DECISION OF THE COLLEGE OF THE EUROPEAN PUBLIC PROSECUTOR'S OFFICE OF 26 JUNE 2024

ON THE SECURITY STRATEGY 2024-2028

The College of the European Public Prosecutor's Office (EPPO),

Having regard to Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('EPPO') (hereinafter referred to as 'the EPPO Regulation')[1], and in particular Article 73 thereof,

Having regard to Regulation (EU, Euratom) 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[2],

Having regard to Decision 014/2024 of the College of the EPPO of 7 February 2024 on Security Rules applicable to the Digital Communication and Information Systems of the EPPO (hereinafter referred to as "College Decision 014/2024"),

Having regard to Decision 018/2021 of the College of the EPPO of 24 March 2021 on the EPPO Internal Control Framework ('ICF'),

Whereas:

(1) Article 9(2) of the College Decision 014/2024 requires the Security Unit to prepare a Security Strategy aligned with the EPPO mandate and priorities.

(2) Principle 11 of the Internal Control Framework Assessment Criteria requires EPPO to develop an IT security strategy.

Has adopted the following decision:

[1] OJ L 283 31.10.2017, p. 1.

[2] OJ L, 2023/2841, 18.12.2023.

Article 1

Adoption of the Security Strategy

The Security Strategy of the European Public Prosecutor's Office for the period 2024-2028, as presented in the Annex which forms integral part of this decision, is hereby adopted.

Article 2

Entry into force

This Decision shall enter into force on the day of its adoption.

Done at Luxembourg on 26 June 2024.

On behalf of the College,

Laura Codruța Kövesi

European Chief Prosecutor

KOVESI Laura

Digitally signed by KOVESI Laura
Date: 2024.06.27 14:46:34 +02'00'

SECURITY STRATEGY

2024-2028

EPPO

EUROPEAN
PUBLIC
PROSECUTOR'S
OFFICE

Contents

Chapter 1 – Context

Introduction

The mandate of the European Public Prosecutor's Office (hereinafter referred to as "EPPO") is to investigate, prosecute and bring to judgement the perpetrators of, and accomplices in, offences against the Union's financial interests, as determined by the EPPO Regulation[3]. It exercises the functions of prosecutor in the competent courts of the participating Member States in relation to such offences.

The EPPO became fully operational on 1 June 2021.

In regards to security, the EPPO Regulation identifies in Articles 73, 108 and 111 several objectives related to:

- The security of processing of operational personal data
- Confidentiality and professional secrecy
- The protection of information handled by the EPPO, in particular sensitive non-classified information and EU classified information.

In this context, security is an essential element for enabling the organisation to reach its mandate. To this end, the Security Strategy aims to set a direction for the measures that are required in the next years to allow EPPO to fulfil its mandate and support the achievement of the strategic objectives outlined in the upcoming Digital Strategy.

The strategy is the result of an analysis of the current global security environment, expected challenges – from technology and upcoming threats – and a need for an enhanced security maturity to address them. Equally, this strategy is an educated guess as to what needs to be done as the EPPO evolves, together with the operational requirements around EPPO investigations. This includes a shift from a reactive to a proactive security approach, focusing efforts on preventing physical risks, cyber-attacks and related incidents and having a dynamic and flexible response to adverse events.

This strategy aims to enhance security maturity across all areas through a comprehensive assessment, enabling the EPPO to timely identify threats and effectively mitigate risks by implementing necessary protective measures. By doing so, the organization can prevent minor incidents from escalating into major ones, thereby preserving its reputation and reducing potential harm to employees, stakeholders, partners, investigations, and other valuable assets.

Context and drivers

The EPPO Single Programming Document for the period 2025-2027[4] identifies the following multi-annual general objectives:

[3] Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the EPPO (OJ L 283 31.10.2017, p. 1).

[4] Decision 013/2024 of the College of the EPPO of 7 February 2024 on the adoption of the preliminary draft Single Programming Document of the European Public Prosecutor's Office for the period 2025-2027.

