



**INFORMATIEVEILIGHEIDSBEWUSTZIJN IS DE
BELANGRIJKSTE BEVEILIGINGSMAATREGEEL**

COLOFON

NAAM DOCUMENT

Informatiebeveiligingsbeleid gemeente Ridderkerk

NUMMER ZAAKSYSTEEM

116728

DOEL EN SCOPE INFORMATIEBEVEILIGINGSBELEID

Dit Informatiebeveiligingsbeleid is er op gericht hoe binnen de gemeente Ridderkerk met informatieveiligheid omgegaan moet worden en bevat de beleidsuitgangspunten voor de verdere implementatie. In dit informatiebeveiligingsbeleid wordt uitgewerkt wat:

1. De verantwoordelijkheden zijn van:
 - a. Het college van burgemeester en wethouders;
 - b. De directieraad van de BAR-organisatie en de directie van NV BAR-afvalbeheer;
 - c. De Chief Information Security Officer (CISO);
 - d. De proceseigenaar (lijnmanagent);
 - e. Medewerkers, (keten)partners en belanghebbende(n).
2. De beleidsuitgangspunten zijn;
3. De wijze is waarop het beschermingsniveau wordt vastgesteld.
4. Het doel van informatieveiligheid is.

Door organisatorische, juridische, technische en fysieke informatiebeveiligingsmaatregelen te treffen en te onderhouden is de gemeente Ridderkerk in staat om de kwaliteitskenmerken zoals de beschikbaarheid, vertrouwelijkheid en integriteit van haar gegevens (data) te waarborgen. In dit informatiebeveiligingsbeleid wordt beschreven met welke beleidsuitgangspunten de gemeente Ridderkerk rekening dient te houden bij het borgen van de informatieveiligheid. De beleidsuitgangspunten in dit informatiebeveiligingsbeleid gaan uit van de minimale eisen die worden gesteld aan informatiebeveiliging op basis van de Baseline Informatiebeveiliging Overheid¹ (BIO). Informatiebeveiliging vindt plaats conform “best practices” (de stand der techniek), waarbij geldt dat de vereiste informatiebeveiligingsmaatregelen sterker dienen te zijn naarmate gegevens gevoeliger zijn.

DOELGROEP

Dit informatiebeveiligingsbeleid is van toepassing op de gemeente Ridderkerk en alle uit te voeren processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen), inclusief gegevensverwerking die door de gemeente Ridderkerk in de Cloud of bij (keten)partners zijn of worden ondergebracht. Dit informatiebeveiligingsbeleid is openbaar en is beschikbaar voor proceseigenaren

¹ Vanaf 1 januari 2020 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO vervangt de bestaande baselines informatieveiligheid voor Gemeenten, Rijk, Waterschappen en Provincies. Van BIG, BIR, BIR2017, IBI en BIWA naar BIO. Hiermee ontstaat één gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid, gebaseerd op de internationaal erkende en actuele ISO-normatiek.

(lijnmanagement), applicatiebeheerders, externe partijen, ketenpartners, medewerkers en andere belanghebbende(n).

Dit informatiebeveiligingsbeleid is gebaseerd op de Baseline Informatiebeveiliging Overheid.

VERSIE

Definitief d.d. 23-06-2020

VERSIEBEHEER

Het beheer van dit document berust bij de Chief Information Security Officer

RELATIE MET ANDERE PRODUCTEN

Dit informatiebeveiligingsbeleid heeft een relatie met:

1. De resolutie informatieveiligheid VNG;
2. Eenduidige Normatiek Single Information Audit (ENSIA);
3. De volgende maatregelen uit de Baseline Informatiebeveiliging Overheid;
 - a. Control: 5.1.1;
 - b. Control: 5.1.2;
 - c. Overheidsmaatregel: 5.1.1.1;
 - d. Overheidsmaatregel: 5.1.2.1
4. Overige relevante documenten.

VASTSTELLING EN INWERKINGTREDING

Dit informatiebeveiligingsbeleid treedt in werking na vaststelling door het college van Burgemeester en Wethouders van de gemeente Ridderkerk. Hiermee komt het voorgaande (vastgestelde) informatiebeveiligingsbeleid te vervallen. Dit informatiebeveiligingsbeleid werd vastgesteld door:

Het college van Burgemeester en Wethouders van de gemeente Ridderkerk op 07-07-2020.

