A.1 Opdrachtverstrekking:
Dit informatiebeveiligingsbeleid wordt in opdracht van het College van Bestuur uitgevoerd.

A.2 Doel van de beleidsnotitie:
Het voor het College van Bestuur verschaffen van aansturing en steun voor informatiebeveiliging in overeenstemming met bedrijfseisen en relevante wet- en regelgeving.

D. Referenties
- Informatiebeleid Informatisering 2017-2019
- CvB meerjarenplan Ambitie, Aandacht en Ambiance 2018-2021

E. Distributie
Het is van groot belang dat het informatiebeveiligingsbeleid en de hieruit volgende principes en richtlijnen bekend zijn bij alle betrokkenen binnen KWIC. De Information Security Officer is verantwoordelijk voor de communicatie van het beleid. Het bevorderen van het beveiligingsbewustzijn bij management en medewerkers vormt een belangrijk aandachtspunt bij deze communicatie.

1. Definities

Onder informatiebeveiliging wordt verstaan:
Informatiebeveiliging betreft alle maatregelen die gericht zijn op het waarborgen van Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) van informatie.

Informatiebeveiliging richt zich dus primair op drie aspecten van de informatievoorziening:
- **beschikbaarheid**, de informatie moet op de gewenste momenten beschikbaar zijn;
  risico: informatie is niet toegankelijk/ raakt zoek.
- **integriteit**, de informatie moet juist en volledig zijn en de informatiesystemen moeten juiste en volledige informatie opslaan en verwerken;
  risico: informatie wordt verminkt / gemanipuleerd.
- **vertrouwelijkheid**, de informatie moet alleen toegankelijk zijn voor degene die hiervoor bevoegd is.
  risico: informatie valt in verkeerde handen.

De doelstelling van informatiebeveiliging is tweeledig:

1. Waarborging van de continuïteit van de interne bedrijfsvoering en primaire processen binnen organisaties;
2. Minimalisatie van de schade en de eventuele gevolgen voor organisaties als gevolg van beveiligingsincidenten.

2. Toepassingsgebied

Dit informatiebeveiligingsbeleid geeft sturing aan het managementsysteem voor informatiebeveiliging (ISMS) dat van toepassing is op de informatie en de -systemen van KWIC. Vanaf 2016 is het toepassingsgebied van het ISMS:

- locatie Vlijmenseweg 2 in ’s-Hertogenbosch;
- locatie Onderwijsboulevard 3 in ’s-Hertogenbosch;
- gegevensuitwisseling van KWIC met andere organisaties.

Het beleid richt zich op de studenten, eigen medewerkers, tijdelijk personeel en op personeel dat door derden wordt ingezet om diensten te verlenen aan onze organisatie, en geeft richting aan het managementsysteem voor informatiebeveiliging (ISMS).
De belanghebbenden die relevant zijn voor de context van dit ISMS zijn:

Belanghebbenden relevant voor ISMS	*Eisen van belanghebbenden*
1 Studenten	Privacy reglement voor studentenbescherming
2 Medewerkers	Vakbekwaamheid Middelen
3 College van bestuur	Statuten KWIC Bestuursreglement (tussen RvT en CvB) Cao mbo: Collectieve arbeidsovereenkomst voor beroepsonderwijs en volwasseneducatie Continuïteit van onderneming
4 Raad van Toezicht	Governance Code BVE overleg Bestuursreglement (tussen RvT en CvB) Reglement commissies Raad van Toezicht Integriteitscode medewerkers
5 Branche organisatie Vereniging MBO Raad te Woerden	Cao mbo: Collectieve arbeidsovereenkomst voor beroepsonderwijs en volwasseneducatie
6 Overheden - Ministerie OCW - Autoriteit persoonsgegevens - Inspectie van onderwijs	Algemene Verordening Gegevensbescherming Leerlingen, deelnemers en studenten. Wet op onderwijs toezicht
7 Accountant	Regels omtrent financiële rapportages en integriteit financiële systemen
8 Strategische ontwikkelpartners	Werkwijze van software ontwikkelpartners
9 (Strategische) leveranciers	Gecategoriseerd volgens Informatiebeveiligingsbeleid voor Leveranciersrelaties Rapportage Informatiebeveiliging en Privacy voor leveranciersrelaties

