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/2020/8
of the Management Board of
the European Union Agency for Cybersecurity

on the general direction of the operation of ENISA
(ENISA Strategy)

The MANAGEMENT BOARD OF ENISA,

Having regard to the Regulation (EU,Euratom) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and repealing Regulation (EU) No 526/20131, in particular Article 15.1 (a);

Whereas a strategy is a result of close cooperation between ENISA Executive Director, its staff and the Management Board after seeking input from the ENISA Advisory Group and after having series of workshops and consultation rounds with ENISA staff, the ENISA Management Team and the Management Board;

Whereas the process-principles that this project followed were: Transparency, Inclusiveness, Partnership, Methodology, Legal basis/ Mandate, Review/ Flexibility and Evolution;

Whereas the Executive Board at its meeting held on 29 May 2020 and on 4 June 2020 (continued) has finalised the text of the strategy.

HAS DECIDED TO ADOPT THE FOLLOWING DECISION:

Article 1

1. The ENISA Strategy is adopted as annexed to this decision.

Article 2

1. This Decision shall enter into force on 1st July 2020.
2. The Management Board shall launch a review procedure, if relevant, as from 1st July 2024.

Done by written procedure on 25 June 2020.

On behalf of the Management Board,

[Signed]
Jean-Baptiste Demaison
Chair of the Management Board of ENISA

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1563265599312&uri=CELEX:32019R0881

A TRUSTED AND CYBER SECURE EUROPE

VISION

A trusted and cyber secure Europe

MISSION

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union in cooperation with the wider community. It does this through acting as a centre of expertise on cybersecurity, collecting and providing independent, high quality technical advice and assistance to Member States and EU bodies on cybersecurity. It contributes to developing and implementing the Union's cyber policies.

Our aim is to strengthen trust in the connected economy, boost resilience and trust of the Union's infrastructure and services and keep our society and citizens digitally secure. We aspire to be an agile, environmentally and socially responsible organisation focused on people.

VALUES

Community Mind-Set ENISA works with communities, respecting their competencies and expertise, and fosters synergies and trust to best achieve its mission.

Excellence ENISA aims for state-of-the-art expertise in its work, upholds the highest quality standards of operation and evaluates its performance to strive for continuous improvement through innovation and foresight.

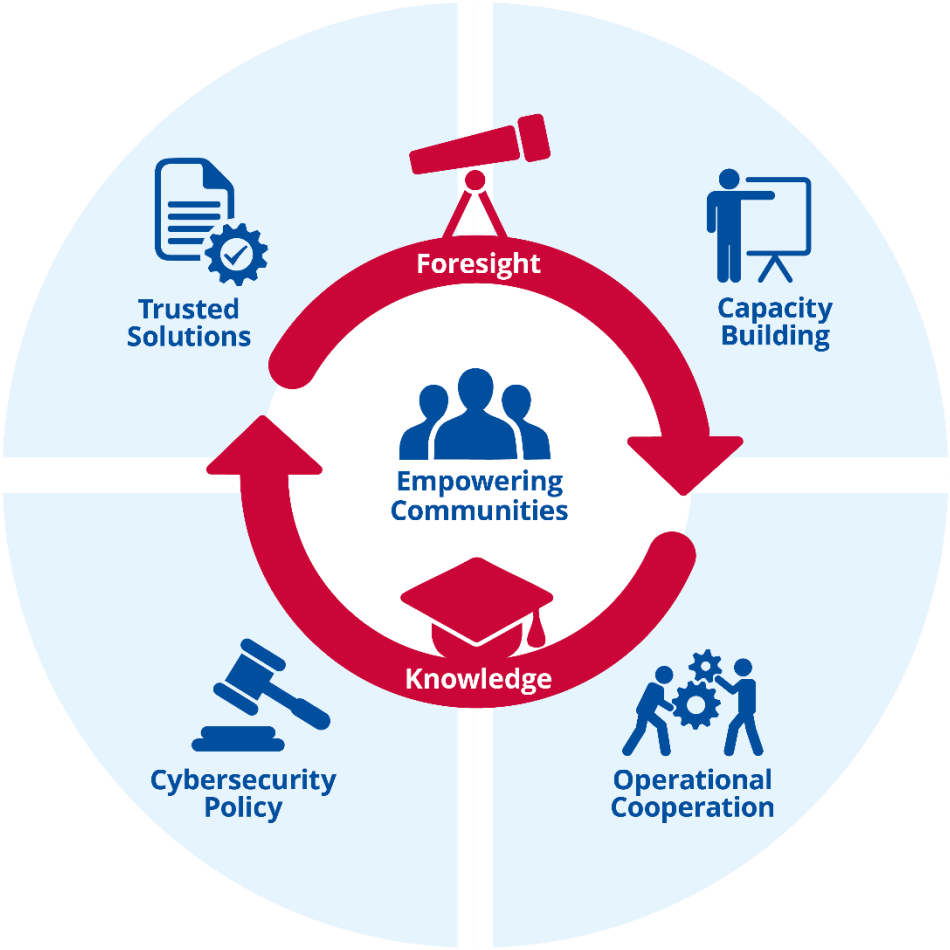
Integrity/ethics ENISA upholds ethical principles and EU relevant rules and obligations in its services and working environment ensuring fairness and inclusiveness.

Respect ENISA respects fundamental European rights and values covering all its services and working environment, as well as the expectations of its stakeholders.

Responsibility ENISA assumes responsibility thus ensuring integration of the social and environmental dimensions into practices and procedures.

Transparency ENISA adopts procedures, structures and processes that are open, factual and independent, thus limiting bias, ambiguity, fraud and obscurity.

