European Union Agency
for Cybersecurity
Vasilissis Sofias Str 1
151 24 Maroussi | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

DECISION No MB/2021/5
OF THE MANAGEMENT BOARD OF THE EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA)

ON ANTI FRAUD STRATEGY and its Action Plan

THE MANAGEMENT BOARD OF ENISA

Having regard to

The Treaty on the Functioning of the European Union (TFEU), in particular Article 325.1;

The Staff Regulations of Officials, laid down by Council Regulation (EEC, EURATOM, ECSC) No 259/68 (hereinafter referred to as "Staff Regulations") and to the Conditions of Employment of Other Servants of the European Union (hereinafter referred to as "CEOS"), both as latest amended by Regulation3 (EU, EURATOM) No 1023/2013 of the European Parliament and of the Council of 22 October 2013, and in particular, Articles 11a, 12a, 12b, 16 and 22a;

The Regulation (EU) (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), in particular Article 15.1 (h), 20.1 (k) and 33

The Decision No MB/2020/9 of the Management Board of the European Union Agency for Cybersecurity (ENISA) on the establishment of ENISA's internal structures;

Decision No MB/2019/8 of the Management Board of ENISA the European Union Agency for Cybersecurity on the Financial Rules applicable to ENISA in conformity with the Commission Delegated Regulation (EU) No 2019/715 of 18 December 2018 of the European Parliament and of the Council (hereafter "ENISA's Financial Rules");

The Decision No MB/2019/13 of the Management Board of the European Union Agency for Cybersecurity (ENISA) delegating the relevant appointing authority powers to the Executive Director;

Whereas

- The European Union (EU) budget represents taxpayers' money to be spent only for implementing the policies approved by the EU legislator. Fraud involving EU funds has a particularly negative impact on the reputation of the EU institutions and on the implementation of EU policies.

- OLAF's Methodology and guidance for anti-fraud strategies for EU decentralised agencies (reference- European Anti-Fraud Office, Methodology and guidance for anti-fraud strategies for EU decentralised agencies, Ref. Ares(2013)3560341, 25.11.2013, as well as the last update of the same Methodology dated 23.02.2016, ref. Ares(2016)931345) proposes for the management boards of new agencies to adopt an anti-fraud strategy which is proportionate to their fraud

risks, having due regard to the costs and benefits of the measures to be implemented. While ENISA in not a new agency, the methodology proposed by OLAF is a valid tool for drafting the ENISA Anti-fraud strategy.

- The Anti-Fraud Strategy and Action plan already in place was adopted by Management Board DECISION No MB/2014/14 under the previous legal mandate of the Agency. The current Anti-Fraud Strategy of ENISA needs therefore to be revised and updated to comply with the new mandate of the Agency provided by the Cybersecurity Act.
  The present ENISA Anti-Fraud strategy takes into account the objectivities set by the European Commission in its Anti-Fraud Strategy (COM(2019) 196 final) and is based on lessons learnt, actions implemented and experience acquired in this field. The latter will allow the EIT to pro-actively continue to reinforce a strong anti-fraud culture and actively encourage fraud prevention with dedicated actions designed to the specifics of the EIT's activities.
- The European Commission also developed a Common Approach for the EU decentralised agencies that, among others, outlines principles for prevention, detection and investigation of fraud, corruption, irregularities and other illegal activities. (reference: https://ec.europa.eu/archives/commission_2010-2014/sefcovic/documents/120719_agencies_common_appr_en.pdf)
- The next update of the ENISA Anti-fraud strategy should be alignedwith the planned update of the Commission's Anti-Fraud Strategy, which is expected after the mid-term review of the Multiannual-Finanical Framework 2021-2027.

HAS DECIDED AS FOLLOWS:

Article 1

To adopt the ENISA Anti-Fraud strategy for the period of 2021- 2024 and it action plan annexed to this Decision.

Article 2

(1) This anti-fraud strategy enters into force on the day of its adoption and shall be reviewed in 2024.

(2) The risk assessment and the action plan is subject to yearly review depending on fraud and irregularities indicators reported to OLAF such as number of reported cases and dismissed cases, but also internal reporting received on suspicious behaviour through internal whistleblowing or fraud reporting. The risk assessment shall also include risk related to internal threats.

(3)

Done by written proceudure on 11 February 2021.

