Definitief vastgesteld door het CvB op 31-1-2018.

Informatiebeveiliging en privacy beleid


Verantwoording

Versiebeheer

Nr.	Aanpassingen	Auteur	Datum
0.1	Eerste opzet	Ludo Cuijpers	24-4-2017
0.2	Aanpassingen en opmerkingen.	Hans Witteveen Bertha Lenstra	16-8-2017
0.3	Een aantal aanpassingen overgenomen. Governance nog bespreken om een en ander beter te verankeren.	Ludo Cuijpers	22-8-2017
0.9	Opmerkingen van Hans Witteveen en Bertha Lenstra verwerkt	Bertha Lenstra Ludo Cuijpers	13-9-2017
1.0	Opmerkingen van Hans Witteveen en Bertha Lenstra verwerkt	Hans Witteveen Bertha Lenstra	1-11-2017
1.1	Opmerkingen van Management verwerkt	Hans Witteveen	31-1-2018

Inhoudsopgave

1 Inleiding

1.1 Toelichting informatiebeveiliging beleid

Informatiebeveiliging is een beleidsverantwoordelijkheid van het College van Bestuur (CvB) van SVO Vakopleiding Food. Ook in het onderwijsveld is sprake van toenemende afhankelijkheid van informatie en computersystemen, waardoor nieuwe kwetsbaarheden en risico's kunnen optreden. Het is daarom van belang hiertegen adequate maatregelen te nemen. Immers, onvoldoende informatiebeveiliging kan leiden tot onacceptabele risico's bij de uitvoering van onderwijs en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

SVO Vakopleiding Food heeft de ambitie om informatiebeveiliging structureel naar een hoger niveau te brengen en daar op te houden door de aspecten governance, wet- en regelgeving, de organisatie van de beveiligingsfunctie en het informatiebeveiligingsbeleid - ook in hun onderlinge relatie - duidelijk in dit document te beschrijven en vast te stellen.

1.2 Toelichting privacy beleid

Het verwerken van persoonsgegevens is een beleidsverantwoordelijkheid van het College van Bestuur (CvB) van SVO Vakopleiding Food. Het privacy beleid heeft betrekking op het beheer en verwerken van Persoonsgegevens[1] van alle Betrokkenen bij SVO Vakopleiding Food waaronder in ieder geval alle medewerkers, studenten, ouders, gasten, bezoekers en externe relaties (inhuur/outsourcing), evenals op andere Betrokkenen waarvan SVO Vakopleiding Food Persoonsgegevens beheert of verwerkt.

In het Beleid ligt de nadruk op de, geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van Persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van SVO Vakopleiding Food alsmede op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Eveneens is het Beleid van toepassing op **niet**-geautomatiseerde verwerking van Persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Uitgangspunt is dat persoonlijke levenssfeer van de Betrokkene wordt gerespecteerd. De gegevens, die betrekking hebben op een Betrokkene dienen beschermd te worden tegen onwettelijk en ongeautoriseerd gebruik dan wel misbruik op basis van het fundamenteel recht op bescherming van zijn/haar Persoonsgegevens. Dit brengt met zich mee dat het beheer en verwerken van Persoonsgegevens voldoet aan relevante wet- en regelgeving en dat Persoonsgegevens veilig zijn bij SVO Vakopleiding Food.

1.3 Vervlechting informatiebeveiliging en privacy (IBP)

Bij SVO Vakopleiding Food wordt informatiebeveiliging (processen) gekoppeld aan Privacy (mensen). Het informatiebeveiliging en privacy beleid binnen SVO Vakopleiding Food heeft betrekking op alle medewerkers, studenten, ouders, gasten, geregistreerde bezoekers en externe relaties (inhuur / outsourcing), alsmede op alle organisatieonderdelen. Tevens vallen onder het informatiebeveiliging en privacy beleid alle devices (pc's, laptops, smartphones, tablets, etc.) van waaraf geautoriseerde toegang tot het instellingsnetwerk verkregen kan worden.

1.4 Doelstelling informatiebeveiliging en privacy beleid

Het informatiebeveiliging en privacy beleid bij SVO Vakopleiding Food heeft als doel het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering en het minimaliseren van de schade door het voorkomen van beveiligings- en privacy-incidenten en het minimaliseren van eventuele gevolgen.

