European Union Agency
for Cybersecurity

Agamemnonos 14
Chalandri 15231 | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

ANNEX – JOB DESCRIPTIONS

A. POLICY DEVELOPMENT AND IMPLEMENTATION UNIT (PDI)

Core tasks and responsibilities:

- Review of Union policy and law in the field of cybersecurity and on sector-specific policy and law initiatives where matters related to cybersecurity are involved, provide independent opinion and analysis as well as carry out preparatory work;
- Assist Member States and their competent authorities to implement Union policy and law regarding cybersecurity consistently, by means of issuing opinions, guidelines, providing and facilitating advice and best practices on topics related to current policies, e.g. NIS Directive, eIDAS, EECC, 5G, GDPR, as well as future ones, e.g. NIS Directive 2.0
- Assist Member States and Union institutions, bodies, offices and agencies in developing and promoting cybersecurity policies related to sustaining the general availability or integrity of the public core of the open internet;
- Contribute to the work of formally established EU Expert Groups and bodies (such as the Cooperation Group, Cooperation Network) by providing its expertise and assistance;
- Support the development and implementation of Union policy in the fields of electronic identity, trust services and cybersecurity aspects of privacy and data protection;
- Support the regular review of Union policy activities by preparing an annual report on the state of the implementation of the respective legal framework regarding:
    - information on Member States' incident notifications provided by the single points of contact to the Cooperation Group;
    - summaries of notifications of breach of security or loss of integrity received from trust service providers provided by the supervisory bodies to ENISA;
    - notifications of security incidents transmitted by the providers of public electronic communications networks or of publicly available electronic communications services, provided by the competent authorities to ENISA.
- Organise, synthetize and prioritize data information from many different sources and according to evolving or changing circumstances;
- Deal with sensitive data and information and translate these into objective and transparent policies;
- Be expert in specific domains of cyber security and take responsibility to drive policy development and implementation from this perspective;
- Lead and be perceived as trusted advisor in Policy Management & Implementation, be up to speed with latest developments and assess their impact on policy development
- Bring a strategic perspective on policy development by creating synergies on policy development across functional as well as geographical domains;
- Administer communities of stakeholders and international relations in the designated competence areas.

Competency profile for Policy Development and Implementation: outlines the core competencies needed for the job role in scope as well as the target proficiency levels per selected competency, based on experience (depicted here on a continuum from left to right).

Foundation **I**ntermediate **E**xpert	Target proficiency level		
Corporate DNA - Analysis and decision making			
Ability to collect, analyse and report information	I	E	E
Risk and conflict management	F	I	I
Work organisation and prioritisation skills	F	I	E
Corporate DNA - Attitude and behaviour			
Objectivity & transparency	I	E	E
Responsibility and ownership	I	E	E
Team work and collaboration	F	I	I
Corporate DNA - Communication			
Presentation and public speaking	F	I	I
Drafting skills	I	I	E
Corporate DNA - Stakeholder relations and management			
Focus on excellence and quality	F	I	E
Internal and external service orientation	F	I	I
Corporate DNA - Project management			
Project management	F	I	I
Next Gen			
Policy advising	I	E	E
Innovation and market foresight	F	I	E
Strategic thinking	I	E	E
Functional			
Cybersecurity technical competencies	I	E	E

B. CAPACITY BUILDING UNIT (CBU)

Core tasks and responsibilities:

- Collect, analyse and compile data originating from various sources on such areas as threat intelligence, threat landscape, risk management/assessment and associated methodologies and tools as well as communication, education and behavioural sciences, capacity building international initiatives;
- Improve the prevention, detection and analysis of, and the capability to respond to cyber threats and incidents by providing Member States with knowledge and expertise in cyber security (in particular through support for the CERT-EU);
- Offer trainings regarding cybersecurity to relevant public bodies, where appropriate in cooperation with stakeholders;
- Support in developing national CSIRTs and national strategies on the security of network and information systems and promote the dissemination of those strategies;
- Monitor the progress in the implementation of cybersecurity strategies across the Union;
- Raise the capability levels of national and Union CSIRTs by promoting dialogue and exchanges of information and best practices to enable that CSIRT's possess a common set of minimum capabilities and operate according to best practices;
- Regularly organise cybersecurity exercises at Union level, making policy recommendations based on the evaluation process of the exercises and lessons learned from them;

- Support information sharing in and between sectors, by providing best practices and guidance on available tools, procedures, as well as on how to address regulatory issues related to information-sharing;
- Continuously consult network within ENISA as well as with external stakeholders to ensure capacity building initiatives remain in line with ENISA's strategy, the stakeholder needs and latest cyber security developments;
- Prioritise and manage projects according to ENISA's strategy and aim for synergies across capacity building initiatives to drive effectiveness and efficiency;
- Administer communities of stakeholders and international relations in the designated competence areas;
- Administer and manage awareness raising and education initiatives whose goal is to promote safer online behaviour by individuals and organisations;
- Research on scientific methods that lead to behavioural change through awareness raising and education;
- Assist with the design of a stakeholder engagement strategy.

