

Kwalificatiedossier mbo

Informatiebeveiliging

Crebonr. 23423

Kwalificaties

» **Informatiebeveiliging (Crebonr. 27049)**

Geldig vanaf

01-08-2025

Opleidingsdomein

Veiligheid en sport (Crebonr. 79100)

Penvoerder: Sectorkamer zakelijke dienstverlening en veiligheid
Gevalideerd door: Sectorkamer Zakelijke dienstverlening en veiligheid (ZDV)
Op: 05-09-2024

Inhoudsopgave

Leeswijzer	4
Overzicht van het kwalificatiedossier	5
Basisdeel	6
1. Beroepsspecifieke onderdelen	6
B1-K1: Onderzoekt digitale dreigingen	6
B1-K1-W1: Signaleert dreigingen in data en informatie	8
B1-K1-W2: Analyseert en maakt dreigingsinschatting	8
B1-K1-W3: Adviseert over en rapporteert bij digitale dreiging	9
B1-K2: Coördineert de uitvoering van informatiebeveiligingsmaatregelen	10
B1-K2-W1: Voert informatiebeveiligingsmaatregelen door	11
B1-K2-W2: Ondersteunt gebruikers bij informatiebeveiligingsmaatregelen	11
B1-K2-W3: Evalueert de uitvoering van informatiebeveiligingsmaatregelen	12
2. Generieke onderdelen	13
Profieldeel	14
P1: Informatiebeveiliging	14

Leeswijzer

Het kwalificatiedossier voor het middelbaar beroepsonderwijs geeft weer wat de beginnend beroepsbeoefenaar moet kennen en kunnen aan het einde van de mbo-opleiding.

Opbouw dossier

Dit kwalificatiedossier bevat de kwalificatie-eisen voor één of meerdere mbo-beroepen en bestaat uit:

1. Het **basisdeel** (B), dat gevormd wordt door:
 - a. De beroepsspecifieke onderdelen. Dit betreft gemeenschappelijke kerntaken en werkprocessen voor het gehele kwalificatie - dossier.
 - b. De generieke onderdelen. De generieke onderdelen zijn door de landelijke overheid geformuleerd. Het betreft de onderdelen:
Nederlandse taal;
rekenen;
loopbaan en burgerschap; en
voor zover het niveau 4 betreft: Engels.
2. Het **profieldeel** (P). Profielen bestaan uit kerntaken (K) en werkprocessen (W) waarop de kwalificaties in dit kwalificatiedossier van elkaar verschillen.

De beroepsopleiding in het mbo is gebaseerd op een kwalificatie en één of meer **keuzedelen** (D). Keuzedelen hebben tot doel om bovenop de kwalificatie een verdieping of verbreding te leveren bij de toerusting voor de arbeidsmarkt of een extra voorbereiding voor een vervolgopleiding. De beschikbare keuzedelen voor dit kwalificatiedossier zijn te vinden op <https://kwalificatie-mijn.s-bb.nl>. Op deze website staat het overzicht met alle keuzedelen.



Taal en rekenen

De generieke kwalificatie-eisen voor taal en rekenen zijn benoemd in het basisdeel. Als sprake is van beroepsspecifieke taal- en rekeneisen is dit aangegeven in de kolom 'vakken en vaardigheden'. Daarnaast kan in de kolom 'gedrag' een extra verduidelijking aangegeven zijn hoe deze beroepsspecifieke taal- en rekeneisen worden ingezet in een werkproces.

Verantwoordingsinformatie

Aanvullende (verantwoordings-)informatie bij dit kwalificatiedossier is te vinden op <https://kwalificatie-mijn.s-bb.nl>. Deze informatie is geen onderdeel van het kwalificatiedossier.

Overzicht van het kwalificatiedossier

Naam profiel	Mbo-niveau (EQF-niveau)	Beroepsvereisten	Typering van de kwalificatie
P1 Informatiebeveiliging	4	Nee	specialistenopleiding

Basisdeel

De gemeenschappelijke kerntaken en werkprocessen voor het gehele kwalificatiedossier zijn de volgende:

B1-K1 Onderzoekt digitale dreigingen	B1-K1-W1	Signaleert dreigingen in data en informatie
	B1-K1-W2	Analyseert en maakt dreigingsinschatting
	B1-K1-W3	Adviseert over en rapporteert bij digitale dreiging
B1-K2 Coördineert de uitvoering van informatiebeveiligingsmaatregelen	B1-K2-W1	Voert informatiebeveiligingsmaatregelen door
	B1-K2-W2	Ondersteunt gebruikers bij informatiebeveiligingsmaatregelen
	B1-K2-W3	Evalueert de uitvoering van informatiebeveiligingsmaatregelen