For ENISA
On behalf of the Management Board

[Signed]

Jean Baptiste Demaison
Chair of the Management Board

Annex of the Decision No MB/2021/5
of the Management Board
of the EU Agency for Cybersecurity
On ENISA Anti-Fraud Strategy and its action plan

ENISA Anti-Fraud Strategy
2021- 2024

1. GENERAL CONTEXT

The European Union (EU) budget represents taxpayers' money to be spent only for implementing the policies approved by the EU legislator. Fraud involving EU funds has a particularly negative impact on the reputation of EU institutions and on the implementation of EU policies.

On 29 April 2019, an updated Commission Anti-Fraud Strategy (CAFS) 2019 was adopted. After evaluating the 2011 CAFS, it was concluded that the strategy is still relevant and effective as a policy framework for the Commission protecting the EU budget. The CAFS 2019 is included in the action plan of this Anti-Fraud Strategy.

The European Commission has also developed a Common Approach[i] on EU decentralised agencies that requires a set of anti-fraud measures to be put in place by the agencies. Taking into consideration the priorities set by the European Commission within the framework of the Common Approach on EU decentralised agencies, the need to pursue the European Commission's main objectives for its implementation ("more balanced governance, improved efficiency and accountability and greater coherence"), the Management Board of ENISA adopted its Anti-Fraud Strategy and the related Action Plan in 2014, which is now updated according to the future obligations and target points for the years 2021-2024.

Moreover, the Anti-Fraud Strategy and its action plan should be aligned with provisions of the Article 33 of the Regulation (EU) 2019/881. This provision calls upon ENISA to combat fraud, corruption and other unlawful activities. The Anti-Fraud Strategy is part of the legal framework of the Agency and meets the requirements of Article 32 of the Framework Financial Regulations of the European Commission which refers inter alia to the need to prevent and detect irregularities and fraud. The updated OLAF's Methodology and guidance for anti-fraud strategies for EU decentralised agencies point out that "the anti-fraud strategy is part of risk management, but given the importance and complexity of the issue, fraud should be addressed in a dedicated process, which runs on top of the annual risk management exercise, though closely interlinked with it". Therefore, although it is part of the internal control system, the ENISA Anti-Fraud Strategy must be consideredas a separate, additional tool to further strengthen the internal control systems.

2. THE ENISA CONTEXT

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cybersecurity policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow.
Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure.

The Agency works closely together with Member States and the private sector to deliver advice and solutions as well as improving their capabilities. This support includes inter alia:

- Pan-European Cybersecurity Exercise;,
- The development and evaluation of National Cybersecurity Strategies;
- CSIRTs cooperation and capacity building;
- Studies on IoT and smart infrastructures, addressing data protection issues, privacy enhancing technologies and privacy on emerging technologies, eIDs and trust services, identifying the cyber threat landscape, among others.

ENISA also supports the development and implementation of the European Union's policy and law on matters relating to network and information security (NIS) and assists Member States and European Union institutions, bodies and agencies in establishing and implementing vulnerability disclosure policies on a voluntary basis.

As a result of the entry into force of the Cybersecurity Act in 2019 (Regulation 2019/881), ENISA has been tasked to prepare 'European cybersecurity certification schemes' serving as the basis for the certification of products, processes and services with the objective tosupport the delivery of the Digital Single Market.

The European Cybersecurity Act introduces processes designed to support the cybersecurity certification of ICT products, processes and services. In particular, it establishes EU wide rules and European schemes for cybersecurity certification of such ICT products, processes and services.

The main stakeholders of the Agency are:

- The European Commission;
- Member States;
- The ENISA Advisory Group;
- The Stakeholders Cybersecurity Certification Group;

Other major stakeholders includea number of Ad Hoc Working groups/expert groups established to contribute to the implementation of the ENISA Single Programming Document.

The management of funds is notdelegated to any member state and/or organization. All procurement procedures and calls are managed by ENISA.

ENISA implements its budget in accordance with the principles of sound financial management (Article 317 TFEU) and complies with the provision of Article 325 TFEU, according to which the EU, and the Member States, shall counter fraud and any other illegal activities affecting the financial interests of the Union. These articles provide an explicit legal basis for operations by the EU and its bodies and agencies to combat fraud and other unlawful activities. In this light, ENISA is committed to ensuring that the framework, the policies, the rules and the procedures in place enable the effective prevention and detection of fraud.