Competency profile for Capacity Building: outlines the core competencies needed for the job role in scope as well as the target proficiency levels per selected competency, based on experience (depicted here on a continuum from left to right):

Foundation **I**ntermediate **E**xpert	**Target proficiency level**		
Corporate DNA - Analysis and decision making			
Problem solving	I	I	E
Work organisation and prioritisation skills	F	I	I
Corporate DNA - Attitude and behaviour			
Adaptability & flexibility	I	I	I
Cultural awareness	F	I	E
Respect and openness towards others	F	I	E
Team work and collaboration	F	I	I
Corporate DNA – Communication			
Presentation and public speaking	I	E	E
Drafting skills	I	I	E
Corporate DNA - Stakeholder relations and management			
Focus on excellence and quality	F	I	E
Internal and external service orientation	I	E	E
Corporate DNA - Project management			
Project management	F	I	I
Next Gen			
Knowledge sharing & education	I	E	E
Network & community development	F	I	E
Policy advising	I	I	E
Innovation and market foresight	I	E	E
Strategic thinking	F	I	E
Functional			
Cybersecurity technical competencies	I	E	E
IT management	F	I	E

C. OPERATIONAL COOPERATION UNIT (OCU)

Core tasks and responsibilities:

- Support operational cooperation among Member States, Union institutions, bodies, offices and agencies, and between stakeholders;
- Cooperate at the operational level and establish synergies with Union institutions, bodies, offices and agencies, including the CERT-EU, with the services dealing with cybercrime and with supervisory authorities dealing with the protection of privacy and personal data, with a view to addressing issues of common concern;
- Provide the secretariat of the CSIRTs network;
- Support Member States with respect to operational cooperation within the CSIRTs network by:
    - advising on how to improve their capabilities;
    - assisting in the assessment of incidents;
    - providing advice in relation to a specific cyber threat at the request of one or more Member States;
    - analysing vulnerabilities and incidents on the basis of publicly available information or information provided voluntarily by Member States;
    - providing support in relation to ex-post technical inquiries regarding cyber security incidents having a significant or substantial impact;
- Engage in structured cooperation with CERT-EU to benefit from synergies and to avoid the duplication of activities;
- Prepare a regular in-depth EU Cybersecurity Technical Situation Report on incidents and cyber threats based on publicly available information, its own analysis, and reports shared by Member States' CSIRTs or other relevant public authorities;
- Contribute to developing a cooperative response at Union and Member States level to large-scale cross- border incidents or crises related to cybersecurity, mainly by:
    - aggregating and analysing reports from national sources;
    - ensuring the efficient flow of information and the provision of escalation mechanisms between the CSIRTs network and the technical and political decision-makers at Union level;
    - facilitating the technical handling of such incidents or crises;
    - supporting Union institutions, bodies, offices and agencies and Member States, in the public communication relating to such incidents or crises;
    - testing the cooperation plans for responding to such incidents or crises.
- Administer communities of stakeholders and international relations in the designated competence areas.

Competency profile for Operational Cooperation: outlines the core competencies needed for the job role in scope as well as the target proficiency levels per selected competency, based on experience (depicted here on a continuum from left to right).

Foundation **I**ntermediate **E**xpert	**Target proficiency level**		
Corporate DNA - Analysis and decision making			
Problem solving	I	I	E
Work organisation and prioritisation skills	F	I	I
Corporate DNA - Attitude and behaviour			
Adaptability & flexibility	I	I	I

Respect and openness towards others	F	I	E
Team work and collaboration	F	I	I
Corporate DNA - Communication			
Presentation and public speaking	F	I	I
Drafting skills	I	I	E
Corporate DNA - Stakeholder relations and management			
Focus on excellence and quality	F	I	E
Internal and external service orientation	I	E	E
Corporate DNA - Project management			
Project management	F	I	I
Next Gen			
Knowledge sharing & education	F	I	I
Network & community development	I	E	E
Policy advising	I	I	E
Functional			
Cybersecurity technical competencies	I	E	E
IT management	F	I	E