure that the appropriate security measures are applied;

(u) ‘security marking’ means a marking indicating the level of confidentiality of the information;

(v) ‘distribution marking’ means a marking indicating the intended addressees of information within originating Union institution or body;

(w) ‘releasability marking’ means a marking indicating the permitted addressees outside the originating Union institution or body;

(x) ‘system owner’ means the individual responsible for the overall procurement, development, integration, modification, operation, maintenance and retirement of a communication and information system;

(y) ‘threat to information security’ means an event or agent that can reasonably be expected to adversely affect information security if not responded to and controlled;

(z) ‘vulnerability’ means a weakness, susceptibility or flaw of an asset, system, process or control that can be exploited by one or more threats;

(aa) ‘risk’ means the potential adverse effect of a given threat, possibly exploiting internal and external vulnerabilities of a Union institution or body or of the systems it uses, causing harm to the legitimate public and private interests, measured as a combination of the likelihood of threats occurring and their impact;

(ab) ‘residual risk’ means the risk which remains after security measures have been implemented;

(ac) ‘risk assessment’ means identifying threats and vulnerabilities and conducting the related risk analysis, there is to say the analysis of probability and impact;

(ad) ‘risk treatment’ means mitigating, removing, reducing (through an appropriate combination of technical, physical, organisational or procedural measures), transferring or monitoring the risk;

(ae) ‘European cybersecurity certificate’ means a certificate within the meaning of Article 2(11) of Regulation EU 2019/881[28];

(af) ‘holder’ means a duly authorised individual with an established need-to-know who is in possession of an item of information requiring protection and accordingly responsible for protecting it;

(ag) ‘material’ means any document, data carrier or item of machinery or equipment, either manufactured or in the process of manufacture;

(ah) ‘European Union classified information’ or ‘EUCI’ means any information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the Union or of one or more of the Member States;

(ai) ‘authorisation to access EUCI’ means a decision by a Security Authority that an official, other servant or seconded national expert of a Union institution or body may be granted access to EUCI up to a specified level for a set period of time;

(aj) ‘National Security Authority’ or ‘NSA’ means a government authority of a Member State with ultimate responsibility for the security of classified information in that Member State;

(ak) ‘Designated Security Authority’ or ‘DSA’ means an authority of a Member State (NSA or any other competent authority) which is responsible

[28] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15–69)

for providing direction and assistance in the implementation of industrial security or in clearances procedures, or both;

(al) 'security investigation' means the investigative procedures conducted by the competent authority of a Member State in accordance with its national law and regulations in order to obtain an assurance that nothing adverse is known which would prevent an individual from being granted a security clearance up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or higher);

(am) 'physical security' means the application of physical, technical and organisational measures to premises, buildings, rooms, offices or facilities of a Union institution or body that require protection against unauthorised access to information that is handled, stored or discussed therein;

(an) 'sites' means the premises, buildings, rooms, offices or facilities of a Union institution or body;

(ao) 'defence in depth' means a type of security which uses several independent layers of security controls to ensure that where one fails another will be operative;

(ap) 'cryptographic (crypto) material' means cryptographic algorithms, cryptographic hardware and software modules, and products including implementation details and associated documentation and keying material;

(aq) 'cryptographic product' means a product whose primary and main functionality is the provision of security services (authenticity, availability, confidentiality, integrity and non-repudiation) through one or more cryptographic mechanisms;

(ar) 'originator' means the Union institution or body, Member state, third country or international organisation under whose authority classified information has been created or introduced into the Union's structures;

(as) 'document' means any content, whatever its medium (paper, electronic, magnetic or other), in written form or visual or audiovisual recording;

(at) 'registration for security purposes' means the application of procedures which record the life-cycle of material, including its dissemination and destruction;

(au) 'declassification' means the removal of any security classification;

(av) 'downgrading' means a reduction in the level of security classification;

(aw) 'classified contract' means a framework contract or a contract, as referred to in Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council, entered into by a Union institution or body, with a contractor for the supply of movable or immovable assets, the execution of works or the provision of services, the performance of which requires or involves the handling, including creation, or storing of EUCI;

(ax) 'classified grant agreement' means an agreement whereby a Union institution or body awards a grant, as referred to in Title VIII of Regulation (EU, Euratom) 2018/1046, the performance of which requires or involves the handling, including creation, or storing of EUCI;

(ay) 'classified subcontract' means a contract entered into by a contractor or beneficiary of a Union institution or body, with a subcontractor for the supply of movable or immovable assets, the execution of works or the provision of

services, the performance of which requires or involves the handling, including creation, or storing of EUCI;

(az) 'Programme or Project Security Instruction' or 'PSI' means a list of security procedures which are applied to a specific programme or project in order to standardise security procedures;

(ba) 'Security Aspects Letter' or 'SAL' means a set of special contractual conditions, issued by the contracting or granting authority, which forms an integral part of any classified contract or grant agreement involving access to or the creation of EUCI, that identifies the security requirements and those elements of the contract or grant requiring security protection;

(bb) 'Security Classification Guide' or 'SCG' means a document which describes the elements of a programme, project, contract or grant agreement which are classified, specifying the applicable security classification levels;

Article 4

General principles

1. Each Union institution and body shall be responsible for the implementation of the provisions of this Regulation within its organisation taking account of its own information security risk management process.

2. Non-compliance with this Regulation, in particular the unauthorised disclosure of information with the confidentiality levels referred to in Article 2(2), except information for public use shall be subject to investigation and may trigger personnel liability in accordance with the Treaties or with their relevant staff rules.

3. Union institutions and bodies shall assess all information they handle and store in order to categorise it in accordance with the confidentiality levels referred to in Article 2(2).

4. Union institutions and bodies shall determine the security needs of all information they handle and store considering the following aspects:

(a) authenticity: the guarantee that information is genuine and from bona fide sources;

(b) availability: accessibility and usability upon request by an authorised entity;

(c) confidentiality: non-disclosure of information to unauthorised individuals, entities, or processes;

(d) integrity: the fact that the information is complete and completeness of information is unaltered;

(e) non-repudiation: the ability to prove an action or event has taken place, so that that event or action cannot subsequently be denied;

5. For each communication and information system under their responsibility, the Union institutions and bodies shall identify the highest confidentiality level that such communication and information system can handle and store, carry out a information security risk assessment and regularly monitor the security needs and the correct implementation of the identified protective measures.

6. All Union institutions and bodies shall provide training and awareness activities on how to handle and store non-classified information and EUCI.

Union institutions and bodies handling and storing EUCI shall organise mandatory training at least once every 5 years for all individuals authorised to access EUCI. The Union institutions and bodies concerned shall organise specific training for the specific functions entrusted with information security tasks.

A Union institution or body may coordinate such training and awareness activities with other Union institutions and bodies.

Article 5

Information security risk management process

1. Each Union institution and body shall establish an information security risk management process for the protection of the information they handle and store.

2. The information security risk management process shall include the following steps:

(a) threat and vulnerability identification;

(b) risk assessment;

(c) risk treatment;

(d) risk acceptance;

(e) risk communication.

3. The information security risk management process shall take account of all factors relevant for the institution or body concerned, in particular:

(a) the confidentiality level of the information and the related legal obligations;

(b) the form and the quantity of the information and the facilities or CISs where the information is handled and stored;

(c) the persons accessing the information on sites or remotely;

(d) the surrounding environment and the structure of the buildings or areas storing the information,

(e) the threats targeting the Union, the Union institutions and bodies or the Member States from cyberattacks, supply chain attacks, espionage, sabotage, terrorist, subversive or other criminal activities;

(f) business continuity and disaster recovery;

(g) the results of inspections, audits or assessment visits, where applicable.

Chapter 2
Governance and organisation of security

Article 6

Interinstitutional Information Security Coordination Group

1. An Interinstitutional Information Security Coordination Group (the ‘Coordination Group’) is established.

It shall be composed of all Security Authorities of the Union institutions and bodies, and shall have a mandate to define their common policy in the field of information security.

2. Acting by consent and in the common interest of all Union institutions and bodies, the Coordination Group shall:

   (a) adopt its rules of procedures and annual common objectives and priorities;

   (b) adopt decisions on the establishment of thematic sub-groups and their terms of reference;

   (c) establish guidance documents on the implementation of this Regulation, in cooperation with the Interinstitutional Cybersecurity Board referred to in Article 9 of the Regulation EU [...] laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union, where appropriate;

   (d) set up dedicated platforms for sharing best practices and knowledge on common topics relevant to information security as well as for providing assistance in case of information security incidents;

   (e) ensure that security measures are coordinated as necessary with the competent National Security Authorities for the purpose of protecting EUCI.

3. The Coordination Group shall designate a chairperson and two vice chairpersons from among its members, for a period of 3 years.

4. The Coordination Group shall meet at least once a year at the initiative of its chairperson or at the request of a Union institution or body.

5. The Coordination Group shall have the administrative support of a permanent secretariat provided by the Commission.

6. Each Union institution or body shall be appropriately represented in the Coordination Group and where applicable, in the thematic sub-groups.

7. Union institutions and bodies shall bring to the attention of the Coordination Group any significant information security policy development within their organisation.

8. In the performance of the tasks referred to in paragraph 2, point (e), the Coordination Group shall be assisted by an Information Security Committee. That Committee shall be composed of one representative from each National Security Authority and shall be chaired by the Secretariat of the Coordination Group, referred to in paragraph 5. The Information Security Committee shall have an advisory role.

Article 7

Thematic sub-groups

1. The Coordination Group shall set up the following permanent thematic sub-groups to facilitate the implementation of this Regulation:

   (a) a sub-group on information assurance;

   (b) a sub-group on non-classified information;

   (c) a sub-group on physical security;

(d) a sub-group on accreditation of communication and information systems handling and storing EUCI;

(e) a sub-group on EUCI sharing and exchange of classified information.