Door het concretiseren van informatiebeveiliging en privacy beleid op procesniveau van SVO Vakopleiding Food wordt aantoonbaar dat dit beleid bijdraagt aan de realisering van de overall doelstellingen die SVO Vakopleiding Food voor zichzelf heeft geformuleerd. Die doelstellingen laten zich samenvatten in het bieden van een kwalitatief hoogwaardige onderwijsomgeving. Deze omgeving behoort veilig te zijn en te voldoen aan relevante wet- en regelgeving.

[1] De termen (persoonsgegevens, betrokkene, etc.) zijn overgenomen uit de AVG. Deze termen zijn met een hoofdletter aangegeven.

1.5 Beschermen van persoonsgegevens

Naast bovenstaande concrete doelstellingen is een meer algemeen doel het instellingsbreed creëren van bewustwording van het belang en de noodzaak van het beschermen van Persoonsgegevens, mede ter vermijding van risico's als gevolg van het niet voldoen aan de relevante wet- en regelgeving.

Opslag en Verwerking van Persoonsgegevens (Privacy) is noodzakelijk om te voldoen aan wettelijk voorgeschreven uitwisselingen van gegevens en voor de bedrijfsprocessen van instellingen van onderwijs. Dit dient met de grootste zorgvuldigheid te gebeuren omdat misbruik van Persoonsgegevens grote schade kan berokkenen aan studenten, ouders, medewerkers en andere Betrokkenen bij SVO Vakopleiding Food, maar ook bij SVO Vakopleiding Food zelf. SVO Vakopleiding Food beschermt de Persoonsgegevens die aan haar worden verstrekt en draagt zorg voor een zorgvuldig beheer en verwerking van de Persoonsgegevens.

Met het beschrijven van de maatregelen in dit beleidsdocument beoogt en neemt SVO Vakopleiding Food haar verantwoordelijkheid om de kwaliteit van de verwerking en de beveiliging van Persoonsgegevens te optimaliseren en daarmee te voldoen aan de relevante privacywet- en regelgeving. Het door SVO Vakopleiding Food gevoerde informatiebeveiligings- en privacy beleid wordt bekend gemaakt aan studenten, ouders en medewerkers.

1.6 Beleidsuitgangspunten informatiebeveiliging en privacy

Het belangrijkste beleidsuitgangspunt bij SVO Vakopleiding Food is:

- Onze filosofie is dat we een open, transparante en toegankelijke instelling zijn.

Dit open en toegankelijk karakter heeft betrekking op gasten, maar ook op studenten en medewerkers. Deze open benadering heeft echter met name voor interne gebruikers ook consequenties. Er wordt van medewerkers en studenten verwacht dat ze zich qua techniek en ook qua houding gedragen (eigen verantwoordelijkheid) zoals verwoord in de privacy regels en de afgesproken processen naleven.

- De informatiebeveiliging en het privacy beleid dienen te voldoen aan de relevante wet- en regelgeving, in het bijzonder aan de wet Algemene Verordening Gegevensbescherming (AVG).

Gestreefd wordt naar een optimale balans tussen het belang van SVO Vakopleiding Food om Persoonsgegevens te verwerken en het belang van Betrokkene om eigen keuzes te maken met betrekking tot zijn Persoonsgegevens.

1.7 Aanvullende uitgangspunten

Naast het bovenstaande beleidsuitgangspunt hanteert SVO Vakopleiding Food de volgende aanvullende uitgangspunten:

- De opvolging van informatiebeveiliging en privacy is een lijnverantwoordelijkheid: dat betekent dat de proceseigenaren (o.a. centrale diensten en onderwijsafdelingen) de primaire verantwoordelijkheid dragen voor een goede informatiebeveiliging en privacy ten aanzien van (proces gebonden) informatie die op hun afdeling / eenheid wordt gebruikt dan wel gegenereerd. Dit omvat ook de keuze van maatregelen en de uitvoering en handhaving ervan.
- Veilig en betrouwbaar omgaan met informatie in het dagelijkse werk is ieders professionele verantwoordelijkheid. Communiceer met medewerkers en derden wat er van hen verwacht wordt dat ze actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie. Dat gebeurt o.a. in de aanstellingsbrief, tijdens functioneringsgesprekken, met een instellingsbrede gedragscode en, met periodieke bewustwordingsactiviteiten. Het opleggen van sancties na (ernstige) overtredingen maakt daar onderdeel van uit.
- Bij het beheer van gegevens wordt gestreefd naar optimaal technisch-beheer, aansluitend op de visie en uitgangspunten.
- Eigendom van informatie: de onderwijsinstelling is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd.