- Deliver on the European Chief Prosecutor, the College, the European Prosecutors, the Permanent Chambers and the European Delegated Prosecutors' crime investigations and prosecution mandate
- Deploy and make available information, analysis and case management tools, to bolster investigations and prosecutions effectiveness and efficiency
- Build up, and integrate in, a network of organisations and individuals, mutualising their capacity to deliver on common standards in fighting crimes against the EU financial interests
- **Protect EPPO personnel, physical and digital assets from security threats**
- Administer the EPPO to deliver on EU public administration standards.

In order to support EPPO reaching its security objective, this Strategy sets the following Mission: *continuously provide a secure environment for EPPO, its personnel and information in alignment with the legal requirements and consistent with the threat landscape*.

This mission shall be aligned with the EPPO organisational mission, vision and values.

In line with the College Decision 014/2024 on the Security Rules applicable to Digital Communication and Information Systems[5], international standards[6] and best practices, the EPPO applies the Plan-Do-Check-Act methodology in the set-up of its security and safety related processes:

Plan*: establish policies, objectives, processes, procedures and controls relevant for developing and improving the security*

Do*: implement and operate the planned objectives, processes, procedures and controls relevant in the field of security*

Check*: monitor and review the performance of the implemented processes, procedures and controls*

Act*: maintain and improve the implemented processes, procedures and controls based on reviews and relevant factors*.

To support a comprehensive management of all security aspects, at the level of EPPO, the responsibilities in terms of security are organised as follows:

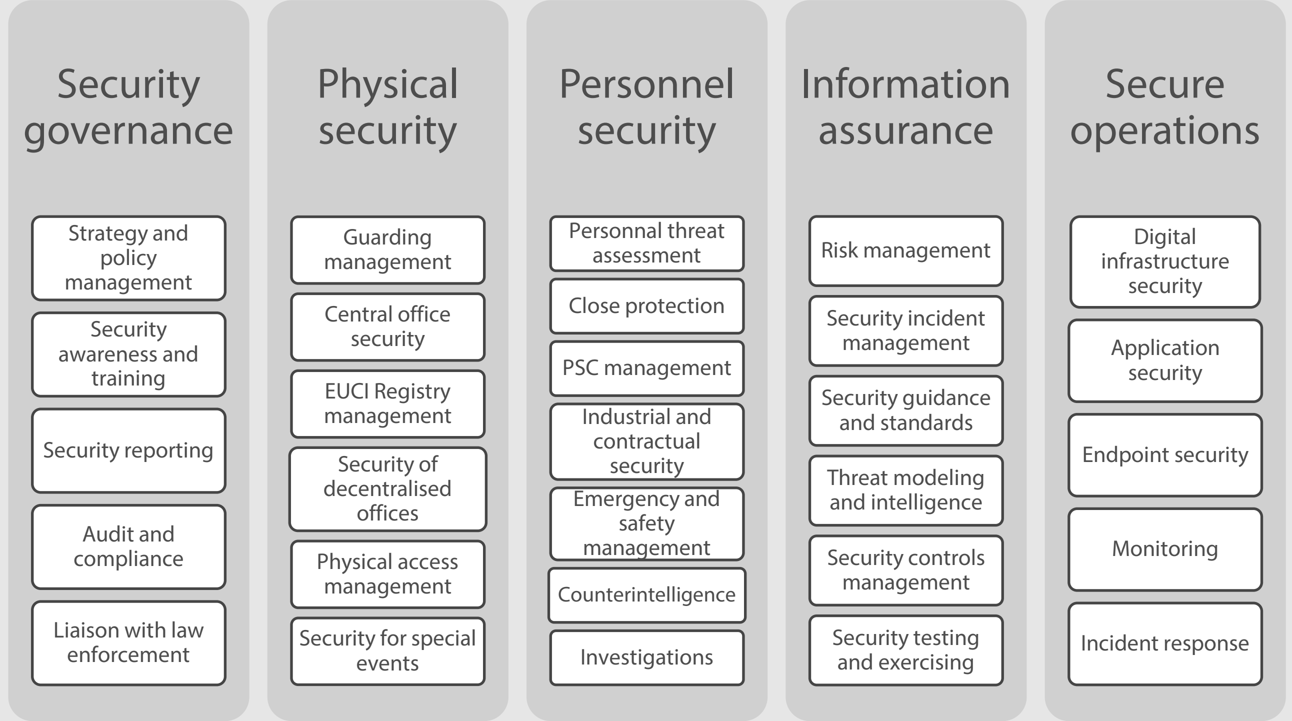
- The Administrative Director is the Security Authority
- The Security Unit is responsible for the establishment of security strategic aspects, including defining the policies, and implementing those security and safety related activities not specifically assigned to the Digital Ecosystem Support Sector and the Corporate Service Sector. Moreover, the Security Unit is responsible for the monitoring and reporting on the implementation of the defined policies.
- The Digital Ecosystem Support Sector is responsible for implementing and managing the digital security operations