The risks and anti-fraud measures in this strategy have been communicated to the partner DG CONNECT of the European Commission.

3. DEFINITIONS[1]

3.1 Fraud

[1] Please refer to Annex II for detailed list of definitions relevant to this strategy

Fraud is a deliberate act of deception intended for personal gain or to cause a loss to another party[ii]. It covers any infringement of the financial interests of the EU as defined by the Convention on the protection of the European Union's financial interest ("PIF Convention"). It also covers both misbehaviour that might not have direct impact on the EU's financial interests, but a reputational impact such as some cases of forgery (for example CVs), money laundering, transmission of confidential information, breaches of IT system, cyber fraud and conflict of interests that intentionally have not been declared. Favouritism, plagiarism and collusion also falls into this category.

3.2 An irregularity

An irregularity is an act which does not comply with EU rules and which has a potentially negative impact on EU financial interests, but which may be the result of genuine errors committed both by beneficiaries claiming funds and by the authorities responsible for making payments. If an irregularity is committed deliberately, it is fraud.

4. FRAUD RISK ASSESSMENT

The Agency deals with both direct public procurement and recruitment in-house.

Public procurement, the largest channel of EU public spending, is known to be one of the most significant areas of fraud risk, therefore attractive for fraudsters using corruption as a way of facilitating fraud.

In order to support cooperation between the EU and national governments, our Agency pools technical and specialist expertise from both the EU institutions and national authorities and the EU population in general.

It is crucial for the reputation of ENISA that its staff is selected according to high standards and set criteria. For this reason, favouritism in employment procedures and contracts or other types of fraud needs to be avoided: the selection and related contract shall be the result of the choice of the best candidates. Breaches of both public procurement and recruitment rules can be prevented, minimised and avoided if comprehensive action plans, measures and initiatives are put in place, followed up and updated regularly.

The initiatives to be taken to that end are meant to gradually improve the quality of procurement and recruitment procedures and strengthen the fight against fraud.

The following fraud risks have been identified:

Area	Risks identified
ENISA Staff/Organisation	Lack of ethics/code of conduct policy
	Lack of anti-fraud policy
	Overcharging on Missions
Procurement	Breach of confidentiality
	Embezzlement
	Conflicts of interests
	Collusion
	Corruption
	Falsification of documents/information
	Favouritism
	Leakage of information
	Non-compliance
	Wilful destruction of records

Recruitment	Conflicts of interests
	Corruption
	Falsification of documents/information
	Favouritism
	Lack of control/crosschecking of documents received
	Leakage of information
	Non-compliance
	Wilful destruction of records
Asset management/Inventory	Embezzlement

5. OBJECTIVES AND ACTIONS

Based on the fraud risks identified above, ENISA concentrates its efforts on achieving the set of objectives listed below, according to the specific areas identified above and aiming at covering the fraud cycle: prevention, detection, investigation and correction/sanctioning. ENISA needs to set certain objectives to counter fraud at all levels – the level of the Governing Board, the ENISA Staff and external contractors and thus reinforce the public trust in ENISA activities.

Whilst prevention remains one of the most important objectives of the present Anti-Fraud Strategy, it is deemed appropriate to focus efforts on detection, in particular by internal reporting of any possible case of fraud as well as proactive random verification in some areas.

In order to address the risks identified in the section above, the following strategic objectives were agreed and endorsed by the ENISA Executive Director:

5.1 Objective 1: Integrity and compliance through efficient and targeted communication on ethics and fraud awareness.

The objective follows the need to constantly communicate the rules and the ethical values of the EU Public service to all levels of staff. It is understood that fraud deterrence is facilitated by wide-spread common knowledge and awareness of relevant rules underlining any activity of ENISA.

- The compulsory training course on ethics, integrity, and fraud prevention, and detection for all staff members thus aiming to promote the values of ethics and integrity amongst staff members.

- The assignment of an Anti-Fraud coordination function would help tailor advice to thedifferent units of ENISA as well as individually to newcomers.