10 Ouders	Zorgvuldige informatievoorziening m.b.t. studenten
11 BPV-bedrijven	Goede praktijkvorming van de studenten

De scope van het managementsysteem voor informatiebeveiliging (ISMS) luidt:

De veiligheid van informatie(-) en communicatiesystemen bij de activiteiten onderwijslogistiek, informatielogistiek, studentenadministratie, HRM en beroepspraktijkvorming voor het MBO onderwijs voor de locaties aan de Vlijmenseweg en de Onderwijsboulevard. Dit is in overeenstemming met de Verklaring Van Toepasselijkheid versie 6.0 d.d. 25-03-2019.

In de verklaring van toepasselijkheid staat welke beheersmaatregelen uit de ISO 27002:2013 van toepassing zijn op de organisatie. Dit is een apart document.

3. Inhoud

Met dit informatiebeveiligingsbeleid wordt beoogd om op een effectieve en efficiënte manier informatiebeveiligingsmaatregelen af te stemmen op de informatiebeveiligings-behoefte van ons college. De informatievoorziening is van essentieel belang voor de continuïteit van de bedrijfsvoering van KW1C. Zowel op papier als digitaal zijn wij bij ons dagelijks werk afhankelijk van de beschikbaarheid van betrouwbare informatie. Onze organisatie en onze informatievoorziening wordt blootgesteld aan een groot aantal bedreigingen, al dan niet opzettelijk van aard. Deze bedreigingen maken het noodzakelijk om gerichte maatregelen te treffen om de risico's tot een aanvaardbaar niveau te reduceren. Het proces van informatiebeveiliging begint met het definiëren van een beleid en doelstellingen op dit punt.

Informatiebeveiligingsdoelstellingen
Het KW1C geeft met dit beleid een duidelijke richting aan op het gebied van informatiebeveiliging en streeft de volgende doelen na om een adequaat niveau van beveiliging conform de ISO 27001 norm en alle relevante wet- en regelgeving te bereiken:

- het garanderen van correcte en veilige informatievoorzieningen;
- het beschermen van kritieke bedrijfsprocessen;
- het beschermen en correct verwerken van persoonsgegevens van studenten, medewerkers, externen etc.;
- het minimaliseren van risico's;
- het adequaat reageren op incidenten;
- het bereiken van informatiebeveiligingsbewustzijn bij medewerkers, management en alle andere bij het KW1C betrokken medewerkers, zoals inhuurkrachten, stagiaires en dienstverleners;
- het inbedden van het component informatiebeveiliging in de werkzaamheden van alle organisatieonderdelen;
- het 'in control' zijn op alle informatiebeveiligingsmaatregelen die genomen zijn en die nog nodig zijn, verankerd in een PDCA-cyclus;
- het waarborgen van de naleving van dit beleid.

Beleidsuitgangspunten informatiebeveiliging

Bij de toepassing van informatiebeveiliging binnen KWIC worden de volgende uitgangspunten gehanteerd:

