Aanvraag
nieuwe opleiding
Associate degree

Cyber Safety & Security
SAMENVATTING

Macrodoelmatigheidstoets
volgens de Regeling macrodoelmatigheid hoger onderwijs
beleidsregel 2018

Oktober 2021

Basisgegevens

Naam instelling(en)	NHL Stenden
Contactgegevens	NHL Stenden Postbus 1080 8900 CB Leeuwarden
Naam opleiding	Cyber Safety & Security
Internationale naam opleiding	Cyber Safety & Security
Taal	Nederlands
In geval dat de opleiding in een andere taal dan het Nederlands wordt verzorgd: een toelichting op de aansluiting van de taalkeuze op de arbeidsmarktbehoefte	n.v.t.
In geval van een Associate degree-opleiding, indien van toepassing: welke bve-instelling verzorgt mede de opleiding	n.v.t.
In geval van een joint degree-opleiding: welke instelling(en) verzorg(t)(en) mede de opleiding	n.v.t.
Niveau	Associate degree (Ad)
Inhoud (korte beschrijving opleiding)	**Cyber Safety & Security** De snelle ontwikkelingen rond ICT en internettoepassingen roepen steeds meer en nieuwe veiligheidsvragen op in alle maatschappelijke domeinen. Cybercrime en bijvoorbeeld financiële criminaliteit nemen toe. Bewustwording en kennis van de risico's zijn daarom steeds belangrijker, voor particulieren maar zeker ook voor organisaties. Van oudsher ligt er veel nadruk op het beschermen van digitale systemen (cyber security), maar steeds meer wordt duidelijk dat het door de mens veilig gebruiken van internet om persoonlijke aanvallen of criminele activiteiten te voorkomen (cyber safety) minstens zo belangrijk is. Cyber security in combinatie met cyber safety wordt steeds meer een integraal onderdeel van de bedrijfsvoering in organisaties, zowel in de private als in de (semi)publieke sector. **De Ad-er Cyber Safety & Security (Ad-er CSS)** NHL Stenden Hogeschool speelt in op deze ontwikkelingen en beoogt een Associate degree (NLQF niveau 5) aan te bieden voor het opleiden

	van deskundigen voor functies op het gebied van Cyber Safety & Security in organisaties in alle sectoren. De Ad-er CSS kan in een organisatie informatiesystemen beschermen tegen verstoring of uitval, veroorzaakt door menselijk handelen of systeemfouten. Dit doet hij[1] door securityprocessen en -procedures in te richten volgens compliance wet- en regelgeving en waar nodig bij te dragen aan de ontwikkeling en implementatie daarvan. Om als Ad-er CSS te kunnen werken, wordt deze bij NHL Stenden Hogeschool multidisciplinair opgeleid. De Ad-er integreert en verbindt kennis en vaardigheden uit de ICT (technische invalshoek) en integrale veiligheid (sociale en psychologische invalshoek) en vertaalt deze naar praktische toepassingen op de werkvloer.
Inrichting van de opleiding (indicatie curriculum per jaar, vakken, leerlijnen)	De Ad Cyber Safety & Security is een tweejarige opleiding met een totale studielast van 120 EC die in voltijd en in deeltijd wordt aangeboden. De Ad-er CSS werkt in de opleiding aan de volgende competenties: 

[1] Overal waar hij of zijn staat, kan ook zij of haar gelezen worden.

De inrichting van het onderwijsprogramma volgt de richtlijnen voor Design Based Education zoals beschreven in het strategisch onderwijsbeleid van NHL Stenden.

De opleiding bestaat uit zes thematische modulen van 15 EC, die samenhangend en herkenbaar zijn voor studenten en werkveld. Actuele vraagstukken uit de praktijk vormen in iedere module de trigger en context voor leren. Er is daarbij aandacht voor het feit dat innovaties in dit vakgebied ontstaan op het snijvlak van disciplines. Naast de zes thematische modulen volgen de studenten gedurende de gehele opleiding de leerlijn Persoonlijke & professionele ontwikkeling (30 EC).

Het onderwijsprogramma ziet er als volgt uit:

	1. *Cyber Basics*: In deze eerste module leren de studenten de verschillende aspecten van en samenhang tussen cyber safety en cyber security kennen. Zij leren digitale problemen, dreigingen en/of risico's van een organisatie te analyseren en daarbij zowel de menselijke als de technische aspecten te beschouwen. 2. *Cyber Explore*: In deze module gaan de studenten aan de slag met het ontwerpen van een oplossingsrichting bij een digitaal probleem, dreiging of risico. Zij leren een advies met aanbevelingen op te stellen voor de organisatie waar het probleem zich voordoet. 3. *Technical Engineering*: In deze module verdiepen de studenten hun technische vaardigheden. Zij werken in een opdracht 'Netwerk & Security' aan een analyse van de IT-Architectuur, zij leren een audit van de huidige situatie uitvoeren en zij leren een Proof of Concept ontwerpen. 4. *Human Factors*: In deze module wordt ingezoomd op de menselijke factoren die ten grondslag (kunnen) liggen aan gesignaleerde digitale problemen, dreigingen of risico's. De studenten leren een probleem signaleren waar menselijke factoren aan ten grondslag liggen, leren een interventie ter verbetering te ontwerpen en een implementatieplan op te stellen. 5. *Ethical Hacking*: In deze module leren de studenten de beveiliging van een organisatie te bekijken door de ogen van een hacker. Ze leren computersystemen en -netwerken scannen, testen, hacken en beveiligen tegen hackers. Na het afronden van de module worden de studenten met een goed eindresultaat in de mogelijkheid gesteld om extern het examen voor de kwalificatie Certified Ethical Hacker te doen. Zij hebben de benodigde kennis en vaardigheden voor deze kwalificatie in de module geleerd. 6. *Cyber Challenge*: In de afsluitende module voeren de studenten hun afstudeeropdracht uit. Zij werken aan een praktijkopdracht op het gebied van cyber safety en cyber security met aandacht voor het doorlopen van de gehele cyclus van signaleren tot evalueren. *Leerlijn PPO*: In deze leerlijn werken de studenten onder andere aan hun schriftelijke en mondelinge vaardigheden, aan hun samenwerkings- en projectvaardigheden en aan het reflecteren op hun (professionele) handelen. Daarnaast is aandacht voor diverse aspecten die van belang zijn in de opleiding, zoals ethisch handelen.
Studielast	7. 120 EC
Vorm van de opleiding (voltijd, deeltijd, duaal)	Voltijd en deeltijd

Gemeente of gemeenten waar de opleiding wordt gevestigd	Emmen (nevenvestiging)
Doelgroep van de opleiding	Studenten en werkenden met (veelal) een MBO-4-diploma
Croho (sub)onderdeel en motivering	Techniek
Geplande startdatum opleiding	1 februari 2023
ISAT code van de opleiding (indien bekend)	n.v.t.
BRIN code van de instelling	31FR
Indien nadere vooropleidingseisen worden gesteld; voorstel daartoe	n.v.t.
Indien capaciteitsbeperking wordt ingesteld; de hoogte ervan	n.v.t.