The objective here is to ensure that all Staff of the Agency complies and maintains the highest standards of professional ethics (specifically in relation to the prevention and detection of fraud). It is highly important to establish a general ethical culture at ENISA. Fraud prevention needs to be accompanied by a culture of integrity and service to the common interest, with the aim to create and maintain a good reputation of ENISA and trust in the programmes it develops.

5.2 Objective 2: Compliance and transparency measures in Procurement.

The objective is to ensure procurement procedures are compliant and transparent throughout all stages of each process — from planning a procurement to contract implementation — while highlighting risk areas. The tasks of ENISA are strictly linked to legal documents and related regulations tenderers, contractors, /beneficiaries, /candidates, external experts, etc. are legally bound to. This is why, it remains crucial to set-up measures and controls designed to detect and investigate fraud, in addition to the preventive measures (mitigating controls) already in place.

This objective is of paramount importance, within the perspective of the other objectives mentioned.

5.3 Objective 3: Compliance and transparency measures in Recruitment.

This objective is to ensure compliance and transparency of all recruitment procedures at everystage of the process – from selection to employment contract signature.

Favouritism in employment procedures and employment contracts needs to be avoided. It is also understood that the recruitment fraud can also occur when a member of staff or applicant makes false representation, wrongfully fails to disclose information or abuses a position of trust for personal gain. During the recruitment process, applicants making false representations of themselves can be considered a criminal offence. While lying on an application form, CV, or presenting a fake certificate or diploma, but presenting this information as real, fraud is being committed and can be prosecuted. Conducting background screening highlights CV or application misrepresentations and protects business.

This objective is of paramount importance, in the light of the other objectives mentioned. Staff play a key role in implementing and fostering a 'zero tolerance' culture towards fraud and corruption.

5.4 Objective 4: Compliance and transparency measures in Assets management/inventory.

The objective is to ensure that the Agency's assets are not being used in a fraudulent and inappropriate way. It aims at ensuring a proper policy is applied and procedures compliant and transparent through all stages – from recording to declassification.

5.5 Objective 5: Establish a system for internal reporting of syspected fraud or irregularities.

The objective is to establish a system of appropriate tools, applications, reporting mechanisms and guidance and to make these available in order to address all the areas presenting potential risk. It should also take account all systems and tools in place for internal controls framework.

6. ROLES AND RESONSIBILITIES

While it is essential that all ENISA staff members should have a clear understaning of ENISA's Anti-Fraud Strategy and its action plan, some individuals and ENISA structural entities may have intrinsic roles or responsibilities and these are identified below.

6.1. ENISA Management Board

The Management Board of ENISA is responsible for the adoption of the ENISA Anti-Fraud Strategy.

6.2. ENISA Executive Director

The Executive Director of ENISA leads by example by promoting an anti-fraud culture across ENISA, sets anti-fraud objectives, monitors the implementation of the strategy and its action plan and puts in place effective arrangements for combating fraud.

TheExecutive Director will report once a year to the Chairman of the ENISA's Management Board on the ongoing or closed OLAF cases via the Annual Activity Report. Cases with significant financial or reputational risk are in addition reported during theclosed sessions of the Meetings of the Management Board.

6.3. Heads of Unit and Team Leaders

The Head of Unit or Team Leader is the "fist line controls" for the prevention and detection of fraud. He/she is responsible for promoting the anti-fraud culture within their units/teams empowered to ensure staff awareness and facilitate the immediate reporting of suspectedcases of potential fraud to the ENISA Executivee Director/Anti-Fraud coordinator therefore without delay, and coordinating with all other actorsinvolved in or responsible for the implementation of the Anti-Fraud Strategy.

6.4. Anti-Fraud Coordinator

The Anti-Fraud coordinator is responsible for identifying and preventing the risks of breach of legal provisions and breach of ethical behaviour rules which may lead toliabilities or reputational damage for ENISA. The role of the Anti-fraud coordinator is to:

- coordinate the implementation of the Anti-Fraud Strategy;
- follow up on actions;
- report to the Executive Director on such implementations;
- act as a contact point for OLAF on strategy related issues.
- provide advice, guidance on managing the fraud risk;
- design additional controls;
- provide induction to the newly recruited staff.