2. Where necessary, the Coordination Group may set up ad-hoc sub-groups for a specific task and for a limited duration.

3. Except where otherwise provided in their terms of reference, the sub-groups shall be based on open membership representing the Union institution or body concerned. The members of the sub-groups shall be experts in the respective field of competence.

4. The Secretariat of the Coordination Group, referred to in Article 5(5), shall support the work of all sub-groups and ensure the communication between its members.

Article 8

Organisation of security

1. Each Union institution and body shall designate a Security Authority to assume the responsibilities assigned by this Regulation and, where applicable, by its internal security rules. In performing its tasks, each Security Authority shall have the support of the department or officer entrusted with Information Security tasks.

2. Where necessary, the Security Authority of each Union institution and body shall adopt internal implementing rules for the protection of information, in accordance with their specific mission, as entrusted by the EU law, and based on their institutional autonomy.

3. Where relevant, each Security Authority shall also assume the following functions:

(a) Information Assurance Authority in charge of developing information assurance security policies and security guidelines and monitoring their effectiveness and pertinence;

(b) Information Assurance Operational Authority responsible for developing security documentation, in particular the Security Operating Procedures and the crypto plan within the communication and information systems accreditation process;

(c) Security Accreditation Authority in charge of accrediting Secured Areas and CIS handling and storing EUCI;

(d) TEMPEST Authority responsible for approving the measures taken to protect against compromise of EUCI through unintentional electronic emanations;

(e) Crypto Approval Authority responsible for approving the use of encrypting technologies based on a request from the system owner;

(f) Crypto Distribution Authority responsible for distributing cryptographic materials used for protecting EUCI (encryption equipment, cryptographic keys, certificates, and related authenticators) to the users concerned.

4. The responsibilities of one or more of the functions referred to in paragraph 3 may be delegated to another Union institution or body whenever decentralised delivery of security offers significant efficiency, resource or time savings.

Chapter 3
Information assurance and communication and information systems (CISs)

Article 9

Principles of information assurance

1. The assessment of the information security needs shall be taken into account from the start of the creation or at the procurement stage as regards all CISs including in-house, outsourced and hybrid CISs.

2. Any CIS that handles and stores EUCI shall be accredited in accordance with Chapter 5, Section 5. Any CIS that handles and stores sensitive non-classified information shall comply with the minimum requirements for sensitive non-classified information in CISs set out in Chapter 4.

Article 10

Sub-group on information assurance

1. The sub-group on information assurance, as referred to in Article 7(1) point (a), shall have the following roles and responsibilities:

   (a) providing guidance and best practices on the marking, handling and storing of information in CISs in close cooperation with the Interinstitutional cybersecurity board referred to in Article 9 of Regulation EU [XXX] laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union;

   (b) establishing a metadata scheme for markings and all necessary technical information to contribute to an interoperable and seamless exchange of information across Union institutions and bodies, when interconnecting their respective CISs;

   (c) contributing to the coherence between the information security rules and the cybersecurity baseline across all Union institutions and bodies, referred to in Article 5 of Regulation EU [XXX] laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union.

Article 11

Requirements for communication and information systems

1. Union institutions and bodies shall inform users about the confidentiality levels of information that can be handled and stored in a CIS. Where a CIS handles and stores multiple confidentiality levels, metadata and visual markings shall be used to ensure that the different levels can be distinguished.

2. Union institutions and bodies shall identify CIS' users before granting them access to any confidentiality levels other than public use. Users shall be authenticated at a level of assurance that is appropriate to the confidentiality level. Where appropriate, a secure common identification scheme shall be used.

3. Adequate security logs shall be maintained for all CISs to ensure swift investigations in the event of breaches or leaks of information. Such logs shall be maintained for a duration established in the business impact assessment or in the relevant security policies, in a non-repudiable manner.

   Where a CIS handles and stores EUCI, logs related to need-to-know and access to information shall be maintained until the information is declassified. Security logs shall be searchable and accessible by the Security Authority.

4. Union institutions and bodies shall adopt internal rules on the security of CISs to specify the appropriate security measures in accordance with the security needs of the information to be handled and stored, and taking into account the jurisdictions in which the information is stored, transmitted to and handled. Where applicable, those measures shall include the following:

   (a) restrictions on the geographical location;

   (b) consideration of potential conflicts of interest, boycotts or penalties relating to contractors;

   (c) contractual provisions to ensure the security of information;

   (d) encryption of information at rest and in transit;

   (e) restrictions on the accessibility of Union institutions and bodies' information by contractor personnel;

   (f) protection of personal data in accordance with the applicable data protection legislation.

5. The Union institutions and bodies shall manage their CISs in compliance with the following principles:

   (a) each CIS shall have a system owner or an Information Assurance Operational authority responsible for its security;

   (b) an information security risk management process covering information security aspects shall be conducted;

   (c) the security requirements and security operating procedures shall be formally defined, implemented, checked and reviewed;

   (d) information security incidents shall be formally recorded and followed up, in accordance with Regulation EU [XXX] laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union.

Chapter 4
Non-classified information

Article 12

Information for public use

1. Information intended for public use or official publication or already disclosed, which can be shared without restrictions inside or outside the Union institutions and bodies, shall be categorised and handled and stored as information for public use.

2. Union institutions and bodies may mark with 'PUBLIC USE' the information referred to in paragraph 1.

3. All Union institutions and bodies shall ensure the integrity and availability of information for public use by appropriate measures based on its security needs.

Article 13

Normal information

1. Information intended for use by a Union institution or body in the execution of its functions which is neither sensitive non-classified nor for public use shall be categorised, handled and stored as normal information. This category covers all normal working level information processed in the Union institution or body concerned.

2. Normal information may be marked visually or in metadata where necessary to ensure its protection, particularly where shared outside Union institutions and bodies. The marking 'EU NORMAL' or the 'name or acronym of the Union institution or body NORMAL' (adjusted on a case-by-case basis) shall be used in that case.

3. Union institutions and bodies shall define standard protective measures for normal information taking into account guidance from the sub-group on non-classified information and any specific risks related to their tasks and activities.

4. Normal information shall be exchanged outside Union institutions and bodies only with natural or legal persons having a need-to-know.

Article 14

Sensitive non-classified information

1. Union institutions and bodies shall categorise, handle and stored as sensitive non-classified all information that is not classified but which they must protect due to legal obligations or because of the harm that may be caused to the legitimate private and public interests, including those of the Union institutions and bodies, Member States or individuals by its unauthorised disclosure.

2. Each Union institution and body shall identify sensitive non-classified information by a visible security marking and shall define corresponding handling instructions in accordance with Annex I.

3. Union institutions and bodies shall protect sensitive non-classified information by applying appropriate measures in respect of its handling and storage. Such information may only be made available inside Union institutions and bodies to individuals with a need-to-know for the fulfilment of their assigned tasks.

4. Sensitive non-classified information shall be exchanged outside Union institutions and bodies only with natural and legal persons that have a need-to-know while respecting the handling instructions accompanying the information. All parties involved shall be made aware of the appropriate handling instructions.

Article 15

Protection of non-classified information and interoperability

1. Union institutions and bodies shall establish procedures for the reporting and management of any incident or suspected incident that could lead to a compromise of the security of non-classified information.

2. Where required, Union institutions and bodies shall use the markings provided for in Articles 12, 13 and 14. Exceptionally, other equivalent markings may be used internally and in relation with their particular counterparts from other Union institutions and bodies or from the Member States, when all parties agree. Such exception shall be notified to the sub-group on non-classified information, as referred to in Article 7(1), point (b).

3. Contractual safeguards shall be established to ensure the protection of normal and sensitive non-classified information processed by outsourced services. The safeguards shall be designed to guarantee at least an equivalent level of protection to that provided by this Regulation, and shall include confidentiality and non-disclosure undertakings to be signed by all relevant service providers involved in the provision of the outsourced systems.

Article 16

Sub-group on non-classified information

1. The sub-group on non-classified information referred to in Article 7(1), point (b), shall have the following roles and responsibilities:

   (a) streamlining the procedures relating to handling and storing the non-classified information and preparing the relevant guidance;

   (b) coordinating with the sub-group on information assurance referred to in Article 7(1), point (a), on matters related to systems handling and storing non-classified information;

   (c) preparing handling instructions for the different confidentiality levels of non-classified information;

   (d) assisting Union institutions and bodies in establishing the equivalence between their particular categories of non-classified information and those provided for in Articles 12, 13 and 14;

   (e) facilitating the sharing of non-classified information between Union institutions and bodies, by providing assistance and guidance.

Article 17

Handling and storing of sensitive non-classified information in CISs

1. Union institutions and bodies shall ensure that CISs meet the following minimum requirements when handling and storing sensitive non-classified information:

   (a) strong authentication shall be implemented to access SNC information and SNC information shall be encrypted in transmission and in storage;

   (b) encryption keys used for storage shall be under the responsibility of the Union institution or body responsible for the operation of the CIS;

(c) SNC information shall be stored and processed in the Union;

(d) contractual provisions covering security of staff, assets and information shall be included in any outsourcing contracts;

(e) interoperable metadata shall be used to record the confidentiality level of electronic documents and to facilitate the automation of security measures;

(f) measures to prevent and detect data leaks shall be implemented by the Union institutions and bodies to protect sensitive non-classified information;

(g) security equipment bearing a European cybersecurity certificate shall be used, where available;

(h) implementation of security measures based on the principles of need-to-know and zero trust to minimise access to sensitive non-classified information by service providers and contractors.