1.8 Privacy principes

Om aan bovenstaande beleidsuitgangspunten te voldoen gelden de volgende privacy principes:

- Elke Verwerking van Persoonsgegevens is gebaseerd op de AVG.

- Persoonsgegevens worden alleen verwerkt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de Verwerking geformuleerd.
- Bij een Verwerking van Persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt tot de Persoonsgegevens die strikt noodzakelijk zijn voor het specifieke doeleinde. De gegevens dienen met het oog op dat doel toereikend, ter zake dienend en niet bovenmatig te zijn.
- Verwerking van Persoonsgegevens gebeurt op de minst ingrijpende wijze en dient in redelijke verhouding te staan tot het beoogde doeleinde.
- Er worden maatregelen getroffen om zoveel mogelijk te waarborgen dat de te verwerken Persoonsgegevens juist en actueel zijn.
- Persoonsgegevens worden adequaat beveiligd volgens de geldende beveiligingsnormen.
- Persoonsgegevens worden niet *verder* verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.
- Persoonsgegevens worden niet *langer* verwerkt dan noodzakelijk is voor de doeleinden van de Verwerking, hierbij worden de van toepassing zijnde bewaar- en vernietigtermijnen in acht genomen.
- Iedere Betrokkene heeft recht op inzage respectievelijk verbetering, aanvulling, verwijdering of afscherming van de in de afzonderlijke Verwerkingen hem betreffende Persoonsgegevens, en heeft het recht van verzet.
- De instelling kan aan Betrokkenen op transparante wijze verantwoording afleggen over welke gegevens er allemaal verzameld worden en over de verwerkingen daarvan en de daarbij gehanteerde principes.
- Bij alle registraties op vrijwillige basis zal aan de Betrokkene altijd, voor bijvoorbeeld het plaatsen van foto's op social media of publicaties (zogenaamde Opt-in), aantoonbare toestemming worden gevraagd en daarnaast krijgt de Betrokkene de mogelijkheid om zijn toestemming weer in te trekken (de zogenaamde Opt-out).

1.9 Toevoegingen vanuit de AVG (2016)

- Studenten onder 16 jaar worden door de ouders vertegenwoordigd in het kader van privacy. Dit geldt ook voor social media. Ouders moeten dus toestemming geven voor het gebruik van Facebook (in een onderwijskader) van hun minderjarig kind.
- Betrokkenen hebben het recht om "vergeten" te worden. Hetgeen betekent dat op het verzoek van een betrokkene alle persoonlijke data gewist moet worden. Indien dit de uitvoering van de te leveren diensten (denk aan wettelijke eisen) door SVO t.b.v. deze persoon niet in de weg staat.
- Iedere onderwijsinstelling dient een Functionaris Gegevensbescherming (FG) te benoemen omdat er sprake is van "regelmatige en stelselmatige observatie".

2 Governance informatiebeveiligingsbeleid

Het goed, efficiënt en verantwoord leiden van een organisatie wordt vaak aangeduid met de term governance. Het omvat vooral ook de relatie met de belangrijkste belanghebbenden van de instelling, zoals de eigenaren, werknemers, ouders, studenten, andere afnemers en de samenleving als geheel. Een goed corporate governance-beleid draagt zorg voor de rechten van alle belanghebbenden.
Gezien de omvang van de SVO organisatie komen er geen nieuwe functies maar worden de taken toebedeeld aan de huidige medewerkers.

Functionarissen die we nu hebben krijgen een rol in dit geheel.

- Directeur bedrijfsvoering
- IBP coördinator als onderdeel (rol) van de functie ICT adviseur
- Functionaris gegevensbescherming
- Functioneel beheer van de systemen Exact, KRD, HR,
- ICT beheer en adviseur;
- Manager OKC
- Proceseigenaren: PZ en Studenteadministratie

2.1 Informatiebeveiliging en Privacy (IBP) governance

In deze paragraaf wordt beschreven hoe IBP-governance in SVO Vakopleiding Food is georganiseerd en wie waarvoor verantwoordelijk is.
Gezien de omvang van de SVO organisatie komen er geen nieuwe functies maar worden de taken toebedeeld aan de huidige medewerkers.