INHOUD

COLOFON	2
NAAM DOCUMENT	2
NUMMER ZAAKSYSTEEM	2
DOEL EN SCOPE INFORMATIEBEVEILIGINGSBELEID	2
DOELGROEP	2
VERSIE	3
VERSIEBEHEER	3
RELATIE MET ANDERE PRODUCTEN	3
VASTSTELLING EN INWERKINGTREDING	3
1: INLEIDING / MANAGEMENTSAMENVATTING	5
2: DOEL VAN HET INFORMATIEBEVEILIGINGSBELEID	5
3: VERANTWOORDELIJKHEDEN	5
3.1: VERANTWOORDELIJKHEDEN VAN HET COLLEGE VAN BURGEMEESTER EN WETHOUDERS	5
3.2: VERANTWOORDELIJKHEDEN DIRECTIERAAD BAR-ORGANISATIE EN DE DIRECTIE VAN DE NV BAR-AFVALBEHEER	6
3.3: VERANTWOORDELIJKHEDEN VAN DE CHIEF INFORMATION SECURITY OFFICER (CISO)	7
3.4: VERANTWOORDELIJKHEDEN VAN DE PROCESSEIGENAAR (LIJNMANAGER)	7
3.5: VERANTWOORDELIJKHEDEN MEDEWERKERS, (KETEN)PARTNERS EN BELANGHEBBENDE(N)	8
3.6: SCHEMATISCH WEERGAVE VAN DE VERANTWOORDELIJKHEDEN OP HOOFDLIJNEN	8
4: DOMEINEN WAAR MAATREGELEN WORDEN GETROFFEN	8
5: BELEIDSUITGANGSPUNTEN	9
6: VERPLICHT UIT TE VOEREN STAPPEN	10
6.1: HET UITVOEREN VAN EEN DATACLASSIFICATIE (STAP 1)	10
6.2: HET UITVOEREN VAN EEN DATA PROTECTION IMPACT ASSESSMENT (STAP 2)	11
6.3: UITVOEREN VAN BBN-TOETS EN (DIEPGAANDE) RISICOANALYSE (STAP 3)	11
7: HET DOEL VAN HET INFORMATIEVEILIGHEID	11
7.1: BESCHIKBAARHEID	11
7.2: INTEGRITEIT	11
7.3: VERTROUWELIJKHEID	12
7.4: CONTROLEERBAARHEID	12
BIJLAGEN	12

1: INLEIDING / MANAGEMENTSAMENVATTING

De gemeente Ridderkerk beheert veel gegevens, waaronder (bijzondere) persoonsgegevens, zoals medische- en strafrechtelijke gegevens en gevoelige gegevens, zoals het **BurgerServiceNummer** en financiële gegevens. Burgers en bedrijven verwachten van de gemeente Ridderkerk dat de gemeente zorgvuldig omgaat met deze (persoons)gegevens. Hoe gevoeliger/waardevoller deze (persoons)gegevens zijn, hoe meer maatregelen er getroffen en in stand gehouden moeten worden om deze gegevens te beschermen tegen onrechtmatige toegang en/of misbruik en/of manipulatie. Het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van deze (persoons)gegevens en de continuïteit van de dienstverlening van de gemeente Ridderkerk is waar het uiteindelijk om gaat. Dit kan de gemeente Ridderkerk realiseren door het treffen en onderhouden van passende organisatorische, juridische, technische en fysieke informatiebeveiligingsmaatregelen.

2: DOEL VAN HET INFORMATIEBEVEILIGINGSBELEID

Dit informatiebeveiligingsbeleid is er op gericht hoe binnen de gemeente Ridderkerk met informatieveiligheid omgegaan moet worden en bevat de beleidsuitgangspunten voor de verdere implementatie. In dit informatiebeveiligingsbeleid wordt uitgewerkt wat:

1. De verantwoordelijkheden zijn van:
 - a. Het college van burgemeester en wethouders;
 - b. De directieraad van de BAR-organisatie en de directie van NV BAR-afvalbeheer;
 - c. De Chief Information Security Officer (CISO);
 - d. De proceseigenaar (lijnmanagent);
 - e. Medewerkers, ketenpartners en belanghebbende(n).
2. De beleidsuitgangspunten zijn;
3. De wijze is waarop het beschermingsniveau wordt vastgesteld;
4. Het doel van informatieveiligheid is.

