The NIS2 Directive is the EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU.

The EU cybersecurity rules introduced in 2016 were updated by the NIS2 Directive that came into force in 2023. It modernised the existing legal framework to keep up with increased digitisation and an evolving cybersecurity threat landscape. By expanding the scope of the cybersecurity rules to new sectors and entities, it further improves the resilience and incident response capacities of public and private entities, competent authorities and the EU as a whole.

The Directive on measures for a high common level of cybersecurity across the Union (the NIS2 Directive) provides legal measures to boost the overall level of cybersecurity in the EU by ensuring:

- Member States’ preparedness, by requiring them to be appropriately equipped. For example, with a Computer Security Incident Response Team (CSIRT) and a competent national network and information systems (NIS) authority,
- cooperation among all the Member States, by setting up a Cooperation Group
to support and facilitate strategic cooperation and the exchange of information among Member States.

- a culture of security across sectors that are vital for our economy and society and that rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.

Businesses identified by the Member States as operators of essential services in the above sectors will have to take appropriate security measures and notify relevant national authorities of serious incidents. Key digital service providers, such as search engines, cloud computing services and online marketplaces, will have to comply with the security and notification requirements under the Directive.

**NIS 2 Directive (Directive (EU) 2022/2555)**

NIS2 Guidelines - application of Article 4 (1) and (2) of Directive (EU) 2022/2...
NIS2 Guidelines - application of Article 3 (4) of Directive (EU) 2022/2555
Follow the latest progress and learn more about getting involved.
The Commission has published a series of new calls for proposals for the Digital Europe Programme. A dedicated budget of €84 million is available for activities supporting Security Operation Centres with novel applications of AI and other enabling technologies, for the implementation of cybersecurity EU legislation such as the Cyber Resilience Act, as well as for the European transition to post-quantum cryptography.
On 14 December, the European Union (EU) and United Kingdom (UK) held their first Cyber Dialogue in Brussels. Underlining the need to advance an open, free, stable and secure cyberspace respecting human rights and fundamental freedoms, the EU and UK presented their latest developments on a range of cyber policy issues as set out under the EU-UK Trade and Cooperation Agreement (TCA).

The Commission has adopted this week the amendment of the Digital Europe work programmes for 2024, assigning €762.7 million in funding for digital solutions to benefit citizens, public administrations, and businesses.

The European Commission has adopted the amendment of the Digital Europe Programme Work Programmes 2023-2024.
The European Union works on various fronts to promote cyber resilience, safeguarding our communication and data and keeping online society and economy secure.

**Dig deeper**

The Commission, together with European Union Agency for Network and Information Security, works closely with the Member States to ensure the NIS Directive's transposition into national legislation.


The Network and Information Systems Cooperation Group was established by the NIS Directive to ensure cooperation and information exchange among Member States.

See Also


On the 18 April 2023, the European Commission proposed the EU Cyber Solidarity Act, to improve the preparedness, detection and response to cybersecurity incidents across the EU.


New EU cybersecurity rules ensure safer hardware and software.


 Operators of Essential Services (OES), National Cybersecurity Certification Authorities (NCCAs) and National Competent Authorities (NCAs) for cybersecurity are among the selected applicants that will receive €11 million in funding by the Connecting Europe Facility cybersecurity...


The European Cybersecurity Network and Cybersecurity Competence Centre help the EU retain and develop cybersecurity technological and industrial capacities.


The Stakeholder Cybersecurity Certification Group was established to provide advice on strategic issues regarding cybersecurity certification.

The Cybersecurity Act strengthens the EU Agency for cybersecurity (ENISA) and establishes a cybersecurity certification framework for products and services.


The EU cybersecurity certification framework for ICT products enables the creation of tailored and risk-based EU certification schemes.

Source URL: https://digital-strategy.ec.europa.eu/policies/nis2-directive