

Cooperating on cybersecurity

POLICY DEVELOPMENT

PRACTICAL MEASURE/INITIATIVE

 NETHERLANDS

Timeline

2023 Implementation

2024 Implementation

2025 Implementation

ID number 46831

Background

Since the COVID-19 crisis, the use of ICT in education has grown significantly, presenting new challenges in maintaining quality and ensuring secure collaborations between schools and digital learning material suppliers. A series of ransomware attacks, including one targeting a VET college in 2021, has highlighted the urgent need to strengthen the digital security of students and schools. Tackling these challenges will enable VET institutions to harness ICT more effectively, fostering both agility and security in their digital environments.

Objectives

Policy measures regarding digitalisation have two primary objectives:

- (a) to develop an agreement system regarding standardised, secure, and reliable exchange of personal data in the educational context to establish a secure infrastructure for digital teaching and learning resources;
- (b) to ensure the protection of students' and VET schools' private data while enhancing schools' digital resilience against cyber threats.

Description

With regard to the first objective, in 2022, the 10-year programme 'Digital education well organised', now called Edu-V, was allocated EUR 34 million from the National growth fund. During its first year, representatives from VET schools and suppliers of digital teaching and learning resources collaborated on developing an agreement system to ensure easy, secure, and reliable access to digital educational resources. A total of eight working groups collaborated on topics such as the framework for the agreement system, combining and arranging digital learning materials, evaluation of learning progress, examinations, privacy, and the secure exchange of personal data. In total, 200 different parties participated in formulating agreements.

Edu-V was initiated by the Ministry of Education, Culture and Science together with sectoral umbrella organisations, VET representatives and digital education stakeholders. Initiators include the Cooperation Organisation of VET Colleges on ICT (MBO Digitaal), the Foundation for Education and ICT (Kennisset), the councils for primary education, secondary education

and upper secondary VET (PO-Raad, VO-raad and MBO Raad), as well as associations representing media education, digital education service providers and educational distributors. All initiators participate in the relevant Edu-V working groups.

The second objective has been pursued since 2023 through the 'Cybersecurity VET programme' (*Programma Cyberveiligheid mbo*), a five-year initiative with a budget of EUR 24 million. This programme brings together ICT experts and schools to share and disseminate knowledge, enabling schools to better identify cyber risks, implement protective measures, and respond effectively to cyber threats.

In the Cybersecurity VET programme, a governance study, culminating in the final report on information security governance in late 2023, revealed that VET school boards acknowledge the importance of cybersecurity. However, the study found that the level of actual security is influenced by the board's engagement with the topic. Additionally, VET school boards agreed to initiate 'cyber risk pooling', a shared insurance mechanism for security breaches. Furthermore, the Council for Upper Secondary VET Schools (MBO Raad) decided to implement mandatory external cybersecurity audits, replacing the prior practice of internal audits.

The Cyber Risk Pooling agreement in the Dutch MBO sector (agreement system) was adopted by the General Assembly in June 2023 and formally signed by the Council for upper secondary VET schools in September 2023. The Cyber Risk Pooling agreement in the Dutch MBO sector has established since 2023 a sector-wide framework for sharing cyber-risks collectively among VET institutions, replacing traditional individual cyber-insurance. Through this agreement, participating schools commit to mutual financial support in case of cyber incidents, under clear governance and auditing rules. Rather than paying regular insurance premiums, institutions contribute only when actual damage occurs, with compensation determined by an independent claims handler. The arrangement aims to strengthen sector-wide cyber-resilience, encourage cooperation, knowledge exchange, and mutual accountability, and allow savings from avoided insurance costs to be reinvested in preventive and recovery measures.

2023 Implementation

For the programme Edu-V in total eight working groups, consisting of representatives from suppliers of digital teaching and learning resources as well as education stakeholders (e.g., schools), collaborated on topics such as the framework for the agreement system, combining and arranging digital learning materials, evaluation of learning progress, examinations, privacy, and the secure exchange of personal data. In total, 200 different parties participated in formulating agreements.

In addition, the programme Cybersecurity VET (*Programma Cyberveiligheid mbo*), was launched. At the end of the year, a covenant on cyber security measures is signed by the Council for upper secondary VET schools.

2024 Implementation

Developments under objective 1

By 2024, the implementation of the agreement system Edu-V began with the issuance of 'quality marks' to suppliers who adhered to the established quality and cybersecurity standards. These quality marks provide assurance to schools that their suppliers of digital tools comply with the information security and privacy requirements established in the agreement system regarding digital data sharing. In the years to follow the programme will focus on the continued implementation of the established agreement system and the development of an infrastructure for digital educational materials. This includes the systems, tools, and frameworks necessary to support the creation, distribution, management, and utilisation of digital learning resources in education. More than 50 suppliers applied for the quality marks.

Developments under objective 2

Additionally, from 2024 onwards, all VET providers, Applied Science Universities and

Research Universities are required to provide justification of their cybersecurity measures in their annual reports.

2025 Implementation

Developments under objective 1

From 2025 onwards, the privacy covenant is now part of Edu-V. The privacy covenant was previously established in 2022 to guarantee privacy and secure data processing in compliance with the GDPR, specifically in digital products or services used in primary education, secondary education and VET. After a transition period, Edu-V eventually replaces the privacy covenant.