Profieldeel

De profielen in dit kwalificatiedossier hebben de volgende (specifieke) kerntaken en werkprocessen:

P1 Informatiebeveiliging
Geen extra kerntaken en werkprocessen

Basisdeel

1. Beroepsspecifieke onderdelen

Typering van de beroepengroep

Context

De Informatiebeveiligers werken, als medewerker of als zelfstandig ondernemer, bij publieke en private organisaties. Deze organisaties kunnen klein, midden en groot zijn, en ook regionaal, landelijk als internationaal actief zijn. De Informatiebeveiligers opereren op het snijvlak van fysieke veiligheid en digitalisering en heeft een uitvoerende rol in het bewaken van de beschikbaarheid, vertrouwelijkheid en integriteit van (digitale) informatie van de organisatie.

Door de opkomst van technologie en het verzamelen van een groeiende hoeveelheid, vaak gevoelige, data en informatie, wordt de veiligheid van personen, groepen en organisaties steeds meer bedreigd. Tegelijkertijd nemen dreigingen als Social engineering toe, een strategie om de vertrouwelijkheid, en daarmee de integriteit en beschikbaarheid van data en informatie te ondermijnen. Dit kan ernstige gevolgen hebben voor zowel de betrokken personen als de algehele veiligheid van de organisatie. De Informatiebeveiligers leveren bijdragen aan het uitvoeren van het informatiebeveiligingsbeleid. Hiervoor beschikt die onder andere over kennis van informatietechnologie en bijbehorende risico's, waardoor die effectief op dreigingen kan reageren en passende maatregelen, technologieën en processen kan inzetten. Daarnaast bevordert de Informatiebeveiligers bewustwording van risico's en ondersteunt de organisatie bij het proberen te voorkomen van dreigingen. Afhankelijk van de organisatie heeft de Informatiebeveiligers contact met bijvoorbeeld Junior Information Security Officers, Chief Information Security Officers, Privacy Officers, Cybersecurity analisten, ICT-medewerkers en andere beveiligers.

Typende beroepshouding

De Informatiebeveiligers kenmerkt zich door een sterk verantwoordelijkheidsgevoel, integriteit en nauwkeurigheid. Met een proactieve houding en scherp analytisch vermogen beschermt die tegen veelal digitale dreigingen. Samenwerkingsgericht en communicatief vaardig werkt de Informatiebeveiligers vanuit het informatiebeveiligingsbeleid, om risico's te minimaliseren en de veiligheid van de organisatie te waarborgen. Discretie en technische bekwaamheid zijn essentieel, evenals het vermogen om problemen snel en effectief op te lossen.

Resultaat van de beroepengroep

Het uitdragen en ondersteunen van de maatregelen van het informatiebeveiligingsbeleid in de organisatie en bedrijfsvoering heeft plaatsgevonden. Eventuele risico's en dreigingen in data en informatie en/of gegevens van personen, groepen en organisatie zijn vroegtijdig gesignaleerd, ingeschat en in goede banen naar een oplossing geleid. Bij dreiging zijn passende maatregelen en hulpmiddelen ingezet voor continuïteit van de organisatie en de bedrijfsvoering.

B1-K1: Onderzoekt digitale dreigingen

Complexiteit

De complexiteit van het onderzoeken van digitale dreigingen wordt met name bepaald door het voortdurend veranderen en het steeds geavanceerder worden van cyberaanvallen. De aard van de werkzaamheden omvat vooral gestandaardiseerde operationele taken die gericht zijn op het onderzoeken van data en informatie. Dit vereist een combinatie van (specialistische) kennis en vaardigheden. De snelheid en de mogelijke omvang van digitale aanvallen, de complexiteit van IT-omgevingen in combinatie met het blijvend volgen van gestandaardiseerde en beleidsmatige processen en protocollen maken het werk complex. Daarnaast is de menselijke factor een van de zwakste schakels in informatiebeveiliging, waardoor de complexiteit van de werkzaamheden verder toeneemt. Fouten en vergissingen kunnen tot ernstige gevolgen voor de gebruikers en organisatie leiden en een hoog afbreukrisico met zich meebrengen, zoals bijvoorbeeld eventuele financiële schade.