2. Any derogation from the minimum requirements set out in paragraph 1 shall be subject to approval by the appropriate level of management of the Union institution or body concerned, on the basis of a risk assessment covering the legal and technical risks to the security of the sensitive non-classified information.

3. The Information Assurance Authority of the Union institution or body concerned may check compliance with the principles set out in paragraph 1 at any time during the lifecycle of a CIS.

Chapter 5
EUCI

SECTION 1
GENERAL PROVISIONS

Article 18

Security classifications and markings

1. EUCI shall be classified at one of the following levels and shall be marked as follows:

(a) TRES SECRET UE/EU TOP SECRET: information and material the unauthorised disclosure of which could cause an exceptionally serious prejudice to the essential interests of the Union or of one or more of the Member States;

(b) SECRET UE/EU SECRET: information and material the unauthorised disclosure of which could seriously harm the essential interests of the Union or of one or more of the Member States;

(c) CONFIDENTIEL UE/EU CONFIDENTIAL: information and material the unauthorised disclosure of which could harm the essential interests of the Union or of one or more of the Member States;

(d) RESTREINT UE/EU RESTRICTED: information and material the unauthorised disclosure of which could be disadvantageous to the interests of the Union or of one or more of the Member States.

2. The Coordination Group shall adopt guidance documents on EUCI creation and classification.

Article 19

Suitability to handle and store EUCI

1. Any Union institution and body may handle and store EUCI where the following conditions are met:

   (a) it establishes rules and procedures in accordance with this Regulation, ensuring the protection of information for a given classification level; and

   (b) it has undergone an assessment visit in accordance with Article 53, and it has been subsequently certified that it can protect EUCI in accordance with this Regulation and where applicable, any other relevant rules and procedures.

2. The conditions set out in paragraph 1 shall be considered as met by default by the members of the sub-group on EUCI sharing and exchange of classified information referred to in Article 7(1), point (e).

Article 20

Protection of EUCI

1. The holder of any item of EUCI shall be responsible for its protection.

2. Where a Member State introduces classified information bearing a national security classification marking into the structures or networks of a Union institution or body, that institution or body shall protect that information in accordance with the corresponding classification marking laid down in the Agreement between the Member States of the European Union, meeting within the Council, regarding the protection of classified information exchanged in the interests of the European Union[29]. The corresponding table of equivalence is set out in Annex VI to this Regulation.

3. An aggregate of EUCI may warrant a level of protection corresponding to a higher classification than that of its individual components.

Article 21

EUCI security risk management process

1. The security Authority of each Union institution and body shall approve the security measures for protecting EUCI throughout its life-cycle in accordance with the outcome of a risk assessment performed by the respective Union institution or body.

2. The security measures taken by each Union institution and body shall be commensurate with the classification level of the information handled and stored, its form and volume, and the location and protective features of the facilities where EUCI is handled and stored and the locally assessed threat of malicious or criminal activities.

3. All Union institutions and bodies shall establish:

   (a) contingency plans to ensure EUCI security during emergencies;

[29] OJ C 202, 8.7.2011, p. 13.

(b) business continuity plans including preventive and recovery measures to minimise the impact of major failures or security incidents on the handling and storage of EUCI.

Article 22

Breaches of security and compromise of EUCI

1. An act or omission of a Union institution or body or an individual, which is in breach of this Regulation, shall be considered as a breach of security.

2. EUCI shall be considered to have been compromised where as a result of a breach, it has been disclosed, wholly or in part, to one or more persons that are not authorised to access that information.

3. Any compromise or suspected compromise of EUCI shall be reported immediately to the Security Authority of the relevant Union institution or body, which shall conduct a security inquiry and take at least the following measures:

   (a) inform the originator;

   (b) ensure that the case is investigated by personnel not immediately concerned with the breach in order to establish the facts;

   (c) assess the potential damage caused to the interests of the Union or of the Member States;

   (d) take appropriate measures to prevent a recurrence;

   (e) notify the competent authorities about the actual or potential compromise and the action taken.

SECTION 2
PERSONNEL SECURITY

Article 23

Basic principles

1. The Security Authority of a Union institution or body may grant individuals access to EUCI where all the following conditions are met:

   (a) the individuals have a need-to-know;

   (b) the individuals have been briefed on the security rules and procedures for protecting EUCI and the relevant security standards and guidelines, and have acknowledged in writing their responsibilities with regard to protecting such information;

   (c) for information classified CONFIDENTIEL UE/EU CONFIDENTIAL or higher, the individuals have been granted security clearance and have been authorised to the relevant level.

2. Union institutions and bodies shall take into account the loyalty, trustworthiness and reliability of an individual as determined by means of a security investigation conducted by the competent authorities of the Member State of which the applicant is a citizen or a national.

3. Union institutions and bodies may accept security clearances from third countries and international organisations with which the Union has a security of information agreement.

4. Union institutions and bodies may manage the clearance processes autonomously or seek a Service Level Agreement ('SLA') with the Commission for security clearance purposes.

   Where a SLA is concluded, the Commission Security Authority shall be the contact point between the security offices of the Union institution and body concerned and the national competent authorities of the Member States in the context of security clearance issues.

5. The Security Authority of each Union institution and body shall keep records of their security clearances, briefings, written acknowledgements and authorisations to access EUCI.

6. Union institutions and bodies that conclude an SLA with the Commission shall make the relevant records available to the Commission's Security Authority regarding as a minimum the level of EUCI to which the individual may be granted access, the date of issue of the authorisation to access EUCI and its period of validity. Those records shall be accessible to other Union institutions and bodies with an SLA, where justified.

Article 24

Authorisation to access EUCI

1. Each Union institution and body shall identify the positions within its organisation requiring access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or higher in order for the holder to perform their duties.

2. Whenever an individual needs to be authorised to access information classified CONFIDENTIEL UE/EU CONFIDENTIAL or higher, the institution or body concerned shall inform the competent Security Authority, which shall proceed with the formalities required in point 1 of Annex II.

3. The Security Authority of each Union institution and body shall be responsible for granting, suspending, withdrawing and renewing authorisations to access EUCI for their staff.

4. In exceptional circumstances, where duly justified in the interests of the service and pending completion of a full security investigation, the Security Authority of a Union institution or body may grant a temporary authorisation for individuals to access EUCI for a specific position, without prejudice to the provisions regarding renewal of authorisation to access EUCI and upon verification of the relevant National Security Authority.

5. Union institutions and bodies shall follow the procedures for managing authorisation to access EUCI set out in Annex II.

Article 25

Recognition of authorisations to access EUCI

1. An authorisation to access EUCI up to the specified level shall be valid in any Union institution or body to which the individual is assigned.

2. Union institutions and bodies shall accept authorisations to access EUCI granted by other Union institution or body.

3. Where the holder of an authorisation to access EUCI takes up employment in another Union institution or body, that Union institution or body shall notify the relevant NSA of a change of employer, through the competent Security Authority.

Article 26

EUCI briefings

1. The Security Authority of a Union institution or body shall brief all individuals who need to access EUCI on any threats to security and about their obligation to report any suspicious activity. The briefing shall take place before access to EUCI is granted and at least every 5 years thereafter.

2. After receiving the briefing referred to in paragraph 1, all individuals concerned shall acknowledge in writing that they have understood their obligations regarding the protection of EUCI and the consequences where EUCI is compromised.

3. The briefing referred to in paragraph 1 shall include the following information:

   (a) any individual who is responsible for a breach of the security rules laid down in this Regulation may be liable to disciplinary action in accordance with the applicable rules and regulations;

   (b) any individual who is responsible for compromising or losing EUCI may be liable to disciplinary or legal action in accordance with the applicable law, rules and regulations.

4. Where individuals who have been granted authorisations to access EUCI no longer require such access, Union institutions and bodies shall ensure that those individuals are aware of, and where appropriate acknowledge in writing, their obligations in respect of the continued protection of EUCI.

5. The task of creating and managing the EUCI briefings may be shared between Union institutions and bodies provided that their specific requirements are taken into account.

SECTION 3
PHYSICAL SECURITY

Article 27

Basic principles

1. Each Union institution and body shall determine the physical security measures appropriate to its sites, in accordance with Annex III and the principle of defence in depth, on the basis of a risk assessment performed by its Security Authority. The measures shall ensure the following objectives:

   (a) to deny access to EUCI or forced entry by an intruder;

   (b) to deter, impede and detect unauthorised actions and respond to security incidents as soon as possible;

   (c) to allow for segregation of personnel in their access to EUCI on a need-to-know basis and where appropriate, on a security clearance basis.

2. Union institutions and bodies shall put in place physical security measures for all sites where EUCI is discussed, stored or handled, including areas housing communication and information systems as referred to in Section 5 of this Chapter.

3. Only security equipment approved by the Security Authority of a Union institution or body shall be used for physically protecting information classified CONFIDENTIEL UE/EU CONFIDENTIAL or higher.

4. Union institutions and bodies may share Secured Areas, as referred to in Annex III, for handling and storing EUCI, upon conclusion of an agreement.

Article 28

Sub-group on physical security

1. The sub-group on physical security as referred to in Article 7(1), point (c), shall have the following roles and responsibilities:

   (a) preparing guidance documents relative to physical security matters;

   (b) defining the general security criteria for acquiring equipment such as security containers, shredding machines, door locks, electronic access control systems, intrusion detection systems and alarm systems for the physical protection of EUCI;

   (c) assisting Union institutions and bodies in determining the appropriate security measures for their sites;

   (d) proposing compensatory measures for the protection of EUCI when EUCI is handled outside the physically protected areas of a Union institution and body.,

Article 29

Physical protection of EUCI

1. To ensure the physical protection of EUCI, the Union institutions and bodies shall establish the following physically protected areas:

   (a) administrative areas, as referred to in Annex III;

   (b) where appropriate, Secured Areas including Class I, Class II and technically Secured Areas, as referred to in Annex III.