1. Alle informatie is beschikbaar volgens het classificatieschema KW1C met bijbehorende beheersmaatregelen (zie hiervoor "*08.2 ISMS Classificatie, labeling en behandeling van informatie*").
2. Het informatiebeveiligingsbeleid is bedoeld voor alle interne en externe gebruikers, die op enige wijze gebruik maken van ICT-infrastructuur, informatie en/of informatie- systemen van het college.
3. Het beleid heeft betrekking op alle netwerk- en informatievoorzieningen die onder verantwoordelijkheid van het KWIC vallen. Voor de toegang vanuit en naar externe netwerken en systeemvoorzieningen dienen door het college specifieke beveiligingseisen te worden vastgesteld.
4. KWIC streeft ernaar aantoonbaar te voldoen aan de norm ISO 27001, het hebben van een geschikt, adequaat en doeltreffend management systeem voor Informatiebeveiliging (ISMS).
5. KWIC voldoet aan alle geïnventariseerde en van toepassing zijnde wet- en regelgeving rondom informatiebeveiliging.
6. Beveiliging van informatie is een onderdeel van de integrale managementverantwoordelijkheid. Alle onderdelen van KWIC hebben hiertoe verantwoordelijkheden voor informatiebeveiliging toegewezen en vastgelegd.
7. Opdrachten aan derden voor het uitvoeren van werkzaamheden worden zodanig omgeven met maatregelen dat er geen inbreuk op de beschikbaarheid, vertrouwelijkheid, integriteit van de geautomatiseerde informatievoorziening kan ontstaan.
8. Bij de verwerking en het gebruik van data worden maatregelen getroffen om de privacy van studenten, medewerkers en overige stakeholders te waarborgen.
9. Wanneer (onderdelen van) KWIC samenwerkingsverbanden aangaan met externe partijen, hetzij inhoudelijk, hetzij voor de ontwikkeling of het beheer van de informatievoorziening, worden ook risico's t.a.v. informatiebeveiliging meegenomen. Afspraken hierover worden schriftelijk vastgelegd en op de naleving hiervan wordt toegezien.
10. De informatiesystemen en informatie van alle onderdelen van KWIC zijn volgens een gestructureerde methode geclassificeerd zodat duidelijk is welke passende beveiligingsmaatregelen van toepassing zijn.
11. Bij de aanname, tijdens het dienstverband en in geval van ontslag van medewerkers of het inhuren van extern personeel (leveranciers/ installateurs, etc.) wordt meegenomen de betrouwbaarheid van de desbetreffende persoon en de waarborging van de vertrouwelijkheid van informatie.
12. KWIC voert een actief beleid om het beveiligingsbewustzijn van management en medewerkers te stimuleren. Hiertoe voert de Information Security Officer, in samenwerking met de leidinggevenden, periodiek bewustwordingscampagnes uit.
13. KWIC beschikt over gedragsregels voor het gebruik van (algemene) informatievoorzieningen. Op de naleving van deze gedragsregels wordt toegezien door de leidinggevenden.
14. Bij overtreding van de regelgeving voor informatiebeveiliging en/of relevante wettelijke bepalingen kan het College van Bestuur en/of afdelingsdirecteur een sanctie opleggen

denkend aan non-actiefstelling, disciplinaire straffen, en beëindiging van het dienstverband.

15. Alle onderdelen van KWIC hebben maatregelen getroffen voor de fysieke beveiliging van mensen en middelen, die van toepassing zijn op de vertrouwelijke informatie en apparatuur waarop deze informatie is opgeslagen.
16. Aanschaf, installatie en onderhoud van geautomatiseerde data verwerkende systemen en/of programmatuur, alsmede inpassing van nieuwe technologieën, mogen geen afbreuk doen aan de veiligheid en continuïteit van de geautomatiseerde informatievoorziening.
17. De organisatie heeft adequate maatregelen getroffen voor continuïteitsbeheer waardoor de beschikbaarheid van de bedrijfsprocessen en de hierbij gebruikte informatie(systemen) is gewaarborgd. Het beheren van een continuïteitsplan, het inrichten van een crisisorganisatie en het oefenen van de getroffen maatregelen vormen hiervan een onderdeel.
18. Als onderdeel van het managementsysteem voor informatiebeveiliging wordt binnen KWIC door interne en externe partijen door middel van audits toegezien op de naleving van het informatiebeveiligingsbeleid.
19. Alle medewerkers van KWIC beschikken over middelen voor het melden en afhandelen van beveiligingsincidenten. De evaluatie van de afhandeling van beveiligingsincidenten wordt benut voor de verbetering van informatiebeveiliging.