Verantwoordelijkheid en zelfstandigheid

De Informatiebeveiligers is, vanuit een initiërende en een uitvoerende rol, verantwoordelijk voor het onderzoeken van data en informatie en het uitvoeren van toegewezen operationele takenverantwoordelijkheid. De werkzaamheden worden meestal zelfstandig, en deels in teamverband, uitgevoerd met bijbehorende verantwoordelijkheid voor de eigen activiteiten. De Informatiebeveiligers draagt gedeelde verantwoordelijkheid voor

B1-K1: Onderzoekt digitale dreigingen

het leveren van goede en doelbewuste onderzoeksresultaten. De opdrachtgever* draagt de eindverantwoordelijkheid.

* Waar opdrachtgever staat is ook leidinggevende te lezen.

Vakkennis en vaardigheden

De beginnend beroepsbeoefenaar:

Communicatie

- heeft specialistische kennis van veelgebruikte vaktaal en vaktermen binnen het vakgebied
- heeft brede kennis van mondelinge en schriftelijke communicatieprocessen
- kan ICT-technische informatie en/of instructies in het Nederlands lezen en interpreteren
- kan in het Nederlands vakgerelateerde gesprekken voeren
- kan ICT-technische informatie en/of instructies in het Engels lezen en interpreteren
- kan in het Engels vakgerelateerde gesprekken voeren
- kan met interne en externe betrokkenen communiceren
- kan feedback geven en ontvangen
- kan luisteren, doorvragen en samenvatten

ICT

- heeft kennis van de werking van netwerken in de context van het internet
- heeft kennis van de opbouw en werking van een ICT systeem (databases, software, hardware, front- en back-end)
- kan werken met gangbare informatie -en communicatiesystemen, software, devices en applicaties

Informatiebeveiliging

- heeft kennis van de invloed van gebruikersgedrag op de veiligheid van digitale systemen en netwerken
- heeft specialistische kennis van veel voorkomende voorbeelden van cybercrime
- heeft specialistische kennis van veelgebruikte vaktaal en vaktermen binnen het vakgebied
- heeft specialistische kennis van (preventieve) netwerk- en informatiebeveiliging
- heeft specialistische kennis van datagedreven informatie
- kan kwetsbaarheden in digitale systemen en applicaties herkennen en identificeren
- kan bij escalatie een responsactie uitzetten
- kan dreigingen voor de informatiebeveiliging identificeren en categoriseren
- kan data uit beveiligingssystemen analyseren

Interne werkprocessen

- heeft kennis van het informatiebeveiligingsbeleid van de organisatie
- heeft kennis van beveiligingssystemen en -applicaties
- kan bepalen op welk moment te escaleren
- kan verbetervoorstellen opstellen en beredeneren
- kan rapportages opstellen

Professionele ontwikkeling

- kan prioriteiten stellen in eigen werkzaamheden
- kan de eigen werkzaamheden evalueren en verbeteringen voorstellen
- kan omgaan met weerstand en conflicten
- kan kennis van culturele achtergronden en culturele verschillen toepassen

Wet- en regelgeving

- heeft kennis van relevante wettelijke bepalingen en gedragscodes met betrekking tot (digitale) veiligheid en beveiliging
- heeft kennis van regelgeving vanuit de bedrijfstak/branche
- heeft specialistische kennis van het beschermen van persoonsgegevens
- heeft specialistische kennis van het beschermen van bedrijfsgegevens

B1-K1-W1: Signaleert dreigingen in data en informatie

Omschrijving

De Informatiebeveiliging monitor de uitvoering van het informatiebeveiligingsbeleid continue. Daarbij let die op signalen die een dreiging kunnen vormen voor de organisatie. Dit kunnen bijvoorbeeld interne of externe dreigingen zijn waarbij de beschikbaarheid, vertrouwelijkheid en integriteit van data en informatie mogelijk in gevaar komen, zoals Malware, Phishing of Ransomware. De Informatiebeveiliging verzamelt data en informatie over de dreigingen. De signalen en alle verzamelde gegevens over onder andere de tijd, locatie en omgeving van de dreiging legt die vast. De Informatiebeveiliging maakt direct een melding en informeert betrokkenen, zoals een ICT-medewerker en/of de opdrachtgever.

Resultaat

Dreiging is gesignaleerd en alle data en informatie is vastgelegd volgens de bedrijfsprocessen.