- Directeur bedrijfsvoering (Hans Witteveen)
- IBP coördinator als onderdeel (rol) van de functie ICT adviseur (Bertha Lenstra)
- Functionaris voor gegevensbescherming (Ronald Sloot)

Schematisch weergegeven:

Niveau	*Wat?*	*Wie?*	*Overleg*	*Documenten*
Strategisch	• *Bepalen IBP strategie* • *Organisatie t.b.v. IBP inrichten*	• *CvB* • *Directeur Bedrijfsvoering* • *IBP coördinator* • *Proceseigenaren PZ en Studentenadministratie*	*CvB stelt vast* *Strategisch IBP-overleg adviseert* *Overleg OR en Studentenraad*	• *IBP beleidsplan*
Tactisch	*Planning & Control IBP:* • *voorbereiden* • *evalueren beleid en maatregelen*	• *Directeur bedrijfsvoering* • *Proceseigenaren PZ, Studentenadministratie en IBP coördinator* • *Manager OKC* • *Functionaris voor de Gegevensbescherming*	*IBP Team*	• *Verbeterplan en jaarplan*
Operationeel	• *Implementeren IBP-maatregelen* • *registreren en evalueren incidenten en aanvragen* • *communicatie eindgebruikers*	• *Functioneel Beheerders* • *ICT beheer* • *IBP Coördinator*	*Operationeel IBP overleg*	• *Incidenten en aanvragen registratie, incl. evaluatie*

De financiering van informatiebeveiliging en privacy wordt bij SVO Vakopleiding Food opgenomen in de begroting van de FPenC.

2.1.1 Het informatiebeveiliging en privacy beleid

Het informatiebeveiliging en privacy beleid ligt ten grondslag aan de aanpak van informatiebeveiliging en privacy binnen de instelling. In het informatiebeveiliging en privacy beleid worden de randvoorwaarden en uitgangspunten vastgelegd en de wijze waarop het beleid wordt vertaald in concrete maatregelen. Om ervoor te zorgen dat het beleid gedragen wordt binnen de organisatie en de organisatie er naar handelt wordt het uitgedragen door (of namens) het College van Bestuur. Het informatiebeveiliging en privacy beleid wordt opgesteld door de directeur Bedrijfsvoering in overleg met de proceseigenaren en vastgesteld door het College van Bestuur.

2.1.2 Jaarplan/verslag

Iedere 2 jaar stelt de directeur Bedrijfsvoering een verslag en een plan voor de komende 2 jaar vast. Het plan is mede gebaseerd op de resultaten van de periodieke controles / audits. Er wordt o.a. ingegaan op incidenten en verzoeken die het afgelopen 2 jaar hebben plaatsgevonden.

2.1.3 Contracten applicaties en educatieve software

Met alle leveranciers van onderwijs- en bedrijfsapplicaties en educatieve software worden verwerkersovereenkomsten afgesloten. SVO Vakopleiding Food maakt gebruik van het Privacy convenant Kennisnet. Dit Privacy convenant zorgt ervoor dat het gebruik van digitale onderwijsmiddelen in lijn is met de AVG. Een "Model overeenkomst", die onderdeel is van het convenant, wordt door SVO Vakopleiding Food altijd ter ondertekening voorgelegd aan leveranciers van digitale onderwijsmiddelen.

2.2 Controle, naleving en sancties

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het informatiebeveiliging en privacy proces. Van belang hierbij is dat directeuren en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Voor de bevordering van de naleving van de AVG vervult de functionaris gegevensbescherming (FG) een belangrijke rol, bijvoorbeeld ten aanzien van opname en afhandeling van klachten. Deze wordt aangesteld door het College van Bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. Deze FG werkt via een door het CvB vast te stellen reglement. Deze rol wordt als een taak belegd binnen de organisatie, met waarborgen voor een functioneren zonder "last of ruggespraak". De omvang van de taak wordt tweejaarlijks in het plan vastgesteld. Mocht de naleving tekort schieten, dan kan SVO Vakopleiding Food de betrokken verantwoordelijke medewerkers een sanctie op leggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.

2.3 Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom wordt bij SVO Vakopleiding Food het bewustzijn voortdurend aangescherpt, zodat kennis van risico's wordt verhoogd en het (veilig en verantwoord) gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingsactiviteiten voor medewerkers, studenten en gasten. Zulke activiteiten kunnen aansluiten bij landelijke campagnes in het mbo en vo onderwijs (Kennisnet). Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van de directeur Bedrijfsvoering; uiteindelijk is ook hiervoor het College van Bestuur eindverantwoordelijk.