2. The Security Authority of the Union institution and body concerned shall conduct an internal inspection to verify whether the conditions for an area to be established as an Administrative Area or a Secured Area, set out in Annex III, are met. Where the inspection report indicates that the conditions are met, the Security Authority may issue an accreditation for the Secured Area to protect EUCI up to the stated level for a period not exceeding 5 years.

   The Security Authority of the Union institution or body concerned shall be responsible for carrying out the re-accreditation process of its Secured Areas, before the expiry of the accreditation or whenever changes have been implemented within the accredited area.

3. Each Union institution and body shall adopt procedures for managing keys and combination settings for offices, rooms, strong rooms and security containers for level CONFIDENTIEL UE/EU-CONFIDENTIAL and for higher levels.

4. The Security Authority may authorise entry and exit searches to deter and detect the unauthorised introduction of material or the unauthorised removal of EUCI from sites.

5. Union institutions and bodies shall establish the measures for the physical protection of the EUCI in accordance with Annex III.

SECTION 4
MANAGEMENT OF EUCI

Article 30

Basic principles

1. Union institutions and bodies shall record, file, preserve and eventually eliminate, sample or transfer their EUCI documents to the relevant archives in accordance with retention policy and rules specific to the files of each Union institution and body.

2. Any Union institution and body which is the originator of EUCI shall determine the security classification of that information upon its creation and in accordance with Article 18(1).

3. Union institutions and bodies shall clearly communicate the classification level to recipients, either by means of a classification marking or by an announcement, where the information is delivered in oral form.

4. The security measures applicable to the original document shall apply to drafts, copies and translations thereof.

5. Union institutions and bodies shall establish the measures for EUCI management in accordance with Annex IV.

Article 31

Creation of EUCI

2. Union institutions and bodies under whose authority EUCI is created shall ensure that the following requirements are met:

(a) each page shall be marked clearly with the classification level;

(b) each page shall be numbered;

(c) the document shall bear a reference number, where applicable a registration number and a subject, which is not itself EUCI, unless it is marked as such;

(d) the document shall include its date of creation;

(e) all the annexes and enclosures shall be listed, whenever possible on the first page;

(f) documents classified SECRET UE/EU SECRET or higher shall bear a copy number on every page, where they are to be distributed in multiple copies. Electronic copies that are distributed outside the holding system shall bear a unique identifier based on an electronic signature.

Article 32

Originator control

1. The Union institution or body under whose authority an EUCI document is created shall have originator control over that document. The originator shall determine the classification level of the document and shall be responsible for its initial dissemination. Without prejudice to Regulation 1049/2001, the originator's prior written consent shall be obtained before the information is:

   (a) declassified or downgraded;

   (b) used for purposes other than those established by the originator;

   (c) forwarded to any entity outside the Union institution or body holding the information, including a third country or international organisation, another Union institution or body, Member States, a contractor or prospective contractor, a beneficiary or prospective beneficiary;

   (d) copied and translated in case of TRES SECRET-UE/EU-TOP SECRET level.

2. Where the originator of an EUCI document cannot be identified, the Union institution or body holding that classified information shall exercise originator control.

3. Originators of any EUCI document shall keep a record of any classified sources used for producing classified documents, including details of sources originally from Member States, international organisations or third countries. Where appropriate, aggregated classified information shall be marked in such a way as to preserve the identification of the originators of the classified source materials used.

Article 33

Classification markings

1. Where appropriate, in addition to one of the security classification markings, EUCI documents may bear additional markings, such as distribution or releasability markings or to indicate the originator.

2. Different parts of a EUCI document may require different classifications and shall be marked accordingly. The overall classification level of a document or file shall be at least as high as that of its most highly classified component.

3. Documents containing parts with different classification levels shall be structured so that parts with a different classification level may be easily identified and detached if necessary.

Article 34

EUCI registry system

1. All Union institutions and bodies that handle and store information classified CONFIDENTIEL UE/EU CONFIDENTIEL or higher shall establish one or more EUCI registries to ensure its registration for security purposes when it arrives at or leaves a Union institution or body.

2. All EUCI registries shall be established in Secured Areas, as referred to in Annex III.

3. Union institutions and bodies shall assign a Registry Control Officer ('RCO') to manage each EUCI registry. The RCO shall have appropriate security clearance and shall be authorised in accordance with Article 24. Union institutions and bodies shall ensure the proper training for their RCO.

Article 35

Downgrading and declassifying

1. Information shall be classified only for as long as it requires protection. EUCI that no longer needs the original classification shall be downgraded to a lower level. EUCI that no longer needs to be considered as classified at all shall be declassified.
2. At the time of creation of EUCI, the originator shall indicate, where possible, and in particular for information classified RESTREINT UE/EU RESTRICTED, whether the EUCI can be downgraded or declassified on a given date or following a specific event.
3. The originating Union institution or body shall be responsible for deciding whether a EUCI document can be downgraded or declassified. It shall review the information and assess the risks regularly and at least every 5 years in order to determine whether the original classification level is still appropriate.
4. Union institutions and bodies holding EUCI of which they are not the originator shall not downgrade or declassify that document, nor shall they modify or remove any of the markings referred to in Article 18(1) without the prior written consent of the originator.
5. Union institutions and bodies may partially downgrade or declassify EUCI they create. In such cases a downgraded or declassified extract shall be produced.
6. Union institutions and bodies shall inform the recipient organisation of the EUCI of its downgrading or declassification.

Article 36

Markings on downgraded and declassified documents

1. Where Union institutions and bodies decide to declassify an EUCI document, consideration shall be given as to whether it is to bear a sensitive non-classified information distribution marking.
2. The original classification marking at the top and bottom of every page shall be visibly crossed out using the 'strikethrough' functionality for electronic formats, or manually for print-outs. The original classification marking shall not be removed.
3. The first page or the cover page shall be stamped as downgraded or declassified and completed with the details of the authority responsible for downgrading or declassifying and the corresponding date. Downgrading or declassification of electronic EUCI documents shall be evidenced by an electronic signature under the authority of the originator.

Article 37

Destruction and deletion of EUCI

1. Union institutions and bodies shall review EUCI, both on paper and in CISs, at least every 5 years to determine whether they are to be destroyed or deleted. Where EUCI is destroyed or deleted, they shall instruct anyone having previously received that EUCI.

2. Union institutions and bodies may destroy duplicates of EUCI which are no longer required, taking account of the relevant rules on document management for the originals.

3. Union institutions and bodies shall only destroy any hard copy of information classified CONFIDENTIEL UE/EU CONFIDENTIAL or higher by their Registry Control Officer. The RCO shall update the logbooks and other registration information accordingly, keeping essential metadata of the destroyed document.

   Documents classified SECRET UE/EU SECRET and higher shall only be destroyed by the RCO in the presence of a witness who shall have security clearance to at least the classification level of the document being destroyed.

4. The RCO and where applicable, the witness, shall sign a destruction certificate which shall be filed in the registry. The certificate shall be kept for at least 5 years in the case of information classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET-UE/EU-SECRET and for at least 10 years in the case of information classified at TRES SECRET-UE/EU-TOP SECRET level.

Article 38

Evacuation and destruction of EUCI in an emergency

1. Each Union institution and body shall develop emergency evacuation and destruction plans based on local conditions to safeguard EUCI that is at significant risk of falling into unauthorised hands.

   The operational details of emergency evacuation and destruction plans shall themselves be classified as RESTREINT UE/EU RESTRICTED.

2. In the event of an emergency, where there is an imminent risk of unauthorised disclosure of EUCI, Union institutions and bodies shall evacuate EUCI.

   Where evacuation is not possible, EUCI shall be destroyed in such a way that it cannot be reconstructed in whole or in part.

3. The originator and the originating registry shall be informed of the emergency evacuation or destruction of registered EUCI.

4. Where emergency plans have been activated, priority shall be given to evacuating or destroying the higher levels of EUCI first, including the enciphering equipment.

Article 39

Archiving

1. Union institutions and bodies shall decide whether and when to archive EUCI, and the corresponding practical measures, in accordance with their policy on document management.

2. EUCI documents shall not be transferred to the Historical Archives of the European Union.

SECTION 5
PROTECTION OF EUCI IN COMMUNICATION AND INFORMATION SYSTEMS (CISs)

Article 40

Sub-group on accreditation of communication and information systems handling and storing EUCI

The sub-group on accreditation of CISs handling and storing EUCI, as referred to in Article 7(1), point (d), shall have the following roles and responsibilities:

(a) assisting the Union institutions and bodies in their accreditation processes;

(b) recommending a standard for accreditation to be followed by all Union institutions and bodies;

(c) disseminating and sharing best practices and guidance regarding the accreditation of CISs.

Article 41

Communication and information systems

Union institutions and bodies shall meet the following requirements in relation with CISs handling and storing EUCI:

(a) the system owner or Information Assurance Operational Authority shall consult the Security Accreditation Authority before developing, procuring or enabling a CIS to handle and store EUCI in order to determine the requirements for accreditation;

(b) key security principles for the design of CIS handling and storing EUCI shall apply at the inception of the project, as part of the information security risk management process and taking into account need-to-know, minimal functionality, defence in depth, least privilege, segregation of duties and four eyes;

(c) the storage, central processing and network management components of a CIS handling and storing EUCI shall be installed in a Secured Area, as referred to in Annex III;

(d) implement 'TEMPEST security measures' which shall be commensurate with the risk of exploitation and the level of classification of the information;

(e) all staff involved in the operation of a CIS handling and storing EUCI shall notify to the Security Authority and the relevant system owner or Information Assurance Operational Authority any potential security weaknesses, incidents, breaches of security or system compromises that may have an impact on the protection of the CIS or the EUCI therein;

(f) where relevant, the Security Authority shall notify the Security Authorities of any other Union institutions and bodies concerned of potential security weaknesses or incidents that could affect their CISs handling and storing EUCI.

