DECISION No GB/2024/7

of the European Cybersecurity Industrial, Technology and Research Competence Centre Governing Board

on the Security in the European Cybersecurity Competence Centre

THE GOVERNING BOARD,

1. Having regard to Regulation (EU) 2021/887 of the European Parliament and of the Council, of 20 May 2021, establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres[1] ('Regulation (EU) 2021/887'),
2. Having regard to Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission[2],
3. Having regard to Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information[3],

Whereas:

1. According to Article 13(3)(v) of the Constituent Act of the ECCC, the Governing Board should adopt security rules for the ECCC.
2. Pursuant to Article 36(1) of its Constituent Act, the security rules of the ECCC shall apply the security principles laid down in Commission Decisions (EU, Euratom) 2015/443 and (EU, Euratom) 2015/444.
3. Commission Decision 2015/443 of 13 March 2015 sets out the objectives, basic principles, organisation and responsibilities regarding security at the Commission and equivalent rules should apply to the ECCC.
4. The objective of security within ECCC is to operate in a safe and secure environment, providing appropriate levels of protection for persons, assets and information commensurate with identified risks, and ensuring timely delivery of security.
5. To fulfil these obligations, the ECCC needs to adopt its Security Rules in line with the requirements mentioned above.
6. The Commission has been consulted on the ECCC's Security Rules.

HAS DECIDED AS FOLLOWS:

Article 1: Security in ECCC

The rules on security in the ECCC laid down in the Annex of this Decision are adopted.

1. _____

[1] OJ L 202, 8.6.2021, p. 1–31
[2] OJ L 72, 17.3.2015, p. 41–52
[3] OJ L 72, 17.3.2015, p. 53–88

Article 2: Entry into force

This Decision shall enter into force on the date following that of its adoption.

Done at Dublin, on 27 June 2024

For the European Cybersecurity Industrial,
Technology and Research Competence
Centre

(e-signed)

Pascal Steichen
Chairperson of the Governing Board

Annex
to the Decision of the Governing Board of the European Cybersecurity Competence Centre on the Security in the European Cybersecurity Competence Centre

CHAPTER 1

GENERAL PROVISIONS

Article 1
Definitions

For the purposes of this Decision the following definitions apply:

a. 'assets' means all movable and immovable property and possessions of the European Cybersecurity Industrial, Technology and Research Competence Centre, founded by Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (ECCC);
b. 'Communication and Information System' or 'CIS' means any system enabling the handling of information in electronic form, including all assets required for its operation, as well as the infrastructure, organisation, personnel and information resources;
c. 'control of risks' shall mean any security measure that can reasonably be expected to effectively control a risk to security by its prevention, mitigation, avoidance or transfer;
d. 'crisis situation' means a circumstance, event, incident or emergency (or a succession or combination thereof) posing a major or an immediate threat to security in the ECCC regardless of its origin;
e. 'incident' means any act or event at ECCC that has an adversary effect on: the integrity of persons (personal security incident), and/or the integrity of physical assets (physical security incident), and/or the authenticity, availability, confidentiality, integrity or non-repudiation of stored, transmitted or processed information (information security incident), and/or the integrity, confidentiality and availability of Communication and Information Systems (CIS) including weaknesses (IT security incident);
f. '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;
g. 'ECCC Security Authority' means the Executive Director (ED) or a staff member of the ECCC to whom the ED delegates the responsibility (or parts of those functions) for the security within the Centre;
h. 'ECCC's security staff' means the ECCC's staff members with responsibilities in defining and implementing security and safety related policies;
i. 'personal data' means personal data as defined in Article 3(1) of 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;

j. ‘premises’ shall mean any immovable or assimilated property and possessions of the ECCC;
k. ‘prevention of risk’ shall mean security measures that can reasonably be expected to impede, delay or stop a risk to security;
l. ‘risk to security’ means the combination of the threat level, the level of vulnerability and the possible impact of an event;
m. ‘security in the ECCC’ means the security of persons, assets and information in the ECCC, and in particular the physical integrity of persons and assets, the integrity, confidentiality and availability of information and communication and information systems, as well as the unobstructed functioning of ECCC operations;
n. ‘security measure’ means any measure taken in accordance with this Decision for purposes of controlling risks to security;
o. ‘Staff Regulations’ means the Staff Regulations of officials and the Conditions of Employment of Other Servants of the European Union, as laid down by Regulation (EEC, Euratom, ECSC) No 259/68 of the Council (5) and its amending acts;
p. ‘threat to security’ means an event or agent that can reasonably be expected to adversely affect security if not responded to and controlled;
q. ‘immediate threat to security’ means a threat to security which occurs with no or with extremely short advance warning; and
r. ‘major threat to security’ means a threat to security that can reasonably be expected to lead to loss of life, serious injury or harm, significant damage to property, compromise of highly sensitive information, disruption of IT systems or of essential operational capacities of the ECCC;
s. ‘vulnerability’ means a weakness of any nature that can reasonably be expected to adversely affect security in the ECCC, if exploited by one or more threats.

