

## Aanvraagformulier nieuwe opleiding

Naam instelling(en)	NHL Stenden Hogeschool
Contactgegevens	NHL Stenden Hogeschool Postbus 1080
Naam opleiding	8900 CB Leeuwarden Master Cybersafety
Internationale naam opleiding	Master Cybersafety
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	nvt
In geval van een associate degree-opleiding, indien van toepassing: welke bv-instelling verzorgt mede de opleiding	nvt
In geval van een joint degree-opleiding: welke instelling(en) verzorg(t)(en) mede de opleiding	nvt
Opleidingsniveau	Hbo master
Inhoud (korte beschrijving opleiding)	<p>Cybersafety is een cruciaal thema in onze steeds verder digitaliserende samenleving. Het is duidelijk te onderscheiden van cybersecurity: cybersafety heeft, in tegenstelling tot de techniek, de mens als primaire invalshoek en kent een sociaalwetenschappelijke focus.</p> <p>Veiligheid in het digitale domein is een "topprioriteit" voor het kabinet. Tegelijkertijd wordt vanuit het werkveld benadrukt dat informatiebeveiliging bij uitstek mensenwerk is. Digitale veiligheid vraagt om een continu leer- en veranderproces met bijzondere aandacht voor de menselijke</p>

	<p>factor. Het opleiden van deskundigen op het gebied van cybersafety is daarmee onmisbaar geworden.</p> <p>Met de Master Cybersafety wil NHL Stenden Hogeschool professionals opleiden die digitale veiligheid vanuit een multidisciplinair perspectief kunnen benaderen en in een regierol op het juiste moment verschillende expertises in de veiligheidsketen kunnen betrekken. De professional spreekt de taal van relevante disciplines en kan maatwerk leveren binnen een organisatie om zo de digitale veiligheid binnen de organisatie te borgen. De professional treedt buiten de gangbare paden en ontwikkelt vernieuwende, toekomstbestendige en creatieve ideeën die leiden tot vakoverstijgende oplossingsrichtingen.</p> <p>Uit diverse onderzoeken komt naar voren dat er landelijk een groot tekort is aan masterprofessionals op het gebied van cybersafety. De master Cybersafety biedt een oplossing voor dit probleem en vult een landelijke lacune op. Afgestudeerden gaan werken in de publieke sector (politie, gemeente, provincie) of in het private domein (adviesbureaus, zorginstellingen, de financiële sector).</p>
<p>Inrichting van de opleiding (indicatie curriculum per jaar, vakken, leerlijnen)</p>	<p>Het onderwijsprogramma bestaat uit drie pijlers. Deze pijlers sluiten inhoudelijk aan bij de drie pijlers van het onderzoeksprogramma van de onderzoeksgroep Cybersafety:</p> <ol style="list-style-type: none"> <li>1. Digitale weerbaarheid</li> <li>2. Politie, partners en digitalisering</li> <li>3. Bestuurlijke handhaving in cyberspace</li> </ol> <p><i>Digitale weerbaarheid</i> gaat over de bescherming van burgers en organisaties tegen cybergerelateerde criminaliteit en hoe te handelen als zich, ondanks die bescherming, toch digitale problemen voordoen. Thema's als social engineering, gedragsverandering en evaluatiemethoden komen bij deze pijler aan bod. De masterstudent bestudeert complexe vraagstukken vanuit de beroepspraktijk, met aandacht voor beroepsethisch handelen en het vinden van een balans tussen veiligheid en gebruikersgemak.</p> <p>Bij de pijler <i>Politie, partners en digitalisering</i> doet de masterstudent verdiepende kennis op over informatiegestuurd politiewerk, artificial intelligence, de opsporingswaarde van nieuwe technologieën als drones en bodycams, de beoordeling van digitaal bewijsmateriaal en publiek-private samenwerking. Met deze kennis kan de afgestudeerde master tijdig en adequaat anticiperen op</p>

	<p>nieuwe uitdagingen voor de politieorganisatie en haar medewerkers. De samenwerking tussen de Onderzoeksgroep Cybersafety en de Politieacademie geeft een impuls aan de betrokkenheid van de politie.</p> <p><i>Bestuurlijke handhaving in cyberspace</i> daagt studenten uit verder te kijken dan digitale veiligheid als zijnde politiewerk. Het gaat over onveiligheid in cyberspace, het monitoren in cyberspace en de innovatieve aanpak die nodig is wanneer het gaat om (lokale) dreigingen online. Daarbij komen ook ethische vragen aan bod. Hoe kunnen we ervoor zorgen dat iedereen zich vrijelijk binnen de gemeentegrenzen kan bewegen, zonder dat de uitings- en bewegingsruimte van diezelfde mensen te veel wordt belemmerd? De bestuurlijke handhaving wordt benaderd vanuit een regionaal, nationaal en internationaal perspectief.</p> <p>In het onderwijsprogramma staat een continue wisselwerking tussen onderwijs, onderzoek en praktijk centraal. In het eerste semester ligt de focus op inhoudelijke kennis over de drie pijlers en wordt deze kennis toegepast middels werkopdrachten die afkomstig zijn uit de beroepspraktijk. In het tweede semester wordt een afstudeeronderwerp gekozen dat gerelateerd is aan één of meerdere pijlers en verschuift de focus naar verdieping en het eindniveau van de kwalificaties.</p>
Studielast	60 EC
Vorm van de opleiding (voltijd, deeltijd, duaal)	Voltijd
Gemeente of gemeenten waar de opleiding wordt gevestigd	Leeuwarden
Doelgroep van de opleiding	<p>Studenten met een afgeronde bachelor in de domeinen:</p> <ul style="list-style-type: none"> <li>▪ Integrale Veiligheidskunde</li> <li>▪ Criminologie</li> <li>▪ Psychologie</li> <li>▪ Sociologie</li> <li>▪ ICT</li> <li>▪ Politiekunde</li> <li>▪ Sociaal werk</li> <li>▪ Pedagogiek</li> <li>▪ Bestuurskunde</li> </ul>
Croho (sub)onderdeel en motivering	Sectoroverstijgend: de master zit op het snijvlak van Economie en Gedrag en Maatschappij.

Geplande startdatum opleiding of nevenvestiging	1 september 2020
ISAT code van de opleiding (indien bekend)	nvt
BRIN code van de instelling	31FR
Indien nadere vooropleidingseisen worden gesteld; voorstel daartoe	nvt
Indien capaciteitsbeperking wordt ingesteld; de hoogte ervan	nvt