# Opdrachtomschrijving

Het wordt steeds belangrijker om goed te weten hoe het op het gebied van informatiebeveiliging en privacy binnen de onderwijsinstellingen ervoor staat, hoe de hele sector het doet, en hoe de onderwijsinstellingen het ten opzichte van het sectorgemiddelde doen. In dit kader is eind 2021 door het Ministerie van OCW en de onderwijskoepels Universiteiten van Nederland en de Vereniging Hogescholen afgesproken dat een (twee)jaarlijkse externe Security Audit uitgevoerd dient te worden om te toetsen of de informatiebeveiliging en privacybescherming van de onderwijsinstellingen op het gewenste niveau ligt. Voor het WO geldt dat deze audit jaarlijks plaats zal vinden, voor HBO geldt dat deze tweejaarlijks uitgevoerd zal worden.

Om deze audits uniform uit te voeren, wordt gebruik gemaakt van het SURFaudit Toetsingskader Informatiebeveiliging, wat gebaseerd is op het NBA Volwassenheidsmodel Informatiebeveiliging. Om de vergelijkbaarheid van de resultaten te borgen, hebben de CISO’s in samenwerking met de IT-Auditors van de universiteiten en van de HBO-instellingen een methodiek opgesteld waarin is beschreven hoe de audit moet worden uitgevoerd (scope, diepgang, toetsingskader). Een uniforme toepassing van deze methodiek draagt daarmee bij aan de vergelijkbaarheid van de resultaten en draagt zodoende bij aan een zo compleet en correct mogelijk beeld in de rapportage richting OCW.

Alhoewel voor deze opdracht de term ‘audit’ wordt gehanteerd, is deze dienstverlening adviserend van aard en betreft het geen controle, beoordeling of andersoortige assurance-opdracht overeenkomstig controle- en assurancestandaarden zoals uitgevaardigd door de Nederlandse Beroepsorganisatie van Accountants (NBA), de International Auditing and Assurance Standards Board, de NOREA en vergelijkbare organisaties. Deze -audits verstrekken derhalve geen enkele vorm van assurance als onderdeel van dit onderzoek. Tevens is ondertekening van de rapporten en benchmark door een geregistreerd EDP-auditor (RE) geen vereiste. Om de kwaliteit van de onderzoeken te waarborgen dienen de externe audits te worden uitgevoerd te worden door of onder leiding van professionals met voldoende aantoonbare ervaring met het uitvoeren van audits en onderzoeken op het gebied van informatiebeveiliging. Daarbij is het wel een vereiste dat het ingezette personeel geregistreerd is als, of onder de verantwoordelijkheid werkt van, een auditor ingeschreven in RE-auditor van de NOREA.

Doel van deze SURF-audit is tweeledig:

* Op basis van het SURFaudit Toetsingskader Informatiebeveiliging inzicht geven in het volwassenheidsniveau van de onderwijsinstelling. Dit volwassenheidsniveau dient voor de onderzochte maatregelen ten minste voor een periode van 3 maanden te zijn aangetoond door de onderwijsinstelling. Met het inzicht in het volwassenheidsniveau per instelling kan door SURF een sectorbeeld worden gepresenteerd richting OCW.
* Middels het verkregen inzicht de onderwijsinstellingen en de sector in staat te stellen te leren en verder te ontwikkelen, om zodoende het niveau van informatiebeveiliging sectorbreed te verhogen. Daarmee zijn deze onderzoeken en resultaten van de onderzoeken expliciet bedoeld om de onderwijsinstellingen en de sector te helpen te groeien in volwassenheid.

# Voorbeeldteksten t.a.v. verspreiding adviesrapport en beperking aard dienstverlening

## Verspreidingskring

Deze schriftelijke rapportage is alleen bestemd voor het management en College van Bestuur van opdrachtgever. Opdrachtgever is gerechtigd onderdelen of samenvattingen van dit rapport aan derden ter beschikking te stellen. Indien Opdrachtgever onderdelen of samenvattingen van dit rapport aan derden ter beschikking wil stellen, dient hij hen erop te wijzen dat dit geen assurance opdracht betreft en de opdracht niet is uitgevoerd conform audit standaarden zoals uitgevaardigd door de Nederlandse Beroepsorganisatie van Accountants (NBA), de International Auditing and Assurance Standards Board, de NOREA en vergelijkbare organisaties. Tevens dient hij hen erop te wijzen dat zonder onze uitdrukkelijke voorafgaande schriftelijke toestemming geen rechten aan dit rapport kunnen worden ontleend.

## Beperkingen aard van dienstverlening

Opdrachtnemer zal geen fouten en/of gebreken ten aanzien van de computersystemen, overige apparatuur dan wel onderdelen daarvan (hierna te noemen: Systemen) signaleren, aan de orde stellen, herstellen of oplossen, ongeacht of deze te wijten zijn aan onnauwkeurige of onduidelijke invoer, opslag, interpretatie of verwerking of rapportage van informatie. Opdrachtnemer is niet verantwoordelijk voor gebreken of problemen die voortvloeien uit of verband houden met gegevensverwerking in bepaalde Systemen.

# Audit dossier opbouw en diepgang

Verschillende auditpartijen hanteren verschillende (interne) kwaliteitseisen met betrekking tot documentatie, vastlegging, diepgang en opbouw van dossiers. In het kader van de audits is het van belang dat de resultaten, bevindingen en scores traceerbaar zijn naar het bewijs in het dossier. Deze traceerbaarheid is essentieel voor de transparantie en betrouwbaarheid van het auditproces.

Bij het opstellen van dossiers dient men ervoor te zorgen dat detailuitkomsten nauwkeurig zijn vastgelegd, bij voorkeur in een gestructureerd format zoals Excel. Verder is het belangrijk dat de in deze documenten opgenomen scores en bevindingen goed onderbouwd zijn met bewijsmateriaal.

De specifieke invulling van dossieropbouw kan variëren per opdrachtnemer, maar het overkoepelende doel altijd hetzelfde blijft: een nauwkeurig, betrouwbaar en verantwoordend onderzoek uitvoeren. Opdrachtnemers dienen daarom de basisprincipes van gedegen dossieropbouw te volgen - met name de traceerbaarheid van resultaten, bevindingen en scores naar het bewijs in het dossier - om de kwaliteit en integriteit van het onderzoek te waarborgen.