Gedrag

Informatiebeveiliging:

- signaleert en interpreteert een mogelijke dreiging vlot;
- verzamelt data en informatie over dreiging correct en volledig;
- legt signalen en eventuele aanvullende informatie juist en volledig vast;
- schakelt betrokkenen tijdig in;
- geeft duidelijke en volledige uitleg over de signalen;
- toont onder druk en spanning objectiviteit en doorzettingsvermogen;
- houdt zich nauwgezet aan procedures, protocollen, kaders en normen van de organisatie;
- volgt consistent vakinhoudelijke trends en ontwikkelingen;
- volgt nauwgezet wijzigingen in wet- en regelgeving.

De onderliggende competenties zijn: Formuleren en rapporteren, Instructies en procedures opvolgen, Vakdeskundigheid toepassen, Met druk en tegenslag omgaan, Samenwerken en overleggen

B1-K1-W2: Analyseert en maakt dreigingsinschatting

Omschrijving

De Informatiebeveiliging analyseert de gesignaleerde en vastgelegde data en informatie over de dreiging. Hierbij zoekt die onder andere uit of de dreiging nieuw is, waar de dreiging vandaan komt, hoe de dreiging in aanraking met de organisatie en/of gebruiker is gekomen en informatie over soortgelijke situaties. Daarbij past die de kaders en normen van de organisatie toe en overlegt waar nodig met een ICT-medewerker of de opdrachtgever. De Informatiebeveiliging vertaalt de analyse en de mogelijke impact ervan op de organisatie in een dreigingsinschatting en informeert betrokkenen, zoals een ICT-medewerker, en/of de opdrachtgever. Hierbij reageert die op vragen en opmerkingen van de betrokkenen en verwerkt deze in de dreigingsinschatting.

Resultaat

Een concrete inschatting van de mogelijke dreiging is gemaakt en over de analyseresultaten zijn betrokkenen geïnformeerd.

Gedrag

Informatiebeveiliging:

- toetst informatie kritisch op onder andere juistheid, betrouwbaarheid en volledigheid;
- schat de impact van een mogelijke dreiging voor de organisatie reëel in;
- houdt zich nauwgezet aan procedures, protocollen, kaders en normen van de organisatie;
- zet hulpmiddelen effectief en op een voorgeschreven wijze in;
- brengt dreigingen en risico's helder en juist in kaart;
- trekt logische conclusies op basis van verzamelde data en informatie;
- overlegt met betrokkenen tijdig en volledig;
- gaat integer met bedrijfsgegevens en persoonsgegevens om.

De onderliggende competenties zijn: Samenwerken en overleggen, Vakdeskundigheid toepassen, Materialen en middelen inzetten, Instructies en procedures opvolgen, Onderzoeken

B1-K1-W3: Adviseert over en rapporteert bij digitale dreiging

Omschrijving

De Informatiebeveiliging verwerkt de gesignaleerde dreigingen, geanalyseerde dreigingsinschattingen en de reacties uit het overleg met betrokkenen, in een rapportage uit tot adviezen over de te nemen of aan te passen maatregelen. Aanvullend werkt die voorstellen uit in de rapportage voor het proberen te voorkomen van dreigingen in data en informatie op operationele processen op de werkvloer. De Informatiebeveiliging volgt daarbij de richtlijnen van de organisatie. De eindversie van de rapportage overlegt die met betrokken zoals de ICT-medewerker en/of de opdrachtgever en verwerkt de eventueel gegeven feedback

Resultaat

Er is geadviseerd over en er zijn voorstellen gedaan om te reageren op digitale dreigingen of de dreiging proberen te voorkomen. De resultaten zijn gerapporteerd en besproken met betrokkenen.

Gedrag

Informatiebeveiliging:

- stelt zorgvuldig een complete en correcte rapportage op over de dreigingsinschatting;
- adviseert objectief, kritisch en vanuit meer invalshoeken;
- onderbouwt adviezen en voorstellen op een overtuigende wijze;
- deelt actief kennis en expertise over het vakgebied;
- vertaalt adviezen naar haalbare en uitvoerbare (verbeter)voorstellen;
- schat effecten/resultaten van adviezen reëel in;
- informeert betrokkenen tijdig en op een vakkundige wijze;
- staat open voor en gebruikt feedback constructief.