[5] Decision 014/2024 of the College of the EPPO of 7 February 2024 on Security Rules applicable to the Digital Communication and Information Systems of the EPPO.
[6] ISO 27000 family, ISO 31000 family

- ➢ The Corporate Service Sector is responsible for implementing building safety aspects.

Security services

In order to ensure the delivery of all security and safety needs in the EPPO, the below diagram identifies the security services that have been set-up in the organisation. The services are grouped in 5 security fields: security governance, physical security, personnel security, information assurance and secure operations.



Security governance
Strategy and policy management
Security awareness and training
Security reporting
Audit and compliance
Liaison with law enforcement

Physical security
Guarding management
Central office security
EUCI Registry management
Security of decentralised offices
Physical access management
Security for special events

Personnel security
Personnal threat assessment
Close protection
PSC management
Industrial and contractual security
Emergency and safety management
Counterintelligence
Investigations

Information assurance
Risk management
Security incident management
Security guidance and standards
Threat modeling and intelligence
Security controls management
Security testing and exercising

Secure operations
Digital infrastructure security
Application security
Endpoint security
Monitoring
Incident response

The services are delivered jointly by the Security Unit, Digital Services Unit and Corporate Services Sector in a coordinated manner in order to ensure efficiency and cost effective use of resources.

Chapter 2 – Challenges

The analysis of the environment and evolution of the EPPO mandate, highlights the following challenges for the next years:

(1) *Enlargement of the threat landscape for personnel and premises* due to EPPO's increasing capacity to dismantle organised crime groups

(2) *Increase in complexity of the EPPO digital ecosystem*, including growth in terms of numbers of technical solutions, applications and stakeholders, both in cloud and on premises. This is combined with a transformation of digital governance including

   a. Increased adoption of cloud services to address enhanced business needs in terms of digitalisation and interoperability

b. Changes in supply chain and adoption of hybrid models for code development services
c. Transition from standard digital services provided by DG DIGIT to IT autonomy within the constraints of limited financial resources attributed to EPPO
d. Increased expectations for innovative and ground-breaking solutions from business users
e. Quick growth of the organisation's user base

(3) *Enlargement of the threat landscape for EPPO digital systems* due to the increase in the digital ecosystem, the proliferation of threat actors and the evolution of the security challenges in Europe following global political instability

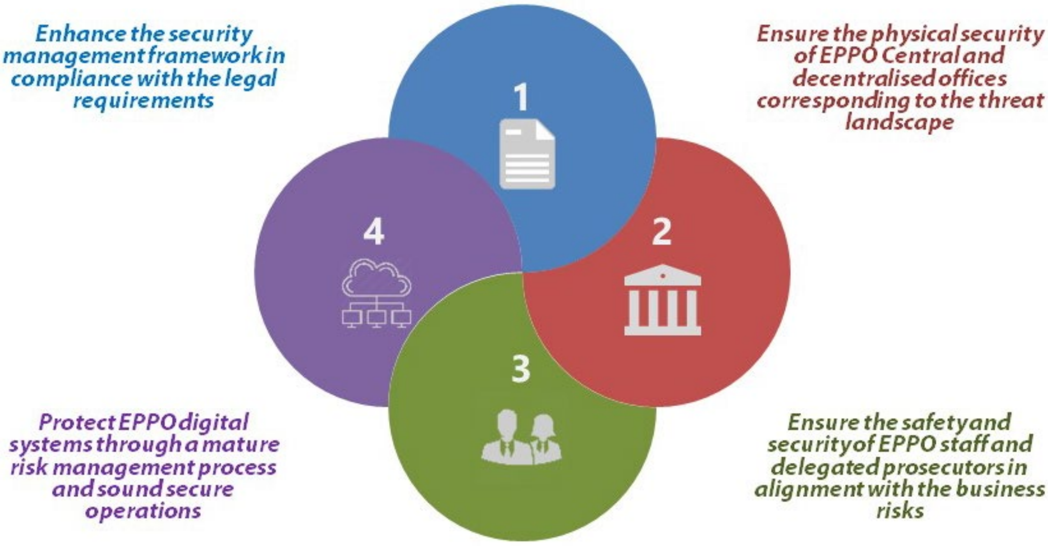
(4) *Enlargement of premises* and need for consolidation of physicals security controls, including enhancement of security measures addressed in the planned refurbishment projects