Risicobeoordeling informatiebeveiliging

De vertaalslag van beleid naar een plan en vervolgens concrete maatregelen heeft alles te maken met het inzichtelijk maken van de informatiebeveiligingsrisico's die KWIC loopt. Hiervoor is een risicobeoordelings- en behandelprocedure opgesteld (gebaseerd op ISO31000 Risicomanagement) voor alle belanghebbenden van dit ISMS.

Organisatie en verantwoordelijkheden

Verantwoordelijkheden voor informatiebeveiliging dienen eenduidig belegd te zijn met scheiding van taken indien noodzakelijk. Zowel voor het management als voor de informatiebeveiligers geldt dat ze verantwoordelijkheden hebben en moeten nemen om de kwaliteit van de informatiebeveiliging te waarborgen. Hiervoor is een apart document organogram en ISMS verantwoordelijkheden opgesteld.

Het **College van Bestuur** bepaalt de strategie, doelen en de hoogte van het beveiligingsniveau. Dit is het bepalen van de hoogte / zwaarte van de investering en de zwaarte van het pakket van beveiligingsmaatregelen.

Namens het College van Bestuur is de beleidsgroep **Informatiebeveiliging & Privacy** bevoegd om o.a. beleid issues rondom informatiebeveiliging goed te keuren, uit te dragen en erop toe te zien. De Information Security Officer maakt deel uit van deze groep.

De **Information Security Officer** valt functioneel onder het College van Bestuur en is op de hoogte van juridische kennis inzake het informatiebeveiligingsbeleid.

Security overleggen
Elke maand vindt een overleg plaats van de Beleidsgroep Informatiebeveiliging & Privacy waarin alle zaken in het kader van Informatiebeveiliging & Privacy besproken worden.

Twee keer per jaar is een overleg betreffende overeenkomsten in het kader van informatiebeveiliging en privacy waarin zitting hebben:
- Information Security Officer;
- Functionaris voor Gegevensbescherming;
- Juridisch specialist DG&C voor onderwijszaken;
- Hoofd Inkoop voor het contractmanagement.

Elk kwartaal vindt een security overleg plaats waarin zitting hebben:
- Information Security Officer;
- Functionaris voor Gegevensbescherming;
- Hoofd Beveiliging voor de fysieke beveiliging;
- Technisch Security Officer.

Desgewenst kunnen experts uit andere afdelingen aan dit overleg deelnemen. Te denken valt aan de afdelingen:

DGC – het beheer en toezien op werking van interne audit proces;

INF – verantwoordelijkheid voor de beveiligingsmaatregelen rondom nieuwe ICT projecten en applicatiebeheer;

FB & IT – verantwoordelijkheid voor de beveiligingsmaatregelen rondom de technische ICT en het bewaken van de dienstverlening van leveranciers (outsourced).
– verantwoordelijkheid voor de beveiligingsmaatregelen rondom fysieke beveiliging

4.a Verantwoordelijkheden / bevoegdheden
Het College van Bestuur is eindverantwoordelijk voor het informatiebeveiligingsbeleid en heeft dit beleid vastgesteld. De Information Security Officer is verantwoordelijk voor het onderhoud van het informatiebeveiligingsbeleid. Jaarlijks wordt dit beleid geëvalueerd en aangepast indien nodig.

5. Middelen / externe documenten
Overige middelen en documenten, die niet tot het beleid behoren, maar wel gehanteerd kunnen / moeten worden.

- Verklaring van toepasselijkheid
- Risicobehandeling en beoordelingsprocedure
- Classificatie, labeling en behandeling van informatie
- Organogram en ISMS verantwoordelijkheden
- Informatiebeveiligingsbeleid voor Leveranciersrelaties