2.4 Organisatie van de informatiebeveiliging en privacy rollen (functies)

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij SVO Vakopleiding Food een aantal rollen onderkend die aan functionarissen in de bestaande organisatie zijn toegewezen.

2.4.1 College van Bestuur

Het College van Bestuur is eindverantwoordelijk voor de informatiebeveiliging en privacy binnen SVO Vakopleiding Food en stelt het beleid en de basis maatregelen op het gebied van informatiebeveiliging en privacy vast. De inhoudelijke verantwoordelijkheid voor informatiebeveiliging en privacy is gemandateerd aan de directeur Bedrijfsvoering. Deze heeft de opdracht om voor de informatiebeveiliging en privacy voor de gehele instelling zorg te dragen.

2.4.2 Portefeuillehouder informatiebeveiliging

Directeur Bedrijfsvoering is gesprekspartner voor de IBP coördinator in kader van informatiebeveiliging en privacy binnen SVO Vakopleiding Food.

2.4.3 Coördinator IBP

IBP is een taak op strategische en tactisch/operationeel niveau, deel uitmakend van de functie van de coördinator IBP. Hij of zij adviseert aan de Directeur Bedrijfsvoering. De coördinator IBP bewaakt de uniformiteit binnen SVO Vakopleiding Food.
Hij ziet er bovendien op toe dat:

- Activiteiten van systeembeheerders en -operators worden vastgelegd en de logbestanden worden beschermd en regelmatig beoordeeld.
- Het management beoordeelt regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen.

2.4.4 Functioneel beheerder

De rol van functioneel beheerder bedrijfsapplicaties is vormgegeven bij de centrale diensten van SVO Vakopleiding Food en de educatieve content applicaties is vormgegeven bij de onderwijsafdelingen.

2.4.5 Proceseigenaar

Een proceseigenaar is iemand die verantwoordelijk is voor een van de primaire of ondersteunende processen, zoals HR en Studenten administratie.
De systeemeigenaar is er verantwoordelijk voor dat de applicatie een goede ondersteuning biedt aan het proces waarvoor deze verantwoordelijk is. Dit betekent dat de systeemeigenaar er voor zorgt dat zowel nu als in de toekomst de applicatie blijft beantwoorden aan de eisen en wensen van de gebruikers en aan wet- en regelgeving. Uiteraard moet de applicatie voldoen aan het informatiebeveiligingsbeleid en tenminste aan de basis maatregelen.
De proceseigenaar is verantwoordelijk om de risico's die veroorzaakt worden doordat personen of applicaties ten onrechte toegang krijgen tot applicaties te verkleinen. Hiertoe hebben ze een drietal bevoegdheden:

- Samen met de directeur Bedrijfsvoering en de IBP coördinator stellen zij het beleid voor toegang vast.
- Samen met functioneel beheer en ICT beheer zien zij er op toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.
- Samen met functioneel beheer en ICT beheer beoordelen zij regelmatig de toegangsrechten van gebruikers.

Een beperkt aantal proceseigenaren is tevens Persoonsgegevensstroom eigenaar. SVO Vakopleiding Food onderkent de volgende Persoonsgegevensstromen:

- **Studenten**;
- Ouders:
- Belangstellenden;
- Alumni;
- Proefpersonen (onderzoek);
- **Medewerkers**;
- Externen;
- Stage verlenende organisatie medewerkers;
- Aanbesteding medewerkersgegevens (Bijvoorbeeld CV van mogelijke externe projectleiders).

2.4.6 Functionaris Gegevensbescherming

De functionaris voor de gegevensbescherming (FG) houdt binnen SVO Vakopleiding Food toezicht op de toepassing en naleving van de Wet bescherming persoonsgegevens. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie.

2.4.7 ICT beheer

De rol van ICT beheer is vormgegeven op het stafniveau van SVO Vakopleiding Food.

3 Classificatie

3.1 Risico's

De volgende vier grootste privacy risico's bij SVO Vakopleiding Food willen we op korte termijn aan pakken:

- Ongewenste verspreiding van zorgdossiers van studenten.
- Ongewenste verspreiding van verslagen voortvloeiend uit de gesprekscyclus (functioneren, beoordelen, etc.).
- Ongecontroleerde toegang tot het netwerk en applicaties.
- Verlies van privacy gevoelige data (datalekken).