In May of 2025, Edu-V became a foundation. It awarded the first quality marks in October of 2025. By October 2025, eight VET suppliers had received a quality mark, and ten VET suppliers were undergoing evaluation.

In a policy letter of 24 April 2025, the Minister for Education reports that generally, digital resilience against cyber threats has been improved, as:

- (a) many VET schools now have a suitable Security Operations Center (SOC)-solution, a service or platform that helps them continuously monitor their digital environment for security incidents. The goal is to detect, analyse, and respond to cyber threats at an early stage.
- (b) knowledge on cybersecurity is being shared with education providers through the Security Expertise Centre (SEC) of the collaborative organisation for IT in Dutch education and research (SURF)
- (c) SURFcert, the Computer Emergency Response Team (CERT) of SURF provides a mechanism for institutions within the Netherlands (that are connected to SURF) to deal with computer security problems and their prevention.

In the same policy letter, the Minister also reports that the ministry meets twice a year with the Universities of the Netherlands (UNL), the Netherlands Association of Applied Sciences (VH), the Council for Upper Secondary VET Schools (MBO Raad), and SURF, to present the annual sector report on measures taken regarding digital security and discuss progress on the agreed measures.

With regards to the private education providers (who do not receive funding from the government), the Minister reports that the Dutch Council of Training (the sectoral association of private VET educators) (NRTO) invests in strengthening digital resilience of their members by raising awareness, providing training to its members, and incorporating cybersecurity processes as a requirement of the NRTO quality mark, which is necessary for membership of NRTO.

The main issue in the policy letter of 24 April 2025 is the announcement that the ministry intends to include higher education providers in the Cybersecurity Law (Cbw), which is the Dutch implementation of the European Network and Information Security directive (NIS 2 Directive), after a cyber-attack on a Research University. Because the government sees less risk in the area of knowledge security for VET colleges (such as espionage or data theft from strategic research), the government sees no grounds to include VET providers in this law.

Developments under objective 2

The Cybersecurity VET programme (*Programma Cyberveiligheid mbo*) is ongoing. Between now and 2027 institutions will implement joint initiatives. Examples include incorporating cyber ethics into curricula and working with a 'CISO as a Service' model that serves as an example for other sectors.

Bodies responsible

- Ministry of Education, Culture and Science

- Cooperation organisation of VET colleges on ICT (MBO digitaal)
- Foundation for Education and ICT (Stichting Kennisnet)
- Council for Primary Education (PO-Raad)
- Council for Secondary Education (VO-raad)
- Council for upper secondary VET schools (MBO Raad)
- Trade association Media Education Trade and Science (Branchevereniging Media Educatie Vak en Wetenschap)
- Trade association Digital Education Service Providers (Branchevereniging Vereniging Digitale Onderwijs Dienstverleners)
- Association of Educational Distributors Netherlands (Vereniging Educatieve Distributeurs Nederland)
- Universities of the Netherlands (UNL)
- Association of Universities of Applied Sciences (Vereniging Hogescholen)

Target group

Entities providing VET

Companies
 Small and medium-sized enterprises (SMEs)
 VET providers (all kinds)

Thematic categories

Governance of VET and lifelong learning

Engaging VET stakeholders and strengthening partnerships in VET

Modernising VET infrastructure

Improving digital infrastructure of VET provision

European priorities in VET

VET Recommendation

VET as a driver for innovation and growth preparing for digital and green transitions and occupations in high demand

Osnabrück Declaration

Resilience and excellence through quality, inclusive and flexible VET

Subsystem

IVET

Further reading

[Edu-V programme website](#)

[News item on Edu-V working groups](#)

[Launch programme Cybersecurity in VET](#)

[News item on approval agreement system](#)

[Governance study on cybersecurity](#)

[Agreement on cyber risk pooling](#)

[Agreement system Edu-V](#)

[Privacy covenant is now part of Edu-V, what does this mean for schools? News item Edu-V, 23 January 2025](#)

[The establishment of a foundation marks a new phase for Edu-V, News item Edu-V, 15 May 2025](#)

[Important milestone: the first digital teaching and learning resources receive the Edu-V quality mark, EduV, 7 October 2025](#)

[Policy letter on the progress in cyber resilience in VET and higher education, Education Ministry, 24 April 2025](#)

[Quality mark register, Edu-V \(accessed 15 October 2025\)](#)

[SURFcert website](#)

Related policy developments

2025 Implementation

Npuls: programme to improve VET and HE by using the opportunities of digitalisation

This development consists of an eight-year programme in which all 113 education institutions in upper secondary vocational education (MBO, HBO and WO) and higher education (post-secondary and higher education) cooperate. They are joining forces to enable system transformation in education.

 NETHERLANDS

Type of development

Practical
measure/Initiative

Subsystem

IVET CVET

“ ... ” Cite as

Cedefop, & ReferNet. (2026). Cooperating on cybersecurity: Netherlands. In Cedefop, & ReferNet. (2026). *Timeline of VET policies in Europe* (2025 update) [Online tool].

<https://www.cedefop.europa.eu/en/tools/timeline-vet-policies-europe/search/46831>