Article 2
Subject matter

1. This Decision sets out the objectives, basic principles, organisation and responsibilities regarding security in the ECCC.
2. This Decision shall apply in all premises of the ECCC.
3. Notwithstanding any specific indications concerning particular groups of staff, this Decision shall apply to ECCC staff under the scope of the Staff Regulations and of the Conditions of Employment of other servants of the European Union, to national experts seconded to the ECCC (SNEs), to service providers and their staff, to trainees and to any individual with access to ECCC buildings or other assets, or to information handled by the ECCC.

CHAPTER 2

PRINCIPLES

Article 3
Principles for security in the ECCC

1. In implementing this Decision, the ECCC shall comply with the Treaties and in particular the Charter of Fundamental Rights and Protocol No 7 on the Privileges and Immunities of the European Union, with any applicable rules of national law as well as with the terms of

the present Decision. If necessary, further security guidelines in the sense of Article 20(2) shall be issued.

2. Security in the ECCC shall be based on the principles of legality, transparency, proportionality and accountability.
3. The principle of legality indicates the need to stay strictly within the legal framework in implementing this Decision and the need to conform to the legal requirements.
4. Any security measure shall be taken overtly unless this can reasonably be expected to impair its effect. Addressees of a security measure shall be informed in advance of the reasons for and the impact of the measure, unless the effect of the measure can reasonably be expected to be impaired by providing such information. In this case, the addressee of the security measure shall be informed after the risk of impairing the effect of the security measure has ceased.
5. ECCC departments shall ensure that security issues are taken into account from the start of the development and implementation of ECCC policies, decisions, programmes, projects and activities for which they are responsible. In order to do so, they shall involve the Local Security Officer and the Local Cybersecurity Officer of the ECCC and their deputies as regards IT systems.
6. The ECCC shall, where appropriate, seek cooperation with the competent authorities of the host Member State, of other Member States and of other EU institutions, agencies or bodies, where feasible, taking account of the measures taken or planned by those authorities to address the risk to security concerned.

Article 4
Obligation to comply

1. Compliance with this Decision and its implementing rules and with the security measures and the instructions given by mandated staff shall be mandatory.
2. Non-compliance with the security rules may trigger liability to disciplinary action in accordance with the Treaties, the Staff Regulations, to contractual sanctions and/ or to legal action under national laws and regulations.

CHAPTER 3

ORGANISATION

Article 5
General responsibilities in ECCC

1. The responsibilities of the ECCC referred to in this Decision shall be exercised by the security staff under the authority and responsibility of the Executive Director, acting as the ECCC Security Authority.
2. The specific arrangements as regards cybersecurity will be defined in the ECCC's policies on the information systems security standards, in accordance with Regulation (EU) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union.

Article 6
The ECCC Security Authority

1. The ECCC Security Authority shall in particular be responsible for:

a. developing the ECCC's security policy, implementing rules and security guidelines;
b. gathering information in view of assessing threats and risks to security and on all issues which may affect security in the ECCC;
c. providing counter electronic surveillance and protection to all the sites of the ECCC, taking due account of threat assessments and evidence of unauthorised activities against the ECCC's interests;
d. ensuring security services for ECCC departments and staff, including through contracts with companies providing security services;
e. implementing security measures aimed at mitigating risks to security and developing and maintaining appropriate CIS to cover its operational needs,
f. raising awareness, organising exercises and drills and providing training and advice on all issues related to security at the ECCC, in view of promoting a security culture.