Deze risico's worden verkleind door beleid, training en classificatie.

3.2 Gehanteerde classificatie standaard

SVO Vakopleiding Food hanteren de classificatie standaarden zoals die verwoord zijn in Certificeringsschema Informatiebeveiliging en privacy dat wordt beheer binnen Edustandaard. Deze standaard is onderdeel van de Referentie Onderwijs Sector Architectuur (ROSA).

Bij SVO Vakopleiding Food zijn alle gegevens waarop dit informatiebeveiligingsbeleid van toepassing is, geclassificeerd. Het niveau van de beveiligingsmaatregelen is afhankelijk van de klasse.
De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses.
Daarbij zijn de volgende kwaliteitsaspecten van informatievoorziening van belang:

Beschikbaarheid: De mate waarin beheersmaatregelen de beschikbaarheid en ongestoorde voortgang van de ICT-dienstverlening waarborgen.

Integriteit: De mate waarin de beheersmaatregelen (organisatie, processen en technologie) de juistheid, volledigheid en tijdigheid van de IT-dienstverlening waarborgen.

Vertrouwelijkheid: De mate waarin uitsluitend geautoriseerde personen, programmatuur of apparatuur gebruik kunnen maken van de gegevens of programmatuur, al dan niet gereguleerd door (geautomatiseerde) procedures en/of technische maatregelen.

A. Beschikbaarheid

Ten aanzien van de beschikbaarheidseisen is voor de volgende classificatie gekozen:

Classificatie indeling	Classificatie gevolg	Beheersmaatregel
Beschikbaarheid **Midden**	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan **48 uur** brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.	Zie: Certificeringsschema Informatiebeveiliging en privacy

B. Integriteit

Voor integriteit wordt de volgende classificatie indeling gehanteerd:

Classificatie indeling	Classificatie gevolg	Beheersmaatregel
Integriteit **Laag**	Het bedrijfsproces staat **enkele** integriteitsfouten toe.	Applicatie controle
Integriteit **Midden**	Het bedrijfsproces staat **zeer weinig** integriteitsfouten toe. Bescherming van integriteit is absoluut noodzakelijk.	Applicatie plus menselijke controle
Integriteit **Hoog**	Het bedrijfsproces staat **geen** integriteitsfouten toe.	Applicatie plus twee maal menselijke controle

C. Vertrouwelijkheid
Vertrouwelijkheid is als volgt geclassificeerd:

Classificatie indeling	Classificatie gevolg	Beheersmaatregel
Vertrouwelijkheid **Laag**	Informatie die toegankelijk mag of moet zijn voor **alle of grote groepen** medewerkers of ouders of studenten. Vertrouwelijkheid is gering.	Toegang tot netwerk op basis van arbeids-overeenkomst of leerling inschrijving.
Vertrouwelijkheid **Midden**	Informatie die alleen toegankelijk mag zijn voor een **beperkte groep** gebruikers. De informatie is vertrouwelijk.	Toegang op basis van autorisatiematrix
Vertrouwelijkheid **Hoog**	Dit betreft zeer vertrouwelijke informatie, alleen bedoeld voor **specifiek benoemde personen**, waarbij onbedoeld bekend worden buiten deze groep grote schade kan toe brengen.	Toegang op basis van autorisatiematrix plus pasje of sms code (2 way authentication)
Vertrouwelijkheid **Zeer hoog**	Dit betreft zeer vertrouwelijke informatie (bijzondere persoonsgegevens), alleen bedoeld voor **één specifiek benoemde personen en de betrokkene**, waarbij onbedoeld bekend worden buiten deze persoon grote schade kan toe brengen	Alleen beschikbaar op papier.

Welk beveiligingsniveau geschikt is voor een bepaald informatiesysteem hangt af van de classificatie van de informatie die het systeem verwerkt. De classificatie dient door de proceseigenaar te worden bepaald.

3.3 Voorbeeld classificatie en labelen

Deze classificatie wordt samengevat tot BIV (Beschikbaarheid-Integriteit-Vertrouwelijkheid) waar vervolgens door de proceseigenaren scores aan worden toegevoegd. Zo zou de proceseigenaar onderwijs het zorgdossier kunnen classificeren met Integriteit en Vertrouwelijkheid Hoog. Kort weergegeven als BIV-MHH. Het gelabelde proces zorgdossier wordt geclassificeerd MHH.