3: VERANTWOORDELIJKHEDEN

3.1: VERANTWOORDELIJKHEDEN VAN HET COLLEGE VAN BURGEMEESTER EN WETHOUDERS

Het college van burgemeester en wethouders van de gemeente Ridderkerk speelt een cruciale rol bij de uitvoering van dit informatiebeveiligingsbeleid. Het college van burgemeester en wethouders van de gemeente Ridderkerk geeft richting aan het informatie-beveiligingsbeleid, bepaalt welke informatiebeveiligingsrisico's acceptabel zijn en welke informatiebeveiligingsrisico's ze wil afdekken. De uitvoering van het informatiebeveiligingsbeleid is belegd bij het bestuur van de BAR-organisatie en de directie van de NV BAR-afvalbeheer. Zij zorgen voor de uitvoering van dit beleid, de implementatie en het onderhouden van een samenhangend pakket aan maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te waarborgen. Het college van burgemeesters en wethouders van de gemeente Ridderkerk houdt hier toezicht op. Daarnaast legt het college van burgemeester en wethouders verantwoording af (aan de landelijke toezichthouders en de gemeenteraad) over de

status van de informatieveiligheid binnen de gemeente. Deze verantwoording bestaat uit een jaarlijkse zelfevaluatie (ENSIA²), een IT-audit, een verklaring van het college van burgemeester en wethouders (collegeverklaring) en een passage over informatieveiligheid in het jaarverslag.

3.2: VERANTWOORDELIJKHEDEN DIRECTIERAAD BAR-ORGANISATIE EN DE DIRECTIE VAN DE NV BAR-AFVALBEHEER

De directieraad van de BAR-organisatie en de directie van de NV BAR-afvalbeheer zijn verantwoordelijk voor het behalen van de gemeentelijke informatiebeveiligingsdoelstellingen. Deze verantwoordelijkheid omvat in elk geval:

1. De implementatie van en het onderhouden van een samenhangend pakket aan maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te waarborgen. Dit pakket van samenhangende maatregelen is gebaseerd op een risicoafweging, waarbij het college van burgemeester en wethouders van de gemeente Ridderkerk aangeeft welke informatiebeveiligingsrisico's worden geaccepteerd en welke informatiebeveiligingsrisico's ze door maatregelen willen afdekken/mitigeren;
2. Het opstellen van en uitvoering geven aan het volgende onderliggend beleid:
 - a. Cryptografiebeleid;
 - b. Logging beleid;
 - c. Wachtwoordbeleid;
 - d. Clear screen clear desk Beleid.
3. Het inrichten en onderhouden van het proces rondom de verplichte jaarlijkse zelfevaluatie over de status van de informatieveiligheid (ENSIA). Het college van burgemeesters en wethouders van de gemeente Ridderkerk dient hierover jaarlijks aan de landelijke toezichthouders en de gemeenteraad bestuurlijke verantwoording af te leggen. Dit proces omvat minimaal:
 - a. Het waarborgen dat aan de auditeisen wordt voldaan;
 - b. Het uitvoeren van de zelfevaluatie;
 - c. Het laten uitvoeren van een IT-audit door een onafhankelijk en daartoe bevoegd auditor;
 - d. Het opstellen en uploaden van de collegeverklaring en het assurance rapport;
 - e. Het opstellen en uploaden van de rapportage BRP en Reisdocumenten;
 - f. Het opstellen en uploaden van de rapportages BAG, BGT en BRO;
 - g. Het afleggen van verantwoording aan het college van burgemeesters en wethouders over de audit resultaten.

3.3: VERANTWOORDELIJKHEDEN VAN DE CHIEF INFORMATION SECURITY OFFICER (CISO)

De Chief Information Security Officer zorgt op basis van de Baseline Informatiebeveiliging Overheid concern breed, voor beleid, coördinatie, advisering en rapportage over een samenhangend pakket aan maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te waarborgen. De verantwoordelijkheid

2 ENSIA (Eenduidige Normatiek Single Information Audit).

voor informatieveiligheid, het implementeren en onderhouden van passende informatiebeveiligingsmaatregelen binnen de organisatieonderdelen van de BAR-organisatie en de NV BAR-afvalbeheer ligt evenwel bij de proceseigenaren (lijnmanagers), waarbij het college van burgemeester en wethouders aangeeft welk risiconiveau zij acceptabel vindt of door maatregelen wil afdekken/mitigeren. De Chief Information Security Officer:

1. Rapporteert rechtstreeks aan de gemeentesecretaris van de gemeente Ridderkerk, aan de directieraad van de BAR-organisatie en aan de directie van de NV BAR-afvalbeheer;
2. Heeft periodiek afstemming met de portefeuillehouder binnen het college van burgemeester en wethouders van de gemeente Ridderkerk over de status van de informatieveiligheid;
3. Controleert steekproefsgewijs de naleving van dit informatiebeveiligingsbeleid;
4. Beoordeeld jaarlijks het informatiebeveiligingsbeleid op haar actualiteit en indien nodig wordt dit geactualiseerd;
5. Is de voorzitter van het interne Computer Emergency Response Team (CERT). (Dit is een intern adviesteam voor wat betreft de afhandeling van informatiebeveiligingsincidenten/cyberdreigingen/cyberaanvallen);
6. Is de vertrouwde contactpersoon voor de informatiebeveiligingsdienst (IBD).