6.5. Head of Finance/procurement sector

The Head of Finance/procurement sector has the responsibility to ensure that financial systems and procurement procedures incorporate strong measures to reduce the risk of fraud and enable the detection of potential fraud cases at an early stage. He also contributes to promoting staff awareness on the anti-fraud principles and on the Strategy. He is empowered to propose sanctions commensurate with the offense or misconduct by the relevant staff member, as decided by the Director in accordance with the reports and recommendations drawn up following the OLAF investigation.

6.6. Internal Control and compliance assistant

This is a new function to be assigned in the Agency after the present decision is adopted.

The internal control and compliance assistant coordinates the overall implementation of the agreed actions of the annual anti-fraud risk assessment. He/she is responsible to inform the Anti-fraud Coordinator as well as the Executive Director, whenever it gets any information relating to possible cases of fraud, corruption or other irregularities that could affect the Communities' financial interests.

OBJECTIVE 1	Integrity and compliance through efficient and targeted communication on ethics and fraud awareness	
	Measure(s)	**Deadline**
Action	Adopt a Code of good administrative behaviour.	01.05.2021
Action	Maintain regular communication to ENISA staff, members of ENISA statutory bodies and members of the Ad Hoc Working Grops/expert groups on anti-fraud related matters.	continuously
Action	Assign an Anti Fraud coordinator function at ENISA who will maintain regular communication on anti-fraud related matters to newly recruited staff by providing an introduction to the ENISA anti-fraud strategy and to the ENISA Code of good Administrative behaviour. He/she shall be properly trained to become the ENISA contact point for OLAF related issues (transmission of cases to OLAF, answering to requests of OLAF, and possibly give advice to Staff in case of fraud suspicions, how and when to report, etc.). Furthermore, the Anti Fraud coordinator function should ensure regular communication with the EC, in particular with OLAF and DG CONNECT in order to follow up and receive updates on trainings/info sessions, legal developments and learn from their experience.	As needs arise (depending on the arrival of new staff)
Action	Provide mandatory and continuous fraud awareness and ethics and integrity trainings/info sessions with the support of the EC, in particular of OLAF and DG CONNECT. Mandatory regular training sessions should be provided also to Authorising Officers, Finance and Procurement staff and HR staff with specific attention to procurement and recruitment (Objective 3 and Objective 4).	Continuous
Action	Prepare an Activity report on the activities implemented to achieve the goals of the Anti-fraud Strategy.	01.07.2024

6.7. Staff members

Staff members are subject to certain obligations laid down in the Staff Regulations (such as conflicts of interest, gifts, external activities, spouse's employment, or publications or speeches on EU-related matters (Articles 11, 11a, 12, 12b,13, 15, 16 17, 17a and 19 of the Staff Regulations)). They are obliged to report facts pointing to a possible illegal activity, including fraud or corruption, or to a serious failure to comply with the professional obligations as staff pursuant to Article 22a of the Staff Regulations.

All staff members are meant to comply with the ENISA Anti-Fraud principles and the present strategy. Staff are also expected toforward any reasonable concerns with regard to fraud to their head of unit, the reporting officer, and/or the Executive Director in accordance with the existing guidelines, for example, following the internal whistleblowing procedure.

7. ACTION PLAN

An action plan is devised as follows to meet the objectives mentioned above. This action plan is

intended to implementthe ENISA Anti-fraud strategy and ensurethe sound management of public procurement, recruitment and the other risk areas identified.

OBJECTIVE 1 INDICATORS:

- Adoption of the Code of good administrative behaviour;
- Assignment of the Anti-Fraud coordinator function;
- Logs of requests for advise from Staff to Anti-Fraud coordinator;
- Fraud related page on internal ENISA created and maintained;
- Number of training sessions with % attendance of: 100% staff for general fraud awareness and ethics and intregrity trainings and 100% staff for newcomers trainings;
- Annual implementation report as part of the AAR.

OBJECTIVE 2	**Compliance and transparency measures in Procurement.**	
	Measure(s)	**Deadline**
Action	Regularly consult the EDES (Early-Detection and Exclusion System).	Continuous
Action	Reinforce fraud detection measures for documents submitted as part of a tender procedure to facilitate the identification of any legal document, report or timesheet not compliant with ENISA/national authorities' requirements..	Continuous
Action	Set-up of policies and procedures for declaring, assessing and managing conflicts of interests.	Continuous
Action	Implement the mandatory signing of declarations of conflict of interest and confidentiality declarations by all experts applying to a Call of Expression of Interest (CEI) list and by parties contracted through a procurement procedure.	Continuous

OBJECTIVE 2 INDICATORS:

- N. of ENISA flagings/year;
- Number of investigations implemented by Departments/Units per year;
- Guidance published on intranet on the policy on conflict of interests.