4 Wet- en regelgeving

4.1 Wettelijke voorschriften

Bij SVO Vakopleiding Food wordt op de volgende wijze omgegaan met relevante wet- en regelgeving.

4.1.1 Wet Educatie en Beroepsonderwijs (WEB) en Wet Voorgezet Onderwijs (WVO)

SVO Vakopleiding Food heeft een kwaliteitszorgsysteem, waarin (onder meer) het zorgvuldig omgaan met gegevens in de studenten administratie en met de zorgdossiers is gewaarborgd..

4.1.2 Algemene Verordening Gegevensbescherming (AVG)

SVO Vakopleiding Food heeft de wettelijke vereisten (juistheid en nauwkeurigheid van gegevens en passende technische en organisatorische maatregelen tegen verlies en onrechtmatige verwerking) geïmplementeerd via het informatiebeveiliging en privacy beleid.
De ingangsdatum van de AVG is 25 mei 2016 en de inwerkingtreding is 25 mei 2018. De AVG komt in plaats van de Wbp (Wet bescherming persoonsgegevens).

4.1.3 Archiefwet

SVO Vakopleiding Food houdt zich aan de voorschriften uit de Archiefwet en het Archiefbesluit over de wijze waarop omgegaan moet worden met informatie vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites, e.d..

4.1.4 Auteurswet

SVO Vakopleiding Food verspreidt geen originele werken zonder dat daarvoor toestemming is verkregen van de eigenaar van de auteursrechten. Dit impliceert ook dat SVO Vakopleiding Food het gebruik van software zonder het bezitten van de juiste licenties tegen gaat.

4.1.5 Wetboek van Strafrecht

In het Wetboek van Strafrecht zijn de laatste decennia een aantal specifieke bepalingen opgenomen over de strafrechtelijke probleemgebieden in relatie tot het computergebruik. De wet schrijft voor dat "enige beveiliging" vereist is alvorens er sprake *kan zijn* van het eventueel strafrechtelijk vervolgen van delicten jegens de onderwijsinstelling en het eventueel vrijwaren van bestuurders van de instelling.
Naleving van dit informatiebeveiliging en privacy beleid en implementatie van de basis maatregelen bij SVO Vakopleiding Food moet leiden tot een niveau van beveiliging dat als voldoende mag worden gezien in het kader van het Wetboek van Strafrecht.

4.2 Overige voorschriften (opties)

1. Bepalingen uit de cao.
2. Gedragscode internet-, e-mail- en social mediagebruik
3. Wachtwoordpolicy
4. Algemene gedragscode (privacy afspraken)
5. Werkproces datalekken (bijlage 1)
6. Reglement verantwoord netwerkgebruik studenten SVO Vakopleiding Food
7. Reglement verantwoord netwerkgebruik medewerkers SVO Vakopleiding Food
8. Dataregister studenten plus toelichting
9. Dataregister medewerkers plus toelichting
10. Dataregister externen (2018)
11. Reglement gebruik social media voor medewerkers en docenten
12. Toestemming gebruik beeldmateriaal studenten
13. Toestemming gebruik beeldmateriaal medewerkers
14. Beleid cameratoezicht
15. Rechten van de betrokkenen (AVG)

16. (Responsible disclosure)
17. Integriteitscode
18. Role Based Access
19. BCM, verwijs naar crisisteam
20. Beleid toegangsbeveiliging netwerk en systemen
21. DSP

5 Melding en afhandeling van incidenten en verzoeken

5.1 Registratie informatiebeveiliging en privacy incidenten

Het is van belang om te leren van incidenten en verzoeken. Incident- en verzoekregistratie en periodieke rapportage over opgetreden incidenten en verzoeken horen thuis in een volwassen informatiebeveiligingsomgeving. Gezien de meldplicht datalekken die per 1 januari 2016 is opgenomen in de WBP heeft SVO Vakopleiding Food een protocol datalekken ontwikkeld. Daarin is beschreven op welke wijze binnen 2 werkdagen bij de toezichthouder datalekken kunnen worden gemeld. Op het niet (tijdig) melden van datalekken staat een boete. Als de privacy van betrokkenen is geschaad, moeten ook zij worden geïnformeerd over het datalek. Deze korte meldingstermijn maakt dat vooraf procesafspraken in een datalekken protocol zijn gemaakt en dat er een medewerker (de Functionaris voor Gegegevensbescherming) is aangewezen om deze melding te doen. De Autoriteit Persoonsgegevens heeft in een richtsnoer in december 2015 bekend gemaakt op welke manieren een datalek[2] moet worden gemeld.