Article 42

Cryptographic products

1. Approved cryptographic products shall be used for transmission and storage of EUCI by electronic means. The list of approved cryptographic products shall be maintained by the Council, on the basis of input from the National Security Authorities.

2. Where the list referred to in paragraph 1 does not include any suitable product for the intended purpose, the Crypto Approval Authority of the Union institution or body concerned shall request an interim approval from the Council. Where possible, a cryptographic product that is approved by the National Security Authority of a Member State shall be selected.

   The Council shall take the necessary steps to ensure that a suitable product is added to the list.

3. Approvals of cryptographic products shall be valid for a maximum of 5 years and reviewed on a yearly basis thereafter.

4. The Council shall remove any cryptographic product from the list of approved cryptographic products for which national approval has been withdrawn or has expired.

5. The Coordination Group shall inform the Council on a yearly basis of any cryptographic products that it recommends for evaluation by a Crypto Authority Approval of a Member State on the basis of a survey carried out in the Union institutions and bodies.

Article 43

Accreditation of CISs handling and storing EUCI

1. By accrediting CISs handling and storing EUCI, Union institutions and bodies shall confirm that all appropriate security measures have been implemented and that a sufficient level of protection of EUCI and of the CIS has been achieved in accordance with this Regulation.

2. The CIS owner or the Information Assurance Operational Authority shall be responsible for the preparation of the accreditation files and documentation, including manuals for different types of users.

3. The Security Accreditation Authority of each Union institution and body shall be responsible for establishing an accreditation process with clear conditions that need approval, for all CISs under their authority.

4. Where a CIS handling and storing EUCI involve both Union institutions and bodies and National Security Authorities, the Union institutions and bodies concerned shall establish, through further implementing rules adopted pursuant to Article 8(2), a joint Security Accreditation Board in charge of the system's accreditation. That Board shall be composed of Security Accreditation Authority representatives of the parties involved and shall be chaired by the Security Accreditation Authority of the Union institution or body that owns the CIS.

Article 44

Accreditation process of a CIS handling and storing EUCI

1. All CISs handling and storing EUCI shall undergo an accreditation process, based upon the principles of information assurance, the level of detail of which shall be commensurate with the level of protection required.

2. The accreditation process shall result in an accreditation statement determining the maximum classification level of the information that may be handled and stored in a CIS as well as the corresponding terms and conditions. The accreditation statement shall be based on the formal validation of the risk assessment and of the security measures implemented for the CIS concerned, providing assurance on the following elements:

   (a) the information security risk management process has been properly carried out;

   (b) the system owner or risk owner has knowingly accepted the residual risk;

   (c) a sufficient level of protection of the CIS, and of the EUCI handled and stored in it, has been achieved in accordance with this Regulation.

3. The Security Accreditation Authority of a Union institution or body shall formally validate the accreditation statement. Upon successful validation, the Security Accreditation Authority shall issue an approval to operate which determines the maximum classification level of the EUCI that may be handled in the CIS as well as the corresponding terms and conditions for operation. The approval shall be issued for a specified period. Where one or more of the required security measures are not in place but this does not significantly impact the overall security, an interim approval to operate may be issued, specifying the points for remediation.

4. At any moment in the life cycle of a CIS, the Security Accreditation Authority of the Union institution or body concerned may take the following actions:

   (a) apply an accreditation process;

   (b) audit or inspect the CIS;

   (c) where the conditions for operation are no longer satisfied, such as when a security incident has revealed a significant vulnerability in the CIS, require the establishment and effective implementation of a security improvement plan within a well-defined timescale, potentially withdrawing permission to operate the CIS until the conditions for operation are satisfied.

5. The system owner or the Information Assurance Operational Authority shall make a formal report to the Security Accreditation Authority annually during the period of validity of an approval to operate, including a summary of any significant incidents, changes and risk factors.

Article 45

Emergency circumstances

1. Union institutions and bodies may apply specific procedures to transmit or store classified EUCI in an emergency, such as during impending or actual crises, conflicts, war situations or in exceptional operational circumstances, after approval by their Crypto Approval Authority.

2. Under the circumstances referred to in paragraph 1, EUCI may be transmitted using cryptographic products which have been approved for a lower classification level or without encryption with the consent of the competent authority where any delay would cause harm clearly outweighing the harm entailed by any disclosure of the classified material and subject to the following conditions:

   (a) the sender or the recipient do not have the required encryption facility;

   (b) the classified material cannot be conveyed in time by other means.

3. Classified information transmitted in accordance to in paragraph 2 shall not bear any markings or indications distinguishing it from information which is unclassified or which can be protected by an available cryptographic product. Recipients shall be notified of the classification level, without delay, by other means.

4. A subsequent report on the transmission of EUCI under the circumstances referred to in paragraph 1 shall be submitted to the relevant Security Authority.

SECTION 6
INDUSTRIAL SECURITY

Article 46

Basic principles

1. Each Union institution or body, as contracting or granting authority, shall ensure that the minimum standards on industrial security set out in this Section and the conditions for the protection of EUCI in classified contracts and grant agreements set out in Annex V, are referred to or incorporated in the contracts or grant agreements and complied with when awarding classified contracts or grant agreements.

2. Industrial security is the application of measures to ensure the protection of EUCI by the following individuals or entities:

   (a) under direct management[30], within the framework of classified contracts, by:

      (i) candidates or tenderers throughout the tendering and contracting procedure;

      (ii) contractors or subcontractors throughout the life-cycle of classified contracts;

   (b) under direct management[31], within the framework of classified grant agreements, by

      (i) applicants during grant award procedures;

      (ii) beneficiaries or subcontractors throughout the life-cycle of classified grant agreements.

   (c) under indirect management, within the framework of financial framework partnership agreements (‘FFPA’) and the related contribution agreements by the entrusted entities throughout the life cycle of these agreements.

3. As the entrusting entity, the Union institution or body shall describe the specific security requirements for the entrusted entity in the security chapter of the FFPA and

30 Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council.

31 Idem

the related contribution agreements. These requirements shall be based on the security principles and provisions as contained in this Regulation in relation to classified contracts and grant agreements, which apply mutatis mutandis.

4. Classified contracts and classified grant agreements shall not involve information classified TRES SECRET UE/EU TOP SECRET.

5. Provisions in this Chapter referring to classified contracts or contractors, or to classified grants or beneficiaries, shall also apply to classified subcontracts or subcontractors within the meaning of, respectively, classified contracts or grants.

6. Union institutions and bodies, as contracting or granting authorities, shall closely cooperate with the security authorities or any other competent authorities of the country on whose territory the contractual party or the grant recipient is registered, as well as with the security or any other competent authorities of the contracted or grant awarded international organisation.

7. Union institutions and bodies, as contracting or granting authorities, shall communicate with the security authorities or any other competent authorities through their Security Authorities.

8. Union institutions and bodies, as contracting or granting authorities, shall notify the authorities referred to in paragraph 6, through its Security Authority, whenever a classified contract or grant agreement has been signed.

The notification shall include relevant data such as the names of the contractor or beneficiaries, the duration of the classified contract or grant agreement, and the maximum level of classification.

Union institutions and bodies, as contracting or granting authorities, shall also notify the authorities referred to in paragraph 6 whenever classified contracts or grant agreements are prematurely terminated.

9. Union institutions and bodies, as contracting or granting authorities, may award classified contracts or classified parts of grants only to entities registered in those third countries or established by those international organisations that have concluded a security of information agreement with the Union. Where the EUCI concerned contains personal data, any transfer of the latter to a third country or international organisation shall be made in accordance with Regulation (EU) 2018/1725.

Article 47

Security elements in a classified contract or grant agreement

1. Classified contracts or grant agreements shall include the following security elements:

(a) security classification guide;

(b) security aspects letter.

2. Classified contracts or grant agreements may include a Programme or Project Security Instruction.

Article 48

Security Classification Guide

1. Before signing a classified contract or grant agreement, the Union institution or body, as contracting or granting authority, shall determine the security classification of any information to be created by contractors or beneficiaries, or by their sub-contractors. For that purpose, it shall prepare a Security Classification Guide to be used for the performance of the classified contract or grant agreement.

2. The Security Classification Guide may be modified throughout the life of the programme or project, as referred to in Article 50, contract or grant agreement and the elements of information may be re-classified or downgraded.

3. In order to determine the security classification of the various elements of a classified contract or grant agreement, the following principles shall apply:

   (a) in preparing a Security Classification Guide, the Union institution or body, as contracting or granting authority, shall take into account all relevant security aspects, including the security classification assigned to information provided and approved to be used for the classified contract or grant agreement by the originator of the information;

   (b) the overall level of classification of the classified contract or grant shall not be lower than the highest classification of any of its elements;

   (c) where relevant, the Union institution or body concerned, as contracting or granting authority, shall liaise, through their Security Authority, with the security authorities or any other competent authorities of the country concerned where making any changes to the Security Classification Guide.

Article 49

Security Aspects Letter

1. Each Union institution or body, as contracting or granting authority, shall describe the specific security requirements of the classified contract or grant in a Security Aspect Letter. That letter shall include the Security Classification Guide and shall be an integral part of a classified contract, grant agreement or sub-contract.