(5) *The decentralised aspect of EPPO* with direct dependency on the security implemented within each Member State

(6) *Alignment with increased legal requirements* in terms of security, in particular timely implementation of security requirements following the adoption of the Cybersecurity regulation[7] and upcoming Information Security Regulation[8].

Chapter 3 – Objectives

In order to provide a structured approach to achieving the EPPO mandate in the area of security, a number of 4 objectives have been identified for the period 2024-2028.


Enhance the security management framework in compliance with the legal requirements
1
Ensure the physical security of EPPO Central and decentralised offices corresponding to the threat landscape
2
4
3
Protect EPPO digital systems through a mature risk management process and sound secure operations
Ensure the safety and security of EPPO staff and delegated prosecutors in alignment with the business risks

[7] Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 lying down measures for high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union
[8] COM(2022) 119 final

Each objective is associated with a number of outcomes that support the implementation and monitoring of the Strategy.

Objective 1: Enhance the security management framework in compliance with the legal requirements

The implementation of this objective shall be achieved though the following outcomes:

1.1. Updated Security Policy Framework, in compliance with the legal requirements and international best practices
1.2. Implemented security controls related to the requirements stemming from the Cybersecurity regulation and upcoming Information Security Regulation
1.3. Implemented framework for exchange of EU Classified Information with the European Commission, Council, Europol and other relevant partners
1.4. Enhanced security awareness programme, including adoption of a Security Awareness Policy, preparation of annual awareness plans targeting all security areas (physical security, information security, cyber security and personnel security) and enriched security intranet platform
1.5. Implemented recommendations following audits and inspections in line with agreed timeline
1.6. Extended catalogue of security related contracts in order to enhance effectiveness in engaging the private sector in managing security needs.

Objective 2: Ensure the physical security of EPPO Central and decentralised offices corresponding to the threat landscape

The implementation of this objective shall be achieved though the following outcomes:

2.1. Updated building security systems for the access control and monitoring of EPPO Central Office
2.2. Enhanced physical access control to EPPO Central Office in line with recommendations of risk assessment
2.3. Implementation of required secure controls for all EPPO Central Office floors following the building refurbishment project
2.4. Increased effectiveness of the guarding services in the EPPO Central Office
2.5. Developed network of security contact points for the coordination of physical security measures for the decentralised offices
2.6. Adopted minimum physical security standards for decentralised offices
2.7. Physical security plans prepared for all EPPO central premises
2.8. Annual check of areas with reinforced security controls.

Objective 3: Ensure the safety and security of EPPO staff and delegated prosecutors in alignment with the business risks

The implementation of this objective shall be achieved though the following outcomes:

3.1. Operational EPPO counterintelligence capability based on general accepted standards
3.2. Operational Close Protection capability
3.3. Operational services for personal threat assessment (PTA) for European Prosecutors
3.4. Implemented solution to ensure safety and security of EPPO staff and delegated prosecutors in case of increased risk
3.5. Yearly emergency drill, updated emergency response procedures and emergency response capability (floor wardens and security agents)
3.6. Adapted tool for alerting staff in case of emergencies
3.7. Timely implementation of the vetting and security authorisation process in line with the Personnel Security Clearance (PSC) Policy.