2. The ECCC Security Authority, through the LSO/ DLSO, shall, without prejudice to other ECCC services' competences and responsibilities, ensure external liaison:
   a. with the Directorate-General for Human Resources and Security of the Commission, in cases of crisis and security incidents management and business continuity, major incidents or of any incident related to the operation of the network which could have an impact on the availability, confidentiality and integrity of data or on the quality or the availability of service to the systems' users and for the purpose of consulting the Commission on draft security measures and any amendment thereto;
   b. with the security departments of the other Union institutions, agencies and bodies on issues relating to the security of the persons, assets and information in the ECCC;
   c. with security, intelligence and threat assessment services, including national security authorities, of the Member States, of third countries and international organisations and bodies on issues affecting the security of persons, assets and information in the ECCC;
   d. with police and other emergency services on all routine and emergency issues affecting the ECCC's security;
   e. with the security authorities of other Union institutions, of agencies and bodies, of the Member States and of third countries in the field of response to cyberattacks with a potential impact on security in the ECCC;
   f. regarding the receipt, assessment and distribution of intelligence concerning threats posed by terrorist and espionage activities affecting security in the ECCC;
   g. regarding issues relating to classified information, as specified further in the dedicated ECCC decision that will be adopted at a later time, after the approval of this Decision.

Article 7
Local Security Officer (LSO)

1. The ECCC Security Authority shall appoint a Local Security Officer (LSO), who shall act as the main point of contact on all matters related to security in the ECCC. If needed, one or more Deputy LSO may be appointed. The LSO/ Deputy LSO shall be temporary agents.
2. As the main point of contact on security within the ECCC, the LSO shall report at regular intervals to the Security Authority on security issues involving the ECCC. The LSO/ Deputy LSO shall report immediately to the Security Authority on any security incidents, including those where EU Classified Information or Sensitive non-classified information may have been compromised.

3. For matters related to security of communication and information systems, the LSO/ Deputy LSO shall liaise with the Local Cybersecurity Officer of the ECCC, as defined in Regulation (EU, Euratom) 2023/2841 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.
4. The LSO/ Deputy LSO shall contribute to security training and awareness activities addressing the specific needs of staff, contractors and other individuals working under the authority of ECCC.
5. The LSO/ Deputy LSO may be assigned specific tasks in cases of major or immediate risks to security or of emergencies at the request of the Security Authority of the ECCC.
6. The responsibilities of the LSO/ Deputy LSO shall be without prejudice to the role and responsibilities assigned to the Local Cybersecurity Officer, Registry Control Officers (RCOs) or any other function implying security or safety-related responsibilities. The LSO// Deputy LSO shall liaise with them in order to ensure a coherent and consistent approach to security and an efficient flow of information on matters related to security at the ECCC.
7. The LSO/ Deputy LSO shall have direct access to the ECCC Security Authority, while informing his direct hierarchy. The LSO/ Deputy LSO shall hold a security authorisation to access EUCI, at least up to the level of SECRET UE/EU SECRET.

Article 8
The Local Cybersecurity Officer

1. The Local Cybersecurity Officer is responsible for the daily operational security matters related to the information systems of the ECCC, including the following:
    a. Developing the systems' security plans and business continuity plans, and monitoring their performance;
    b. Contributing to the dissemination of the information systems security policy in ECCC and preparing and performing the security awareness campaigns;
    c. Ensuring that an inventory of all information systems is kept and updated with a description of the security needs and a grading of the requirements;
    d. Cooperating with the ECCC's LSO/ Deputy LSO on all the information systems security matters;
    e. Ensuring that the IT service providers put in place the necessary security measures;
    f. Taking part in checks whenever security risks and incidents are identified.
2. The Local Cybersecurity Officer shall have the appropriate experience, knowledge and skills in the information systems security in order to fulfil their specific tasks and responsibilities efficiently and effectively.

CHAPTER 4

DELIVERING SECURITY

Article 9
Mandated staff

1. Only staff authorised on the basis of a nominative mandate conferred to them by the ECCC Executive Director, given their current duties, may be entrusted with the power to take one or several of the following measures:
    a. Conduct security inquiries as referred to in Article 16;
    b. Take security measures as referred to in Article 15, as specified in the mandate.

2. The mandates referred to in paragraph 1 shall be conferred for a duration which shall not exceed the period during which the person concerned hold the post or function in respect of which the mandate has been conferred. They shall be conferred in compliance with the applicable provisions set out in Article 3(1).
3. As regards mandated staff, this Decision constitutes a service instruction within the meaning of Article 21 of the Staff Regulations.