2. The Security Aspect Letter shall contain provisions requiring the contractor or beneficiary, and their subcontractors, to comply with the provisions laid down in this Regulation and any further implementing rules adopted pursuant to Article 8(2) regarding industrial security. The Security Aspect Letter shall clearly indicate that non-compliance with such provisions may constitute sufficient grounds for the termination of the classified contract or grant agreement.

Article 50

Programme or Project Security Instruction

1. Union institutions and bodies, as contracting or granting authorities, may develop a Programme or Project Security Instruction, in close cooperation with their Security Authorities, in particular for programmes and projects characterised by their considerable scope, scale or complexity, or by the multitude or the diversity of contractors, beneficiaries and other partners and stakeholders involved.

2. The Security Authority of each Union institution or body, as contracting or granting authority, shall submit the specific Programme or Project Security Instruction for

advice to the relevant Member State advisory security body consisting of their National Security Authorities and/or Designated Security Authorities.

When a Union institution or body does not have such an advisory body, the Programme or Project Security Instruction shall be submitted to the Information Security Committee, referred to in Article 6(8).

SECTION 7
SHARING EUCI AND EXCHANGING CLASSIFIED INFORMATION

Article 51

Basic principles

1. All Union institutions and bodies may share EUCI with other Union institutions or bodies under the conditions set out in Article 54.

2. Union institutions and bodies may share EUCI with Member States and the European Atomic Energy Community provided that they protect that information in accordance with the corresponding classification marking laid down in the Agreement between the Member States of the Union, meeting within the Council, regarding the protection of classified information exchanged in the interests of the Union and the corresponding table set out in Annex VI to this Regulation.

3. Union institutions and bodies shall only exchange classified information with third countries or international organisations with which a Security of information agreement or an administrative arrangement has been concluded in accordance with Articles 55 and 56.

   Such agreements and arrangements shall contain provisions to ensure that third countries or international organisations receiving EUCI protect such information at a level commensurate with its classification level and corresponding to minimum standards that are no less stringent than those laid down in this Regulation.

4. Where there is no Security of information agreement or administrative arrangement in place, a Union institution or body may, in exceptional circumstances, release EUCI to another Union institution or body, a third country or an international organisation in accordance with Article 58.

5. Union institutions and bodies shall designate those registries that serve as the main points of entry and exit for EUCI shared with other Union institutions or bodies or classified information exchanged with third countries and international organisations.

Article 52

Sub-group on EUCI sharing and exchange of classified information

1. The sub-group on EUCI sharing and exchange of classified information, referred to in Article 7(1), point (e), shall have the following roles and responsibilities:

   (a) organising assessment visits to Union institutions and bodies, third countries and international organisations and adoption of the yearly programme of visits;

   (b) preparing and carrying out of the assessment visits;

   (c) drawing up a report on the outcome of the visits referred to in point (a).

except in cases referred to in Article 56(2).

2. The sub-group on EUCI sharing and exchange of classified information shall be composed of representatives from the Commission, the Council and the European External Action Service and shall work by consensus.

Article 53

Assessment visits related to EUCI sharing

1. The sub-group on EUCI sharing and exchange of classified information shall carry out assessment visits in full cooperation with the officials of the Union institution or body being visited. It may seek assistance from the NSA on whose territory the Union institution or body is located.

2. The assessment visits to the Union institutions and bodies concerned shall serve the following purposes:

   (a) to check whether the requirements for protecting EUCI laid down in this Regulation are complied with and therefore, whether the measures implemented are effective;

   (b) to emphasise the importance of security and effective risk management within the organisation visited;

   (c) to recommend countermeasures to mitigate the specific impact of loss of availability, confidentiality or integrity of classified information;

   (d) to reinforce security authorities' ongoing security education and awareness programmes.

3. At the end of the assessment visit, the sub-group on EUCI sharing and exchange of classified information shall carry out the following tasks:

   (a) draw up a report with the main conclusions of the assessment;

   (b) seek the opinion of the Information Security Committee, referred to in Article 6(8), on the report;

   (c) send the report for follow up to the security authority of the Union institution or body visited.

4. Where the report proposes any corrective action or makes recommendations, a follow-up visit shall be organised for the purpose of verifying whether such action was taken or recommendations followed.

Article 54

Sharing EUCI

1. A Union institution or body may share EUCI with another Union institution or body where the following conditions are fulfilled:

   (a) there is a proven need for the exchange;

   (b) an assessment visit has been carried out at the Union institution or body concerned, in accordance with Article 53, the outcome of which certifies the capacity of that Union institution or body to handle and store a specified level of EUCI;

(c) the Security Authority of the Union institution or body concerned decides that it may share information classified up to a specified level with other such certified Union institutions and bodies.

2. The secretariat of the Coordination Group shall establish a list of EUCI levels that may be handled and stored by each Union institution and body fulfilling the conditions in paragraph 1, points (b) and (c). It shall regularly update that list.

Article 55

Security of information agreements

1. Where it is necessary to exchange classified information with a third country or an international organisation on a long term basis, the competent institution or body shall seek to negotiate and conclude a security of information agreement, in accordance with Article 218 of the Treaty on the Functioning of the European Union.

2. A security of information agreement shall establish the basic principles and the minimum standards governing the exchange of classified information between the Union and a third country or international organisation.

3. Security of information agreements shall provide for technical implementing arrangements to be agreed between the competent security authorities of the relevant Union institutions and bodies and the competent security authority of the third country or international organisation concerned.

4. Prior to the approval of the technical implementing arrangements, referred to in paragraph 3, the sub-group on EUCI sharing and exchange of classified information shall carry out an assessment visit in accordance with Article 57.

Article 56

Administrative arrangements with third countries and international organisations

1. Where their rules of procedure or founding acts provide for such possibility, Union institutions and bodies may enter into an administrative arrangement with their counterparts in a third country or international organisation, after informing the EUCI sharing and exchange of classified information sub-group, where the following conditions are met:

   (a) the Union institution or body concerned needs to exchange, on a long-term basis information classified, as a general rule, no higher than RESTREINT UE/EU RESTRICTED with its counterpart in a third country or international organisation;

   (b) the Union institution or body concerned satisfies the conditions set out in Article 54(1);

   (c) the report of the assessment visit, referred to in Article 57, certifies that the relevant counterpart in the third country or international organisation concerned has the capacity to handle and store a specified level of EUCI.

2. Before concluding an administrative arrangement, an assessment visit shall be conducted in accordance with the principles in Article 57. The Union institution or body seeking the administrative arrangement may request the Subgroup on EUCI sharing to conduct the assessment visit on its behalf or to participate in the visit.

3. The Security Authority of the Union institution or body seeking the administrative arrangement shall decide on any specific conditions governing the exchange as well as on the maximum level of EUCI which may be exchanged. That level shall not be higher than the level set for sharing EUCI with other Union institutions and bodies, in accordance with Article 54, and, where applicable, should not be higher than that provided for under a Security of Information Agreement with the same third country or international organisation.

Article 57

Assessment visits for the exchange of classified information with third countries and international organisations

1. An assessment visit to a third country or international organisation shall be conducted to determine whether an Union institution or body may exchange classified information with the third country or international organisation concerned.

2. The aim of the assessment visit shall be to assess the effectiveness of the security rules and procedures in the third country or international organisation concerned as regards the protection of EUCI at a given level. The assessment visit shall be carried out in mutual agreement with the third country or international organisation concerned.

3. The assessment visits shall evaluate at least the following:

   (a) the regulatory framework applicable for protecting classified information and its adequacy for the protection of EUCI at a given level;

   (b) any specific features of the security policy and the way in which security is organised in the third country or international organisation which may have an impact on the level of classified information that may be exchanged;

   (c) the security measures and procedures actually in place;

   (d) security clearance procedures relative to the EUCI level to be released.

4. The Information Security Committee referred to in Article 6(8) shall receive a report on the findings of such visits before the EUCI is actually released to the third country or international organisation concerned. Where relevant, the report shall also be shared with the Union institution or body concerned.

5. The security authorities of the Union institution or body concerned shall communicate to the third country or international organisation the date as from when it is in a position to exchange EUCI, as well as the maximum level of EUCI which may be exchanged in hard copy or by electronic means.

6. Follow-up visits shall be organised where the following conditions are met:

   (a) it is necessary to raise the level of EUCI which may be exchanged;

   (b) the Union institution or body concerned has been notified of fundamental changes in the security arrangements of the third country or international organisation that might have an impact on how EUCI is protected;

   (c) there has been a serious security information incident involving unauthorised disclosure of EUCI.

Article 58

Exceptional ad-hoc release of EUCI

1. In the absence of a security of information agreement or an administrative arrangement, where a Union institution or body determines that there is an exceptional need to release EUCI to another Union institution or body or to a third country or international organisation, or

   where a security of information agreement or an administrative arrangement has been concluded and a Union institution or body determines that there is an exceptional need to release a higher level of EUCI than already stipulated under the agreement or arrangement, the Union institution or body providing EUCI shall take the following steps:

   (a) to the extent possible, verify with the security authorities of the third country, international organisation or receiving Union institution or body that their security rules, structures and procedures can ensure the protection of EUCI released to standards no less stringent than those set in this Regulation;

   (b) seek an opinion from the Information Security Committee, referred to in Article 6(8), on the basis of the verification made pursuant to point (a), unless operational circumstances require an immediate ad-hoc release, in which case the Information Security Committee shall be subsequently informed.

2. All documents released pursuant to this Article shall bear a releasability marking indicating the third country, international organisation or Union institution or body to which it has been released.