5.2 IBP Team[3]

Het doel van het IBP Team bij SVO Vakopleiding Food is instelling brede preventie en curatieve zorg voor informatiebeveiliging en privacy incidenten.
De leden van het IBP Team zijn benoemd door het College van Bestuur en opereren in diens opdracht. Het IBP Team is gerechtigd het isoleren van computersystemen of netwerksegmenten te gelasten.
Het IBP Team van SVO Vakopleiding Food heeft de volgende opdracht:

- Het signaleren en registreren[4] van alle privacy verzoeken, beveiligingsincidenten en datalekken, het coördineren van de bestrijding en het toezien op de oplossing van problemen die tot incidenten hebben geleid of door de incidenten zijn veroorzaakt (of het bieden van ondersteuning daarbij);
- Het geven van voorlichting en het doen van algemene aanbevelingen aan netwerkbeheerders, systeembeheerders, ontwikkelaars en eindgebruikers door het verspreiden van informatie;
- De IBP coördinator zal eens per jaar een rapportage aanleveren over alle ibp incidenten.

Bij een calamiteit kan het IBP Team terstond bij elkaar worden geroepen op initiatief van de Coördinator IBP, in opdracht van het College van Bestuur. Doel is om de **continuïteit** van de informatievoorziening en de privacy te continueren. Onder calamiteiten wordt verstaan:

- Datalek;
- Grote verstoringen van het netwerk (bijvoorbeeld DDoS aanval);
- Natuurrampen (brand, overstroming, storm, etc.).

Het IBP Team bij SVO Vakopleiding Food behandelt meldingen vertrouwelijk en verstrekt alleen informatie over beveiliging en privacy incidenten als dat noodzakelijk en relevant is voor de oplossing van een incident.
De dienstverlening van het IBP Team bij SVO Vakopleiding Food is gedocumenteerd en door het College van Bestuur bekrachtigd.
De rol van IBP Team coördinator wordt belegd bij de Coördinator IBP.

[2] Zie bijlage 4: Datalekken
[3] Zie 2.1 voor de samenstelling.
[4] Bijvoorbeeld m.b.v. Topdesk

Bijlage 4: Datalekken

De Wet bescherming persoonsgegevens (Wbp) is per 1 januari 2016 gewijzigd en er geldt een meldplicht voor datalekken. Organisaties die verantwoordelijk zijn voor de verwerking van persoonsgegevens, zijn voortaan verplicht om een datalek bij de Autoriteit Persoonsgegevens (AP) te melden.

Voorbeelden van een datalek zijn:
- per ongeluk gegevens wissen
- verloren USB-stick of ander opslagmedium
- gestolen apparatuur zoals laptops
- inbraak (hacker)
- calamiteit zoals een brand zonder dat er een back-up is

Het personeelslid dat geconfronteerd wordt met een datalek meldt dit direct bij de afdeling IM. IM doet een analyse en inschatting van het risico en bepaald na afstemming met directeur Bedrijfsvoering of het datalek gemeld dient te worden bij AP. IM informeert tevens de betreffende leidinggevende van het personeelslid over de melding. Bij afwezigheid van de directeur Bedrijfsvoering wordt afgestemd met CvB.

In geval van een daadwerkelijk datalek zal de Functionaris voor Gegevensbescherming (of medewerker IM) binnen 72 uur het volgende doen:
- melding bij de autoriteit persoonsgegevens
- de slachtoffers informeren

De Functionaris voor Gegevensbescherming (IM) zal het datalek registreren en de acties uitzetten die nodig zijn. IM draagt zorg voor het vernietigen van gegevensdragers zoals tapes en harde schijven.
Alle tapes en harde schijven die niet meer gebruikt worden moeten ingeleverd worden bij de afdeling IM en deze laat ze vervolgens door een gecertificeerd bedrijf vernietigen. Dus bij systemen die vervangen worden zal als eerste de harde schijf verwijderd worden voor het systeem wordt afgevoerd.