Objective 4: Protect EPPO digital systems through a mature risk management process and sound secure operations

The implementation of this objective shall be achieved through the following outcomes:

4.1. Secure deployment of IT autonomy programme, in line with the recommended security controls
4.2. Completed risk assessment for each EPPO digital system
4.3. Updated Security and Business Continuity Plan for each EPPO digital system
4.4. Implemented Computer Security Incident Response Team (CSIRT) available 24/7 to address cybersecurity incidents
4.5. Implemented comprehensive Security Information and Event Monitoring (SIEM) solution monitoring the EPPO digital environment
4.6. Implemented security controls baseline framework that addresses the transversal security risks and requirements
4.7. Comprehensive security architecture designed for the EPPO digital environment based on zero-trust principle
4.8. Implemented hybrid insourcing model for software development addressing security aspects in the full chain of delivery and cloud hosting of non-sensitive data
4.9. Implemented management framework and tools for enhanced security patching and vulnerability management.

Chapter 4: Implementation

Performance measurement

In order to drive and measure the implementation of the Strategy objectives, a number of key performance indicators (KPIs) are set-up for the objectives.

Objective	Key Performance Indicator
1. Enhance the security management framework in compliance with the legal requirements	1.1. 85% of the planned Security Policy Framework adopted by Q4 2025 1.2. Implemented security controls required Cybersecurity Regulation by Q1 2026 1.3. Signed EUCI exchange agreements with the relevant partners by Q3 2027 1.4. Security Awareness Policy adopted by Q4 2024 1.5. Implemented critical recommendations following audits within 6 months of report 1.6. Extend the catalogue of security related contracts with minimum 1 new contract per year
2. Ensure the physical security of EPPO Central and decentralised offices corresponding to the threat landscape	2.1. Update the access control, video-surveillance and alarm systems by Q4 2026 2.2. Updated physical access controls for EPPO Central Office by Q2 2026 in line with the risk assessment recommendations 2.3. 90% of planned security controls for new Central Office floor implemented 2.4. 98% of planned 24/7 guarding services delivered in line with the Framework contract 2.5. At least 1 meeting/year with the network of national security contact points 2.6. Adopted minimum physical security standards for the EPPO decentralised offices by Q4 2024 2.7. Physical security plans of EPPO central premises issued by Q4 2025 2.8. Annual check of areas with reinforced security controls
3. Ensure the safety and security of EPPO staff and delegated prosecutors in alignment with the business risks	3.1. Counterintelligence capability operational by Q1 2025 3.2. Close Protection capability available 24/7 to address any possible incidents 3.3. PTA issued within 6 months for each new EP 3.4. Adopted response procedures for increased risk for post-holders by Q2 2025 3.5. Annual safety exercise carried out 3.6. Yearly review of tool for alerting staff in case of emergencies 3.7. Issue security authorisation briefings within the PSC policy timeline
4. Protect EPPO digital systems through a mature risk management process and sound secure operations	4.1. Secure deployment of IT Autonomy programme by Q4 2024 in line with the approved security plan 4.2. Updated risk assessment for CMS by Q3 2025

	4.3. Updated security plan for CMS by Q4 2025 4.4. Implemented 24/7 CSIRT by Q1 2028 4.5. Implemented SIEM by Q2 2026 4.6. Implemented baseline security controls by Q1 2025 4.7. Issued comprehensive security architecture by Q1 2027 4.8. Implemented hybrid insourcing model by Q4 2025 4.9. Implemented framework for vulnerability management by Q1 2028

Major risks

The following internal and external risks might affect the delivery of the planned objectives for the EPPO Security Strategy 2024-2028:

☒ Substantial increase in threat landscape, beyond the currently planned security measures, may negatively impact the ability of the EPPO effective deploy preventive measures to ensure security of premises, personnel and assets

☒ EPPO inability to retain or engage skilled personnel for the planned security related activities and projects may impact the timely delivery of the planned objectives

☒ EPPO inability to engage the external stakeholders (Host State, national security services, private security sector) for support with the implementation of security related projects may negatively impact the effectiveness of the planned security controls

☒ Lack of sufficient financial and human resources attributed to EPPO by the Budgetary Authority may negatively impact the organisation's ability to deliver the security related objectives, in particular sound secure operations of the digital systems

☒ Substantial changes in the regulatory framework in terms of security requirements may impact EPPO's ability to timely deliver an updated security management system aligned with the planned objectives.