3. Prior to or upon actual release, the Union institution or body providing EUCI shall seek a written undertaking from the receiving party that it will protect the EUCI it receives. Where applicable, it shall be requested to undertake to protect the EUCI in accordance with the basic principles and the minimum standards set out in this Regulation.

Chapter 6
Final provisions

Article 59

Implementation

1. The Coordination Group shall establish information security guidance for implementing this Regulation.

2. Based on their specific needs, Union institutions and bodies may adopt internal rules for the purpose of implementing this Regulation, in accordance with Article 8(2).

Article 60

Transitional provisions

1. The internal rules on information security adopted by individual Union institution or body before ¨[dd/mm/yyyy date of application] shall be reviewed by [3 years after the entry into force of this Regulation] at the latest.

2. All Union institutions and bodies that have been assessed either by Commission or Council or EEAS before the [dd/mm/yyyy date of applicability], as suitable to handle and store EUCI, shall be considered as meeting the conditions referred to in Article 19(1).

3. Any administrative arrangement concluded by the Union institutions and bodies with third countries and international organisations before [dd/mm/yyyy date of application] shall remain valid.

4. Where the Member States on whose territory the beneficiaries of the Commission grant agreement under the European Defence Industrial Development Programme have decided to have a specific security framework for the protection and handling of nationally classified information relating to the grant agreement concerned, the Commission, when applying industrial security procedures contained in this Regulation, will respect this security framework until the end of life cycle of the grant agreement.

Article 61

Monitoring and evaluation

1. By [dd/mm/yyyy 3 years after the date of application] at the latest, the Commission shall present a report on the implementation of this Regulation to the European Parliament and the Council.

2. No sooner than [5 years after the date of application] and every 5 years thereafter, the Commission shall carry out an evaluation of this Regulation and present a report on the main findings to the European Parliament and the Council.

Article 62

Entry into force and application

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

2. It shall apply from [date: the first day of the month following the period of 2 years after the date of entry into force]

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*
[...]	*[...]*

LEGISLATIVE FINANCIAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

1.2. Policy area(s) concerned

1.3. The proposal/initiative relates to:

1.4. Objective(s)

1.4.1. General objective(s)

1.4.2. Specific objective(s)

1.4.3. Expected result(s) and impact

1.4.4. Indicators of performance

1.5. Grounds for the proposal/initiative

1.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative

1.5.2. Added value of Union involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this point 'added value of Union involvement' is the value resulting from Union intervention which is additional to the value that would have been otherwise created by Member States alone.

1.5.3. Lessons learned from similar experiences in the past

1.5.4. Compatibility with the Multiannual Financial Framework and possible synergies with other appropriate instruments

1.5.5. Assessment of the different available financing options, including scope for redeployment

1.6. Duration and financial impact of the proposal/initiative

1.7. Management mode(s) planned

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

2.2. Management and control system(s)

2.2.1. Justification of the management mode(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed

2.2.2. Information concerning the risks identified and the internal control system(s) set up to mitigate them

2.2.3. Estimation and justification of the cost-effectiveness of the controls (ratio of "control costs ÷ value of the related funds managed"), and assessment of the expected levels of risk of error (at payment & at closure)

2.3. Measures to prevent fraud and irregularities

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

3.2. Estimated financial impact of the proposal on appropriations

3.2.1. Summary of estimated impact on operational appropriations

3.2.2. Estimated output funded with operational appropriations

3.2.3. Summary of estimated impact on administrative appropriations

3.2.4. Compatibility with the current multiannual financial framework

3.2.5. Third-party contributions

3.3. Estimated impact on revenue

LEGISLATIVE FINANCIAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on information security in the institutions, bodies, offices and agencies of the Union

1.2. Policy area(s) concerned

European public administration

The information security rules of Union institutions and bodies should together constitute a comprehensive and coherent general framework within the European administration for protecting information, and should ensure equivalence of basic principles and minimum standards. The level of protection afforded to information should also be equivalent across all Union institutions and bodies.

1.3. The proposal/initiative relates to:

☑a new action

☐ a new action following a pilot project/preparatory action[32]

☐ the extension of an existing action

☐ a merger or redirection of one or more actions towards another/a new action

1.4. Objective(s)

1.4.1. General objective(s)

The general objective of the initiative is to create information security rules for all Union institutions and bodies with the aim to ensuring an enhanced and consistent protection against the evolving threats to their information.

1.4.2. Specific objective(s)

• SO 1: Establish harmonised and comprehensive categories of information, as well as common handling requirements for all information handled by the European administration, and facilitate secure information exchange between the Union institutions and bodies, while minimising the impact on Member States.

• SO 2: Ensure that all Union institutions and bodies identify any security gaps in their processes and implement the measures required to ensure a level playing field of information security.

• SO 3: Establish a lean cooperation scheme on information security between Union institutions and bodies able to foster a coherent information security culture across the European administration.

• SO 4: Modernise the information security policies at all levels of classification/categorization, for all Union institutions and bodies, taking into account the digital transformation and the development of teleworking as a structural practice.

[32] As referred to in Article 58(2)(a) or (b) of the Financial Regulation.

1.4.3. Expected result(s) and impact

Specify the effects which the proposal/initiative should have on the beneficiaries/groups targeted.

The proposal will have the following effects on the Union institutions and bodies:

- Review of their internal rules and procedures with the aim to adapting to the Regulation;
- Categorize all information handled in line with the scheme provided by the Regulation;
- Ensure that their communication and information systems are complaint with the requirements laid down in the Regulation;
- Participate in the Interinstitutional Information Security Coordination Group ('Coordination Group').

The Member States will benefit from this Regulation as cooperation with Union institutions and bodies in all relevant fields (personnel security, industrial security or information sharing) would be based on same concepts, rules and procedures.

1.4.4. Indicators of performance

Specify the indicators for monitoring progress and achievements.

Indicators relevant for Specific objective no 1

- Adoption of suitable guidelines
- Implementation of new markings
- Publication of updated handling instructions for all categories of information
- Implementation of common systems handling sensitive non-classified information and EUCI

Indicators relevant for Specific objective no 2

- Number of recommendations made / implemented
- Number of information leaks across institutions and bodies

Indicators relevant for Specific objective no 3

- Statistics on centralised versus local procurement
- Inspection reports
- Number of queries dealt with by the Secretariat of the Information security coordination group

Indicators relevant for Specific objective no 4

- Number of users undergoing training
- Level of awareness of staff for the information security rules
- Percentage of staff enabled to work with secure teleworking equipment

1.5. Grounds for the proposal/initiative

1.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative

The implementation of this initiative will follow a phased approach as follows:

- 2022/2023: adoption of the Regulation, enter into force
- 2024/2025: review by all Union institutions and bodies of their internal rules on information security with the aim of adjusting them to the Regulation
- 2025: organisational work for the set-up of the Coordination Group and its Secretariat, as well as of the technical sub-groups
- 2024/2025: start of application for the Regulation
- 2025/2026: adoption of Rules of procedure for the Coordination group and the technical sub-groups
- 2026-2028: work on guidance documents as support for the implementation of the Regulation, exchange of best practices across institutions and bodies
- 2029/2030: preparation of first evaluation of the Regulation (every 5 years from the date of application)
- 2030: first evaluation of the Regulation

1.5.2. Added value of Union involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this point 'added value of Union involvement' is the value resulting from Union intervention which is additional to the value that would have been otherwise created by Member States alone.

The initiative contributes to ensuring that the Union institutions and bodies are assisted in their mission by an open, efficient and independent administration.

It adds to the general national efforts of Member States in the area of EU security by protecting the institutions and bodies from external interferences and spying activities.

1.5.3. Lessons learned from similar experiences in the past

N/A

1.5.4. Compatibility with the Multiannual Financial Framework and possible synergies with other appropriate instruments

The project requires the reallocation/assignment of 2FTEs for the Secretariat of the Information Security coordination group.

Other projects, such as the development of common tools and the centralisation of some activities is already partly ongoing and covered by SLAs and framework contracts.

1.5.5. Assessment of the different available financing options, including scope for redeployment

See previous section.

1.6. Duration and financial impact of the proposal/initiative

☐ **limited duration**

– ☐ in effect from [DD/MM]YYYY to [DD/MM]YYYY

– ☐ Financial impact from YYYY to YYYY for commitment appropriations and from YYYY to YYYY for payment appropriations.

– ☑ **unlimited duration**

1.7. Management mode(s) planned[33]

☑ **Direct management** by the Commission and by each Union institution and body

– ☑ by its departments, including by its staff in the Union delegations

– ☐ by the executive agencies

☐ **Shared management** with the Member States

☐ **Indirect management** by entrusting budget implementation tasks to:

– ☐ third countries or the bodies they have designated;

– ☐ international organisations and their agencies (to be specified);

– ☐ the EIB and the European Investment Fund;

– ☐ bodies referred to in Articles 70 and 71 of the Financial Regulation;

– ☐ public law bodies;

– ☐ bodies governed by private law with a public service mission to the extent that they are provided with adequate financial guarantees;

– ☐ bodies governed by the private law of a Member State that are entrusted with the implementation of a public-private partnership and that are provided with adequate financial guarantees;

– ☐ persons entrusted with the implementation of specific actions in the CFSP pursuant to Title V of the TEU, and identified in the relevant basic act.

– *If more than one management mode is indicated, please provide details in the 'Comments' section.*

Comments

[33] Details of management modes and references to the Financial Regulation may be found on the BudgWeb site: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

Specify frequency and conditions.

Every 5 years the Regulation will be evaluated and the Commission will report on its findings to the Council and the European Parliament.