Article 10
General provisions regarding security measures

1. When taking security measures, the ECCC shall in particular ensure so far as reasonably possible, that:
    a. it only seeks support or assistance from the state concerned, provided that that state either is a Member State of the European Union or, if not, party to the European Convention on Human Rights, or guarantees rights which are at least equivalent to the rights guaranteed in this Convention;
    b. it shall only transfer information on an individual to recipients established in the Union, other than Union institutions and bodies, in accordance with Article 9 of Regulation (EU) 2018/1725[4];
    c. where an individual poses a threat to security, any security measure shall be directed against that individual and that individual may be subjected to bearing the incurring costs. Those security measures may only be directed against other individuals if an immediate or major threat to security must be controlled and the following conditions are fulfilled:
        i. the envisaged measures against the individual posing the threat to security cannot be taken or are not likely to be effective;
        ii. the ECCC cannot control the threat to security by its own actions or cannot do so in a timely manner;
        iii. the measure does not constitute a disproportionate danger for the other individual and his rights.
2. The ECCC Security Authority shall have an overview of security measures which may require an order by a judge in accordance with the laws and regulations of the Member State hosting the ECCC premises.
3. The ECCC Security Authority may turn to a contractor or to other Union institution or body to carry out, under their direction and supervision, tasks relating to security.

Article 11
Security measures regarding persons

1. An appropriate level of protection shall be afforded to persons in the premises of the ECCC, taking into account security and safety requirements.
2. In case of major risks to security, the ECCC Security Authority shall provide protection to all individuals referred to in Article 2(3) of the present Decision where a threat assessment has indicated that such protection is needed to ensure their safety and security.
3. In case of major risks to security, the ECCC may order the evacuation of its premises.
4. Victims of accidents or attacks within ECCC premises shall receive assistance.

1.

[4] 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

5. In order to prevent and control risks to security, mandated staff may carry out background checks of persons falling under the scope of this Decision, so as to determine whether giving such persons access to ECCC premises or information presents a threat to security. For that purpose, and in compliance with Regulation (EU) 2018/1725[5] and provisions referred to under Article 3(1), the mandated staff concerned may:
    a. use any source of information available to the ECCC, taking into account the reliability of the source of information;
    b. access the personnel file or data the ECCC holds with regard to individuals it employs or intends to employ, or for contractors' staff when duly justified.

Article 12
Security measures regarding physical security and assets

1. Security of assets shall be ensured by applying appropriate physical and technical protective measures and corresponding procedures, hereinafter called 'physical security', creating a multi-layered system.
2. Measures may be adopted pursuant to this Article in order to protect persons or information in the ECCC as well as to protect assets.
3. Physical security shall have the following objectives:
    a. preventing acts of violence directed against any persons falling within the scope of this Decision,
    b. preventing espionage and eavesdropping on sensitive non-classified or classified information,
    c. preventing theft, acts of vandalism, sabotage and other violent actions aimed at damaging or destroying ECCC buildings and assets,
    d. enabling investigation and inquiry into security incidents including through checks on access and exit control log files, CCTV coverage, telephone call recordings and similar personal data as referred to in Article 21(2) hereunder and other information sources.
4. Physical security shall include:
    a. an access policy applicable to any individual or vehicle requiring access to ECCC premises, including the parking lots, which shall be adopted as implementing rules of this Decision,
    b. access control and intrusion-detection systems comprising guards, technical equipment and measures, information systems or a combination of all of those elements.
5. In order to ensure physical security, the following actions may be taken:
    a. recording entry to and exit from ECCC premises of persons, vehicles, goods and equipment,
    b. performing identity controls at its premises,
    c. ensuring inspection of vehicles, goods and equipment by visual or technical means,
    d. applying measures to prevent unauthorised persons, vehicles and goods, from entering ECCC premises.

Article 13
Security measures regarding information

1. Security of information covers all information handled by the ECCC.

1.

[5] 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

2. Security of information, regardless of its form, shall balance transparency, proportionality, accountability and efficiency with the need to protect information from unauthorised access, use, disclosure, modification or destruction.
3. Security of information shall be aimed at protecting its confidentiality, integrity and availability.
4. Risk management processes shall therefore be used to assess the security needs of the information assets and to develop proportionate security measures, procedures and standards for its protection.
5. These general principles on the security of information shall be applied in particular as regards:
    a. 'European Union Classified Information' (hereafter 'EUCI'), that is to say 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 European Union or of one or more of the Member States;
    b. 'Sensitive non-classified information' (hereafter "SNC information"), that is to say information or material the ECCC must protect because of legal obligations laid down in the Treaties or in acts adopted in implementation thereof, and/ or because of its sensitivity. SNC information includes, but is not limited to, information or material covered by the obligation of professional secrecy, as referred to in Article 339 TFEU, information covered by the interests protected in Article 4 of Regulation (EC) No 1049/2001 of the European Parliament and of the Council read in conjunction with the relevant case-law of the Court of Justice of the European Union or personal data within the scope of Regulation (EU) 2018/1725[6].
6. EUCI and SNC information shall be subject to specific rules regarding their access, handling and storage, with a view to ensure their protection.
7. Any individual who is responsible for compromising or losing EUCI or SNC information, which is identified as such in the rules regarding its handling and storage, may be liable to disciplinary action in accordance with the Staff Regulations. That disciplinary action shall be without prejudice to any further legal or criminal proceedings by the competent national authorities of the Member States in accordance with their laws and regulations and to contractual remedies.