OBJECTIVES



SO1 - Strategic objective: "Empowered and engaged communities across the cybersecurity ecosystem"

Context: Cybersecurity is a shared responsibility. Europe strives for a cross sectoral, all-inclusive cooperation framework. ENISA plays a key role in stimulating active cooperation between the cybersecurity stakeholders in Member States and the EU institutions and agencies. It strives to ensure complementarity of common efforts, by adding value to the stakeholders, exploring synergies and effectively using limited cybersecurity expertise and resources. Communities should be empowered to scale up the cybersecurity model.

What we want to achieve:

- An EU-wide, state of the art body of knowledge on cybersecurity concepts and practices, that builds cooperation amongst key actors in cybersecurity, promotes lessons learned, EU expertise and creates new synergies.
- An empowered cyber ecosystem encompassing Member States authorities, EU institutions, agencies and bodies, associations, research centres and universities, industry, private actors and citizens, who all play their role in making Europe cyber secure;

SO2 - Strategic Objective: "Cybersecurity as an integral part of EU policies"

Context: Cybersecurity is the cornerstone of digital transformation and the need for it permeates all sectors, therefore it needs to be considered across a broad range of policy fields and initiatives. Cybersecurity must not be restricted to a specialist community of technical cyber experts. Cybersecurity must therefore be embedded across all domains of EU policy. Avoiding fragmentation and the need for a coherent approach while taking into account the specificities of each sector is essential.

What we want to achieve:

- Proactive advice and support to all relevant EU-level actors bringing in the cybersecurity dimension in policy development lifecycle through viable and targeted technical guidelines;
- Cybersecurity risk management frameworks that are in place across all sectors and followed throughout the cybersecurity policy lifecycle.

SO3 - Strategic objective: "Effective cooperation amongst operational actors within the Union in case of massive cyber incidents"

Context: The benefits of the European digital economy and society can only be fully attained under the premise of cybersecurity. Cyber-attacks know no borders. All layers of society can be impacted and the Union needs to be ready to respond to massive (large scale and cross-border) cyber-attacks and cyber crisis. Cross-border interdependencies have highlighted the need for effective cooperation between Member States and the EU institutions for faster response and proper coordination of efforts at all levels (strategic, operational, technical and communications).

What we want to achieve:

- Continuous cross-border and cross layer support to cooperation between Member States as well as with EU institutions. In particular in view of potential large scale incidents and crises, support the scaling up of technical operational, political and strategic cooperation amongst key operational actors to enable timely response, information sharing, situational awareness and crises communication across the Union;
- Comprehensive and rapid technical handling upon request of the Member States to facilitate technical and operational needs in incident and crises management.

SO4 - Strategic objective: "Cutting-edge competences and capabilities in cybersecurity across the Union"

Context: The frequency and sophistication of cyberattacks is rising speedily, while at the same time the use of ICT infrastructures and technologies by individuals, organisations, and industries is increasing rapidly. The needs for cybersecurity knowledge and competences exceeds the supply. The EU has to invest in building competences and talents in cybersecurity at all levels, from the non-expert to the highly skilled professional. The investments should focus not only on increasing the cybersecurity skillset in the Member States but also on making sure that the different operational communities possess the appropriate capacity to deal with the cyber threat landscape.

What we want to achieve:

- Aligned cybersecurity competencies, professional experience and education structures to meet the constantly increasing needs for cybersecurity knowledge and competences in the EU;
- An Elevated base-level of cybersecurity awareness and competences across the EU while mainstreaming cyber into new disciplines;
- Well prepared and tested capabilities with the appropriate capacity to deal with the evolving threat environment across the EU.

SO5 - Strategic objective: "High level of trust in secure digital solutions"

Context: Digital products and services bring benefits as well as risks, and these risks must be identified and mitigated. In the process of evaluating security of digital solutions and ensuring their trustworthiness, it is essential to adopt a common approach, with the goal to strike a balance between societal, market, economic and cybersecurity needs. A neutral entity acting in a transparent manner will increase customer trust on digital solutions and the wider digital environment.

What we want to achieve:

- Cyber secure digital environment across the EU, where citizens can trust ICT products, services and processes through the deployment of certification schemes in key technological areas;

SO6 - Strategic objective: "Foresight on emerging and future cybersecurity challenges"

Context: Numerous new technologies, still in their infancy or close to mainstream adoption, would benefit from the use of foresight methods. Through a structured process enabling dialogue among stakeholders, decision- and policy-makers would be able to define early mitigation strategies that improve the EU resilience to cybersecurity threats and find solutions to address emerging challenges.

What we want to achieve:

- Understanding emerging trends and patterns using foresight and future scenarios that contribute to mitigating our stakeholder's cyber challenges;
- Early assessment of challenges and risks from the adoption of and adaptation to the emerging future options, while collaborating with stakeholders on appropriate mitigation strategies.

SO7 - Strategic objective: "Efficient and effective cybersecurity information and knowledge management for Europe"

Context: The energy that fuels the mill of cybersecurity is information and knowledge. For cybersecurity professionals to be efficient at tackling our objectives, to work in a constantly moving environment – in terms of digital developments as well as with regard to actors – to face the challenges of our time, we need a continuous process of collecting, organising, summarising, analysing, communicating, and maintaining cybersecurity information and knowledge. All phases are essential to ensure that information and knowledge is shared and expanded within the EU cybersecurity ecosystem.

What we want to achieve:

- Shared information and knowledge management for the EU cybersecurity ecosystem in an accessible, customised, timely and applicable form, with appropriate methodology, infrastructures and tools, coupled and quality assurance methods to achieve continuous improvement of services.