OBJECTIVE 3	**Compliance and transparency measures in Recruitment.**	
	Measure(s)	**Deadline**
Action	Review policies and procedures for declaring, assessing and managing conflicts of interests in the context of risk or fraud.	Continuous

OBJECTIVE 3 INDICATORS:

- Guidance published on intranet on the policy on conflict of interests;
- Missing documents from Recruitment selection procedures and Staff members personal files.

OBJECTIVE 4	**Compliance and transparency measures in Assets management/Inventory.**	
	Measure(s)	**Deadline**
Action	Continuously update of the policy on assets management/inventory, including inventory control policy, declassification policy and ensure adequate internal controls.	Continuous

OBJECTIVE 4 INDICATORS:

- Publication on the intranet of guidance on the policy on assets management/inventory. ;
- Excessive inventory shrinkage;
- Excessive number of adjusting entries.

OBJECTIVE 5	**Establish a system for internal reporting of suspected fraud or irregularities.**	
	Measure(s)	**Deadline**
Action	Carry out annual fraud risk assessment as part of the annual risk assessment (mainly focussed on processes and sensitive functions).	Continuous
Action	• Develop a Document classification policy and ensure its proper implementation; • Adopt other technical measures as appropriate to enhance data security, in particular, a secure mail system.	For document classification policy 01.01.2022. For the rest-continuous
Action	Implement the ENISA whistleblowing policy by putting in place internal reporting and whistleblowing procedures.	01.01.2022
Action	Create an online page with a template (Annex I) on ENISA's website for reporting on whistleblowing and fraud.	01.01.2022
Action	Create an internal whistleblowing and fraud register for reported fraud and irregularities.	01.01.2022
Action	Revise - and develop if needed - check lists for financial transactions (financial circuit), procurement procedure steps (including contracts), and missions.	Continuous

Action	Create a dedicated page on the ENISA staff intranet is created for anti-fraud tools to be more visible. It may includes such items as: • reporting template; • anti-fraud procedures; • anti-fraud activities performed by the Anti-Fraud coordinator; • Etc.	01.07.2021.

OBJECTIVE 5 INDICATORS:

- N. of ENISA flagings/year as per OLAF's recommendation or per ENISA Whistleblowing policy;
- Annual implementation report as part of the AAR.

8. THE FRAUD REPORTING PROCEDURES

8.1 MECHANISM FOR REPORTING IRREGULARITIES OR ALLEGED FRAUD

All ENISA staff members (including seconded national experts, interim agents, or other external workfoce working at ENISA) are expected to report irregularities and alleged frauds. Different mechanisms are in place to report possible fraudulent behaviour.

As per Article 22a of the Staff Regulations, staff members can report to their immediate supervisor or to the Executive Director. In case the staff member considers that taking such action might endanger their position, he or she can report directly to the Chair of the Management Board or to OLAF.

As per Article 22b of the Staff Regulations, staff members can alternatively address their concerns to another institution (e.g. President of the Commission or of the Court of Auditors or of the Council or of the European Parliament, or to the Europen Ombudsman).

As per Article 22c of the Staff Regulations, each institution shall in accordance with articles 24 and 90 of the Staff Regulations, put in place a procedure for the handling of complaints made by staff members concerning the way in which they were treated after or as a consequence of fulfilling their obligations under the above Articles 22a or 22b of the Staff Regulations.

Protection of whistleblowers is provided for in the ENISA whistleblowing strategy, and in Annex 3 which addresses specifically the protection of personal data.

8.1.1 OPTION TO REPORT DIRECTLY TO ENISA

Staff members will be able to report on alleged fraud directly, either through the reporting template in Annex 1 of this Stategy , or through an anonymous template on ENISA's website.

8.1.2 WHEN TO REPORT TO OLAF?

OLAF investigates corruption and serious misconduct within the European institutions, fraud against the EU budget and develops the anti-fraud policy for the European Commission.