Article 14
Security measures regarding Communication and Information Systems

1. All Communication and Information Systems ('CIS') used by the ECCC shall comply with the ECCC's IT Security Policy, in accordance with Regulation (EU) 2023/2841 [7].
2. ECCC services owning, managing or operating CISs shall only allow other Union institutions, agencies or bodies to have access to those systems provided that those Union institutions, agencies or bodies can provide reasonable assurance that their IT systems are protected at a level equivalent to the ECCC's IT Security Policy , its implementing rules and corresponding security standards. The ECCC shall monitor such compliance, and in case of serious non-compliance or continued failure to comply, be entitled to prohibit access.

1. _____

[6] 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

[7] Regulation (EU) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union, its implementing rules and corresponding security standards.

Article 15
Security measures regarding persons and objects

1. In order to ensure the security in the ECCC and to prevent and control risks, staff mandated in accordance with Article 9 may, in compliance with the principles set out in Article 3, take inter alia one or more of the following security measures:
    a. securing of scenes and evidence, including access and exit control log files, CCTV images, in case of incidents or conduct that may lead to administrative, disciplinary, civil or criminal procedures;
    b. limited measures concerning persons posing a threat to security, including ordering persons to leave the ECCC's premises, escorting persons from the ECCC's premises, banning persons from the ECCC's premises for a period of time;
    c. limited measures concerning objects posing a threat to security including removal, seizure and disposal of objects;
    d. searching of ECCC premises, including of offices, within such premises;
    e. searching of CIS and equipment, telephone and telecommunications traffic data, log files, user accounts, etc.;
    f. other specific security measures with similar effect in order to prevent or control risks to security, in particular in the context of the ECCC's rights and obligations with regards to its physical premises, or as an employer in accordance with the applicable national laws.
2. Under exceptional circumstances (including threat to the interest of ECCC vital for the ECCC's management and functioning), the ECCC security staff mandated in accordance with Article 9, may take any urgent measures needed, in strict compliance with the principles laid down in Article 3. As soon as possible after having taken those measures, they shall inform the ECCC Security Authority, who shall confirm the measures taken and authorise any further necessary actions. The ECCC mandated staff shall also liaise, where appropriate, with the competent national authorities.
3. Security measures pursuant to this Article shall be documented at the time they are taken or, in the event of an immediate risk or a crisis, within reasonable delay after they are taken. In the latter case, the documentation must also include the elements on which the assessment regarding the existence of an immediate risk or a crisis was based. The documentation can be concise, but should be constituted in such a way as to allow the person subjected to the measure to exercise his rights of defence and of protection of personal data in accordance with Regulation (EU) 2018/1725[8], and to allow a scrutiny as to the legality of the measure. No information about specific security measures addressed to a member of staff shall be part of the person's personnel file.
4. When taking security measures pursuant to point (b), the ECCC shall in addition guarantee that the individual concerned is given the opportunity to contact a lawyer or a person of his confidence and be made aware of their right to have recourse to the European Data Protection Supervisor.

Article 16
Inquiries

1. Without prejudice to Article 86 and Annex IX of the Staff Regulations, security inquiries may be conducted:

1.

[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

a. in case of incidents affecting security at the ECCC, including suspected criminal offences;
b. in case of potential leakage, mishandling or compromise of SNC information or EUCI;
c. in the context of counter-intelligence and counter-terrorism;
d. in case of serious cyber-incidents, in line with Regulation (EU) 2023/2841[9].