2.2. Management and control system(s)

2.2.1. Justification of the management mode(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed

The Regulation lays down rules on information security applicable to all Union institutions and bodies. Monitoring of its proper implementation will take place through a coordination group involving all the security authorities of the institutions and bodies. Full responsibility for security remains in the hand of the security authority of each institution or body, and subject to the existing internal control framework of each institution or body.

2.2.2. Information concerning the risks identified and the internal control system(s) set up to mitigate them

The Regulation will create a baseline of information security rules and ensure transparency of security measures for information exchanges between Union institutions and bodies, it will thus reduce the information security related risks across the board. The Regulation is compliant with the Internal Control Standards, and includes a risk-based approach for policy-making.

2.2.3. Estimation and justification of the cost-effectiveness of the controls (ratio of "control costs ÷ value of the related funds managed"), and assessment of the expected levels of risk of error (at payment & at closure)

The existing control mechanisms for the institutions and bodies will be applicable. Compliance with the Regulation and information security related risks should be reported in institutions' and bodies' annual risk reporting.

2.3. Measures to prevent fraud and irregularities

Specify existing or envisaged prevention and protection measures, e.g. from the Anti-Fraud Strategy.

N/A

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

- Existing budget lines

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./Non-diff.[34]	from EFTA countries [35]	from candidate countries[36]	from third countries	within the meaning of Article 21(2)(b) of the Financial Regulation
H7	20 01 02 01	Non-diff.	NO	NO	NO	NO

- New budget lines requested

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./Non-diff.	from EFTA countries	from candidate countries	from third countries	within the meaning of Article 21(2)(b) of the Financial Regulation
	None		YES/NO	YES/NO	YES/NO	YES/NO

34 Diff. = Differentiated appropriations / Non-diff. = Non-differentiated appropriations.
35 EFTA: European Free Trade Association.
36 Candidate countries and, where applicable, potential candidates from the Western Balkans.

3.2. Estimated financial impact of the proposal on appropriations

3.2.1. Summary of estimated impact on operational appropriations

– ☑ The proposal/initiative does not require the use of operational appropriations

– ☐ The proposal/initiative requires the use of operational appropriations, as explained below:

EUR million (to three decimal places)

Heading of multiannual financial framework	Number	

DG: <…….>			Year **N**[37]	Year **N+1**	Year **N+2**	Year **N+3**	Enter as many years as necessary to show the duration of the impact (see point 1.6)			**TOTAL**
• Operational appropriations										
Budget line[38]	Commitments	(1a)								
	Payments	(2a)								
Budget line	Commitments	(1b)								
	Payments	(2b)								
Appropriations of an administrative nature financed from the envelope of specific programmes[39]										
Budget line		(3)								
TOTAL appropriations for DG <…….>	Commitments	=1a+1b +3								
	Payments	=2a+2b +3								

37 Year N is the year in which implementation of the proposal/initiative starts. Please replace "N" by the expected first year of implementation (for instance: 2021). The same for the following years.

38 According to the official budget nomenclature.

39 Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former 'BA' lines), indirect research, direct research.

• TOTAL operational appropriations	Commitments	(4)								
	Payments	(5)								
• TOTAL appropriations of an administrative nature financed from the envelope for specific programmes		(6)								
TOTAL appropriations under HEADING <….> of the multiannual financial framework	Commitments	=4+ 6								
	Payments	=5+ 6								

If more than one operational heading is affected by the proposal / initiative, repeat the section above:

• TOTAL operational appropriations (all operational headings)	Commitments	(4)								
	Payments	(5)								
TOTAL appropriations of an administrative nature financed from the envelope for specific programmes (all operational headings)		(6)								
TOTAL appropriations under HEADINGS 1 to 6 of the multiannual financial framework (Reference amount)	Commitments	=4+ 6								
	Payments	=5+ 6								

Heading of multiannual financial framework	7	'Administrative expenditure'

This section should be filled in using the 'budget data of an administrative nature' to be firstly introduced in the Annex to the Legislative Financial Statement (Annex V to the internal rules), which is uploaded to DECIDE for interservice consultation purposes.

EUR million (to three decimal places)

		Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL**
DG: HR							
• Human resources		0.314	0.314	0.314	0.314	0.314	**1.570**
• Other administrative expenditure							
TOTAL DG <…….>	Appropriations	0.314	0.314	0.314	0.314	0.314	**1.570**

TOTAL appropriations under HEADING 7 of the multiannual financial framework	(Total commitments = Total payments)	0.314	0.314	0.314	0.314	0.314	**1.570**

EUR (to three decimal places)

		Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL**
TOTAL appropriations under HEADINGS 1 to 7 of the multiannual financial framework	Commitments	0.314	0.314	0.314	0.314	0.314	**1.570**
	Payments	0.314	0.314	0.314	0.314	0.314	**1.570**

3.2.2. Estimated output funded with operational appropriations

Commitment appropriations in EUR million (to three decimal places)

Indicate objectives and outputs ⇩			Year **N**		Year **N+1**		Year **N+2**		Year **N+3**		Enter as many years as necessary to show the duration of the impact (see point 1.6)						**TOTAL**	
	OUTPUTS																	
	Type[40]	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 1[41]…																		
- Output																		
- Output																		
- Output																		
Subtotal for specific objective No 1																		
SPECIFIC OBJECTIVE No 2 ...																		
- Output																		
Subtotal for specific objective No 2																		
TOTALS																		

40 Outputs are products and services to be supplied (e.g.: number of student exchanges financed, number of km of roads built, etc.).

41 As described in point 1.4.2. 'Specific objective(s)…'

3.2.3. *Summary of estimated impact on administrative appropriations*

– ☐ The proposal/initiative does not require the use of appropriations of an administrative nature

– ☑ The proposal/initiative requires the use of appropriations of an administrative nature, as explained below:

EUR million (to three decimal places)

	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL**
HEADING 7 of the multiannual financial framework						
Human resources	0.314	0.314	0.314	0.314	0.314	**1.570**
Other administrative expenditure						
Subtotal HEADING 7 of the multiannual financial framework	0.314	0.314	0.314	0.314	0.314	**1.570**

Outside HEADING 7[42] of the multiannual financial framework						
Human resources						
Other expenditure of an administrative nature						
Subtotal outside HEADING 7 of the multiannual financial framework						

TOTAL	0.314	0.314	0.314	0.314	0.314	**1.570**

The appropriations required for human resources and other expenditure of an administrative nature will be met by appropriations from the DG that are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

[42] Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former 'BA' lines), indirect research, direct research.

3.2.3.1. Estimated requirements of human resources

– ☐ The proposal/initiative does not require the use of human resources.

– ☑ The proposal/initiative requires the use of human resources, as explained below:

Estimate to be expressed in full time equivalent units

		Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**
20 01 02 01 (Headquarters and Commission's Representation Offices)		2	2	2	2	2
20 01 02 03 (Delegations)						
01 01 01 01 (Indirect research)						
01 01 01 11 (Direct research)						
Other budget lines (specify)						
20 02 01 (AC, END, INT from the 'global envelope')						
20 02 03 (AC, AL, END, INT and JPD in the delegations)						
XX 01 xx **yy zz** [43]	- at Headquarters					
	- in Delegations					
01 01 01 02 (AC, END, INT - Indirect research)						
01 01 01 12 (AC, END, INT - Direct research)						
Other budget lines (specify)						
TOTAL		**2**	**2**	**2**	**2**	**2**

XX is the policy area or budget title concerned.

The human resources required will be met by staff from the DG who are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

Description of tasks to be carried out:

Officials and temporary staff	Secretariat of the information security coordination group: 1 AD official + 1 AST official
External staff	

[43] Sub-ceiling for external staff covered by operational appropriations (former 'BA' lines).

3.2.4. Compatibility with the current multiannual financial framework

The proposal/initiative:

– ☑ can be fully financed through redeployment within the relevant heading of the Multiannual Financial Framework (MFF).

The proposal requires allocating two staffs to the permanent secretariat of the Interinstitutional Coordination Group, located in HR.DS.

– ☐ requires use of the unallocated margin under the relevant heading of the MFF and/or use of the special instruments as defined in the MFF Regulation.

Explain what is required, specifying the headings and budget lines concerned, the corresponding amounts, and the instruments proposed to be used.

– ☐ requires a revision of the MFF.

Explain what is required, specifying the headings and budget lines concerned and the corresponding amounts.

3.2.5. Third-party contributions

The proposal/initiative:

– ☑ does not provide for co-financing by third parties

– ☐ provides for the co-financing by third parties estimated below:

Appropriations in EUR million (to three decimal places)

	Year **N**[44]	Year **N+1**	Year **N+2**	Year **N+3**	Total
Specify the co-financing body					
TOTAL appropriations co-financed					

Remark: the proposal will intensify current cooperations on information security through SLAs.

[44] Year N is the year in which implementation of the proposal/initiative starts. Please replace "N" by the expected first year of implementation (for instance: 2021). The same for the following years.

3.3. Estimated impact on revenue

– ☑ The proposal/initiative has no financial impact on revenue.

– ☐ The proposal/initiative has the following financial impact:

☐ on own resources

☐ on other revenue

please indicate, if the revenue is assigned to expenditure lines ☐

EUR million (to three decimal places)

Budget revenue line:	Appropriations available for the current financial year	Impact of the proposal/initiative[45]			
		Year **N**	Year **N+1**	Year **N+2**	Year **N+3**

For assigned revenue, specify the budget expenditure line(s) affected.

Other remarks (e.g. method/formula used for calculating the impact on revenue or any other information).

[45] As regards traditional own resources (customs duties, sugar levies), the amounts indicated must be net amounts, i.e. gross amounts after deduction of 20 % for collection costs.