Reporting on alleged fraud or serious irregularity can be done:

- In case the staff member whowishes to report considers that taking such action might endanger their position at the Agency;
- In case of alleged fraud or other serious irregularities with a potential negative impact for EU public funds, whether EU revenue, expenditure or assets held by EU institutions;
- In case of serious misconduct by Members or staff of EU Institutions and bodies.

Fraud and irregularities are not to be confused with alleged maladministration or broader systemic issues by EU institutions and bodies. Such issues fall into the authority of the European Ombudsman as provided for in Article 22b of the Staff Regulations.

ANNEX 1 – Reporting template for transmission of alleged fraud

What are you reporting?

How do the irregularities, fraud or corruption you want to report relate to the European Union?

Select the one or more options of the checkboxes below, as appropriate:

- Irregularities detrimental to ENISA Budget ☐
- Serious misconduct by Members, Stakeholders or Staff of ENISA ☐
- Serious violations of professional duties committed by ENISA's Staff ☐
- I do not know ☐

Please describe the facts as objectively as possible and explain how you have becomeaware of the facts.

Do you know when the irregularities occurred?

Have you reported these irregularities to other bodies or authorities?
If yes, please indicate the name(s) of these organisation(s)and the date you contacted them.

You can optionally upload a single attachment if you wish.

ANNEX 2 –Lexicon

Non-exhaustive list of actions considered to fall within the definition of fraud or linked to fraud:

- **breach of confidentiality**: when data or private information is disclosed to a third party without the data owner's consent. It is generally considered as a disclosure of confidential information (depending upon the definition of confidential information)**;**
- **embezzlement**: is the act of withholding assets for the purpose of conversion (theft) of such assets, by one or more persons to whom the assets were entrusted, either to be held or to be used for specific purposes. Embezzlement is a type of financial fraud;
- **conflicts of interests**: situation where the impartial and objective exercise of the functions of a financial actor or other person is compromised for reasons involving family, emotional life, political or national affinity, economic interest or any other shared interest with a recipient;
- **collusion**: agreement between two or more parties, sometimes illegal and therefore secretive, to limit open competition by deceiving, misleading, or defrauding others;
- **corruption**: abuse of entrusted power for private gain. Corruption practices hurt everyone dependent on the integrity of people in a position of authority;
- **double claiming of costs**: submitting the same items of expenditure to different funding sources in parallel in order to obtain the same financial support from different parties;
- **extortion, blackmail, bribery**: requesting or accepting money or valuables to influence the award of a grant or contract;
- **falsification of documents**: is the act of intentionally changing or modifying information on a document with the intention of misleading a person or company;
- **favouritism**: preference given to acquaintances, friends and family over strangers. When public (and private sector) officials demonstrate favouritism to unfairly distributed positions and resources, they are guilty of cronyism or nepotism, depending on their relationship with the person who benefits;
- **fraudulent bankrupcy** may occur in various ways but one of the most common methods of indulging in fraud is to make false statements with regards to one's assets while filing a claim for bankruptcy protection. Concealment of assets from the court can be done by illegal transfer of money to family members or friends, shift the property or assets to offshore accounts and failing to report the various sources of income;
- **leakage of information** takes place when confidential information is revealed to unauthorized persons or parties;
- **non-compliance** with the provisions and/or legal requirements of the contract or grant agreement (e.g. non respect of the obligation to organize tenders or market consultations for subcontracted activities);
- **overcharging** (by forgery or alteration of documents, e.g. by knowingly generating false time sheets or invoices, by declaring fictitious contractors or employees or unjustified trips, or by using substandard materials);
- **plagiarism**: use or close imitation of the language and ideas of another author and representation of them as one's own original work;
- **wilful destruction** or removal of records intentionaly.

Abbreviation	Meaning
OLAF	Office Européen de Lutte Antifraude (European Anti-Fraud Office)
OLAF Regulation	Regulation (EU, Euratom) No 883/2013
PIF	Protection des Intérêts Financiers des Communautés européennes (Protection of the EU's financial interests)
PIF Directive	Directive (EU) 2017/1371
SG	Secretariat-General
LS	Legal Service
SOCTA	Serious and Organised Crime Threat Assessment
SPP	Strategic Planning and Programming
TFEU	Treaty on the Functioning of the European Union
TOR	Traditional own resources
VAT	Value Added Tax

891