2. The decision to conduct a security inquiry shall be taken by the ECCC Security Authority who will also define the purpose and the scope of the inquiry, the process to be followed and will be the recipient of the inquiry report.
3. Security inquiries shall be conducted only by dedicated members of staff duly mandated in accordance with Article 9.
4. The mandated staff shall exercise their powers of security inquiry independently, as specified in the mandate and shall have the powers listed in Article 15.
5. Mandated staff having the competence to conduct security inquiries may gather information from all available sources related to any administrative or criminal offences committed within the ECCC premises or involving individuals referred to in Article 2(3) either as victim or perpetrator of such offences.
6. The ECCC Security Authority shall inform the competent authorities of the host Member State or any other Member State concerned, where appropriate, and in particular if the inquiry has given rise to indications of a criminal act having been perpetrated. In this context, the ECCC Security Authority may, where appropriate or required, provide support to the authorities of the host Member State or any other Member State concerned.
7. In the case of serious cyber-incidents the Local Cybersecurity Officer shall collaborate closely with the LSO/ Deputy LSO to provide support on all technical matters. The LSO/ Deputy LSO shall decide, in consultation with the Local Cybersecurity Officer, when it is appropriate to inform the competent authorities of the host Member State or any other Member State concerned. The incident coordination services of Computer Emergency Response Team for the European institutions, bodies and agencies ('CERT-EU') will be contacted for support and advice on cybersecurity.
8. Security inquiries shall be documented.

Article 17
Delineation of competences with regard to security inquiries and other types of investigations

1. Where the ECCC's mandated staff conducts security inquiries, as referred to in Article 16, and if these inquiries fall within the competences of the European Anti-Fraud Office (OLAF) or of any disciplinary board of the ECCC, it shall liaise with those bodies at once with a view, in particular, not to compromise their steps.
2. The security inquiries, as referred to in Article 16, shall be without prejudice to the powers of OLAF and any disciplinary board of the ECCC, as laid down in the rules governing those bodies. The ECCC's mandated staff may be requested to provide technical assistance for inquiries initiated by OLAF or by any disciplinary board of the ECCC.
3. Without prejudice to Article 22(a) of the Staff Regulations, where a case may fall within the competence of both the ECCC's mandated staff and the disciplinary board, the ECCC's mandated staff shall, when it reports to the Security Authority in compliance with Article 16 at the earliest possible stage, advise whether there are grounds that justify that the disciplinary board is seized with the matter. This stage shall in particular be considered to

1.

[9] Regulation (EU) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union, its implementing rules and corresponding security standards

have been reached when an immediate threat to security has come to an end. The Security Authority shall decide on the matter.

Article 18
Security inspections

1. The ECCC's security staff shall undertake security inspections in order to verify compliance by ECCC services and individuals with this Decision and its implementing rules and to formulate recommendations when deemed necessary.
2. Where appropriate, the ECCC Security Authority shall ensure that security inspections or security monitoring or assessment visits are undertaken to verify whether the security of ECCC staff, assets and information falling under the responsibility of other Union institutions, agencies or bodies, Member States, third states or international organisations, is appropriately protected in accordance with security rules, regulations and standards which are at least equivalent to those of the ECCC.
3. Security inspections shall be documented and the results shall be reported to the Security Authority of ECCC without delay.

Article 19
Alert states and management of crisis situations

1. The ECCC's security staff shall be responsible for putting in place appropriate alert state measures in anticipation of or in response to threats and incidents affecting security at the ECCC, and for measures required for managing crisis situations.
2. The alert state measures referred to in paragraph 1 shall be commensurate with the level of threat to security. The alert states levels shall be defined in close cooperation with the competent services of the Commission, and of the Member State hosting ECCC's premises.
3. The ECCC's security staff shall be the contact point for alert states and management of crisis situations and shall inform accordingly the ECCC Security Authority.

CHAPTER 5

IMPLEMENTATION

Article 20
Implementing rules and security guidelines

1. As necessary, the ECCC's Security Authority shall establish any Implementing Rules for this Decision, after consulting them with the Commission.
2. Any further security guidelines and best practices within the scope of this Decision and its implementing rules may be developed under the supervision of the ECCC's Security Authority.

CHAPTER 6

MISCELLANEOUS AND FINAL PROVISIONS

Article 21
Processing of personal data

1. The ECCC shall process personal data needed for the implementation of this Decision in accordance with Regulation (EU) 2018/1725[10].
2. The ECCC's Security Authority shall be responsible for the security of any processing of personal data undertaken in the context of this Decision.

Article 22
Transparency

1. This Decision and its implementing rules, security guidelines and procedures shall be brought to the attention of all ECCC staff, of the external service providers, of trainees and of any other individual to whom they apply, immediately after their entry into force.

1.

[10] 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