De onderliggende competenties zijn: Samenwerken en overleggen, Formuleren en rapporteren, Vakdeskundigheid toepassen, Op de behoeften en verwachtingen van de "klant" richten, Instructies en procedures opvolgen

Complexiteit

Bij het coördineren van de uitvoering van informatiebeveiligingsmaatregelen op de werkvloer wordt de complexiteit met name bepaald door de verscheidenheid aan dreigingen, de complexiteit van IT-omgevingen en de menselijke factor. De aard van de werkzaamheden omvat vooral operationele taken gericht op het naleven van de maatregelen van gestandaardiseerde en beleidsmatige processen en protocollen uit het informatiebeveiligingsbeleid van de organisatie. Dit vereist een combinatie van (brede/specialistische) kennis en vaardigheden. Mede van invloed op de complexiteit is het spanningsveld tussen doelgericht en respectvol kunnen omgaan met het gedrag van de gebruikers en het bewaken van de continuïteit van de maatregelen. Fouten en vergissingen bij gebruikers kunnen tot ernstige gevolgen voor de organisatie leiden wat een hoog afbreukrisico met zich mee brengt voor de beschikbaarheid, vertrouwelijkheid en integriteit van data en informatie.

Verantwoordelijkheid en zelfstandigheid

De Informatiebeveiliging is verantwoordelijk voor het naleven en continueren van het informatiebeveiligingsbeleid en werkt veelal zelfstandig en deels in teamverband. De Informatiebeveiliging heeft gedeelde verantwoordelijkheid in het coördineren van de maatregelen van het informatiebeveiligingsbeleid. De opdrachtgever* draagt de eindverantwoordelijkheid.

* Waar opdrachtgever staat is ook leidinggevende te lezen.

Vakkennis en vaardigheden

De beginnend beroepsbeoefenaar:

Communicatie

- heeft brede kennis van mondelinge en schriftelijke communicatieprocessen
- kan ICT-technische informatie en/of instructies in het Nederlands lezen en interpreteren
- kan in het Nederlands vakgerelateerde gesprekken voeren
- kan ICT-technische informatie en/of instructies in het Engels lezen en interpreteren
- kan in het Engels vakgerelateerde gesprekken voeren
- kan met interne en externe betrokkenen communiceren
- kan feedback geven en ontvangen
- kan luisteren, doorvragen en samenvatten

ICT

- heeft kennis van de werking van netwerken in de context van het internet
- heeft kennis van de opbouw en werking van een ICT systeem (databases, software, hardware, front- en back-end)
- heeft kennis van systeembeheer en besturingssystemen van toegangscontroles of beveiligingsinstellingen
- kan werken met gangbare informatie -en communicatiesystemen, software, devices en applicaties

Informatiebeveiliging

- heeft kennis van de invloed van gebruikersgedrag op de veiligheid van digitale systemen en netwerken
- heeft kennis van applicatiebeveiliging voor het vermijden van kwetsbaarheden en het implementeren van authenticatie en autorisatie
- heeft specialistische kennis van (preventieve) netwerk- en informatiebeveiliging
- kan kwetsbaarheden in digitale systemen en applicaties herkennen en identificeren
- kan bij escalatie een responsactie uitzetten
- kan dreigingen voor de informatiebeveiliging identificeren en categoriseren
- kan data uit beveiligingssystemen analyseren
- kan beveiligingshulpmiddelen inzetten om netwerken en systemen te monitoren op verdachte activiteiten
- kan assisteren bij het implementeren van beveiligingsmaatregelen voor het beheer van toegangscontroles

Interne werkprocessen

- heeft kennis van het informatiebeveiligingsbeleid van de organisatie
- heeft kennis van beveiligingssystemen en -applicaties
- kan een doelgroep monitoren en observeren
- kan rapportages opstellen
- kan routinematige veiligheidsscans uitvoeren

Professionele ontwikkeling

- heeft specialistische kennis van veelgebruikte vaktaal en vaktermen binnen het vakgebied

B1-K2: Coördineert de uitvoering van informatiebeveiligingsmaatregelen

- kan bepalen op welk moment te escaleren
- kan prioriteiten stellen in eigen werkzaamheden
- kan de eigen werkzaamheden evalueren en verbeteringen voorstellen
- kan omgaan met weerstand en conflicten
- kan kennis van culturele achtergronden en culturele verschillen toepassen
- kan coördinerend optreden bij beveiligingsincidenten met responsacties en/of forensisch onderzoek
- kan toezicht houden op het gedrag van gebruikers en deze corrigeren

Wet- en regelgeving

- heeft kennis van relevante wettelijke bepalingen en gedragscodes met betrekking tot (digitale) veiligheid en beveiliging
- heeft kennis van regelgeving vanuit de bedrijfstak/branche

B1-K2-W1: Voert informatiebeveiligingsmaatregelen door

Omschrijving

De Informatiebeveiliging voert technische en organisatorische maatregelen op operationele processen door. Hierbij waarborgt die de vertrouwelijkheid, integriteit en beschikbaarheid van informatie. Dit gaat bijvoorbeeld over het begeleiden van de implementatie van technische maatregelen op de werkvloer, zoals encryptie, toegangsbeheer en firewalls of het bijdragen aan een trainingsprogramma om bewustzijn bij de gebruikers te creëren over informatiebeveiliging. De Informatiebeveiliging begeleidt de implementatie en let hierbij op het kwalitatief, consistent en doeltreffend doorvoeren van het informatiebeveiligingsbeleid op de werkvloer. Aanvullend voert die in samenwerking met ICT-medewerkers en/of de opdrachtgever een of meer interventies uit ter controle of verbetering van de maatregelen.

Resultaat

De informatiebeveiligingsmaatregelen zijn consistent doorgevoerd, eventuele interventies hebben geleid tot het controleren of verbeteren van de maatregelen.

Gedrag

Informatiebeveiliging:

- toont vakkundig inzicht in de haalbaarheid van door te voeren maatregelen;
- werkt zorgvuldig conform de richtlijnen van de organisatie;
- informeert betrokkenen juist, volledig en op een duidelijke wijze;
- stemt het doorvoeren van maatregelen zorgvuldig af op het niveau van de gebruikers;
- reageert vlot en adequaat op het niet naleven van de maatregelen;
- legt met nadruk de focus op de bewustwording van gebruikers in het veilig werken volgens de maatregelen;
- schakelt tijdig een ICT-medewerker of andere betrokkenen in bij het (vermoeden) niet zelf te kunnen of mogen handelen.

De onderliggende competenties zijn: Ethisch en integer handelen, Vakdeskundigheid toepassen, Instructies en procedures opvolgen, Op de behoeften en verwachtingen van de "klant" richten, Samenwerken en overleggen, Overtuigen en beïnvloeden

B1-K2-W2: Ondersteunt gebruikers bij informatiebeveiligingsmaatregelen

Omschrijving

De Informatiebeveiliging ondersteunt gebruikers op de werkvloer in het veilig en bewust naleven van de informatiebeveiligingsmaatregelen. Hierbij treedt die op als aanspreekpunt en is beschikbaar voor vragen, uitleg, tips of klachten. Aanvullend volgt die wat online gedeeld wordt over de organisatie door de gebruikers, waarbij die reageert op het (onbewust) incorrect gebruiken van data en informatie of onveilig gedrag. De Informatiebeveiliging is veelal fysiek aanwezig op de werkvloer waarbij die signalen over (niet) veilig werken opvangt en de gebruiker indien nodig hulp en begeleiding biedt. Daarbij licht die het beoogde effect en/of eventuele risico's van het niet naleven van de maatregelen toe om de bewustwording te verhogen. Indien noodzakelijk neemt die het initiatief om training of begeleiding aan te bieden.

B1-K2-W2: Ondersteunt gebruikers bij informatiebeveiligingsmaatregelen

Resultaat

Gebruikers zijn ondersteund en geïnformeerd in het veilig en bewust naleven van de informatiebeveiligingsmaatregelen.

Gedrag

Informatiebeveiliging:

- toont actief voorbeeldgedrag;
- informeert gebruikers juist, volledig en op een duidelijke wijze;
- stemt de wijze van ondersteunen zorgvuldig en passend af op het niveau van de gebruikers;
- reageert vlot en adequaat op mogelijke dreigingen en het beperken van de risico's;
- schakelt tijdig een ICT-medewerker of andere betrokkenen in bij het (vermoeden) niet zelf te kunnen of mogen handelen;
- gaat actief en zorgvuldig na of de gebruikers de maatregelen goed gebruiken;
- volgt actief wat online gedeeld wordt over de organisatie door de gebruikers.

De onderliggende competenties zijn: Begeleiden, Samenwerken en overleggen, Ethisch en integer handelen, Overtuigen en beïnvloeden, Vakdeskundigheid toepassen, Op de behoeften en verwachtingen van de "klant" richten

B1-K2-W3: Evalueert de uitvoering van informatiebeveiligingsmaatregelen

Omschrijving

De Informatiebeveiliging evalueert de uitvoering van de informatiebeveiligingsmaatregelen met betrokkenen, zoals een ICT-medewerker en de opdrachtgever. Hierbij beoordeelt die de effectiviteit, consistentie en het doorvoeren van de maatregelen door deze te vergelijken met adviezen, verwachtingen en ingezette maatregelen. De Informatiebeveiliging heeft aandacht voor het doorlopen proces, de eventuele interventies, de kwaliteit van de uitvoering op de werkvloer en trekt conclusies over de impact ervan op de gebruikers. Aanvullend reflecteert die op het eigen handelen, trekt conclusies, noteert aandachtspunten en vertaalt feedback in adviezen en voorstellen ter verbetering van de maatregelen op operationele processen. De evaluatieresultaten legt die vast in een rapportage en verwerkt hierin aanvullend de te ondernemen activiteiten.

Resultaat

De evaluatie over de uitvoering van de informatiebeveiligingsmaatregelen met betrokkenen heeft plaatsgevonden. Er zijn adviezen gegeven ter verbetering van de maatregelen op operationele processen. De evaluatieresultaten en de te ondernemen activiteiten zijn vastgelegd in een rapportage.

Gedrag

Informatiebeveiliging:

- brengt de verzamelde gegevens met elkaar in verband en trekt logische conclusies;
- formuleert (voorlopige) conclusies en/of voorstellen helder en bondig;
- reflecteert kritisch op het eigen handelen;
- staat open voor en gebruikt feedback constructief;
- analyseert de verzamelde gegevens grondig;
- legt evaluatieresultaten en bevindingen nauwkeurig vast.

De onderliggende competenties zijn: Samenwerken en overleggen, Formuleren en rapporteren, Vakdeskundigheid toepassen, Onderzoeken, Kwaliteit leveren, Instructies en procedures opvolgen

2. Generieke onderdelen

Elke kwalificatie kent - naast (beroepsgerichte) specifieke kwalificatie-eisen - ook generieke kwalificatie-eisen.

Nederlandse taal

Het generieke examenonderdeel Nederlandse taal maakt deel uit van elke kwalificatie in dit kwalificatiedossier. De referentieniveaus en de kwalificatie-eisen voor dit generieke onderdeel zijn opgenomen in bijlage 1 bij het Besluit referentieniveau Nederlandse taal en rekenen. Deze bijlage is te vinden op <https://wetten.overheid.nl/BWBR0027879> en vormt integraal onderdeel van het kwalificatiedossier.

Rekenen

Het generieke examenonderdeel rekenen maakt deel uit van elke kwalificatie in dit kwalificatiedossier. De referentieniveaus en de kwalificatie-eisen voor dit generieke onderdeel zijn opgenomen in de bijlagen 2 en 3 bij het Besluit referentieniveaus Nederlandse taal en rekenen. Deze bijlage is te vinden op <https://wetten.overheid.nl/BWBR0027879> en vormt integraal onderdeel van het kwalificatiedossier.

Loopbaan en burgerschap

Het generieke examenonderdeel loopbaan en burgerschap maakt deel uit van elke kwalificatie in dit kwalificatiedossier. De kwalificatie-eisen voor dit generieke onderdeel zijn opgenomen in bijlage 1 bij het Examen- en kwalificatiebesluit beroepsopleidingen WEB. Deze bijlage is te vinden op <https://wetten.overheid.nl/BWBR0027963> en vormt integraal onderdeel van het kwalificatiedossier.

Engels (alleen voor niveau 4)

Het generieke examenonderdeel Engels maakt deel uit van elke kwalificatie op mbo-niveau 4 in dit kwalificatiedossier. De referentieniveaus en de kwalificatie-eisen voor dit generieke onderdeel zijn opgenomen in bijlage 2 bij het Examen- en kwalificatiebesluit beroepsopleidingen WEB. Deze bijlage is te vinden op <https://wetten.overheid.nl/BWBR0027963> en vormt integraal onderdeel van het kwalificatiedossier.

Profieldeel

P1 Informatiebeveiliging
Mbo-niveau
4
Typering van het beroep
N.v.t.
Beroepsvereisten
Nee