3.4: VERANTWOORDELIJKHEDEN VAN DE PROCESEIGENAAR (LIJNMANAGER)

Het beveiligen van gegevens (data) en de informatiesystemen is geen eenmalige zaak, maar een proces waarbij steeds de Plan-Do-Check-Act cyclus wordt doorlopen. De noodzaak, aard en omvang van de informatieveiligheid is binnen ieder vakgebied en/of organisatieonderdeel anders. Zo heeft ieder proces te maken met een eigen informatievoorziening en eisen die volgen uit (sectorale) wet- en regelgeving. De proceseigenaar (lijnmanager) is verantwoordelijk voor de implementatie en het in stand houden van de informatieveiligheid en de bijbehorende informatiebeveiligingsmaatregelen binnen:

1. Het betrokken organisatieonderdeel en de processen;
2. De bijbehorende informatiesystemen (applicaties, procedures, enzovoorts), inclusief informatiesystemen die in de Cloud³ zijn ondergebracht;
3. De gegevensverzamelingen, inclusief gegevensverwerkingen (data) die in de Cloud of bij (keten)partners zijn ondergebracht;

Daarnaast is de proceseigenaar (lijnmanager) verantwoordelijk voor de periodieke rapportage over de status van de informatieveiligheid binnen zijn of haar organisatieonderdeel en processen aan de Chief Information Security Officer;

3.5: VERANTWOORDELIJKHEDEN MEDEWERKERS, (KETEN)PARTNERS EN BELANGHEBBENDE(N)

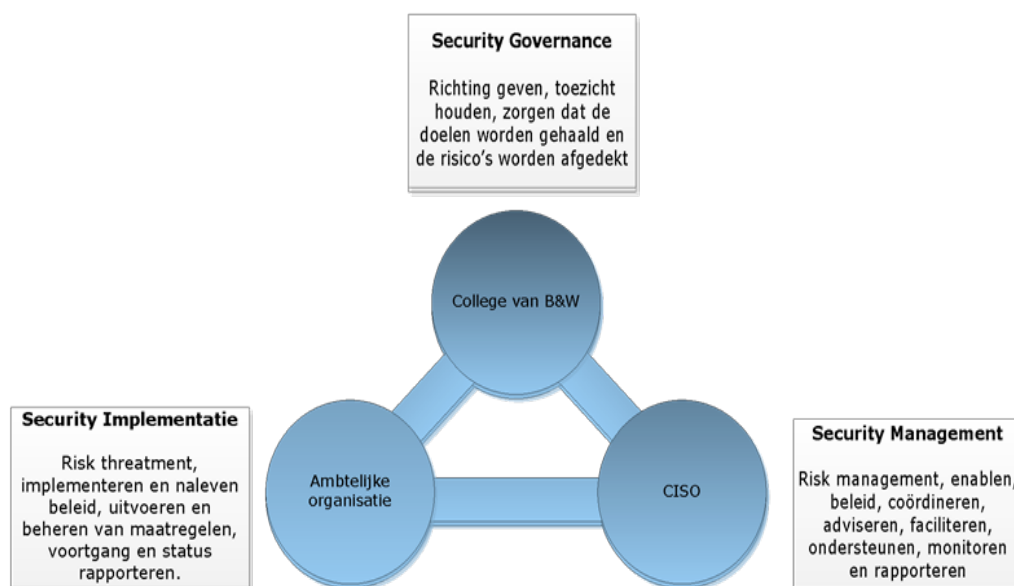
Informatieveiligheid behoort tot de verantwoordelijkheid van alle medewerkers zowel vast als tijdelijk, intern of extern, (keten)partners en andere belanghebbende(n). We gaan daarbij uit van de eigen verantwoordelijkheid voor hun gedrag binnen het vastgestelde beleid, de basisregels en geldende normenkaders. Dit omvat echter altijd:

³ Cloud computing is het via een netwerk – vaak het internet – op aanvraag beschikbaar stellen van hardware, software en gegevens. Oftewel via het internet verbind je met een server die eender waar kan staan, waarna je alle nodige gegevens (data) en software kan bekijken en gebruiken.

1. Dat gegevens (data) en applicaties worden beschermd tegen ongeautoriseerde toegang (naleven informatiebeveiligingsbeleid), gebruik, verandering (manipulatie), openbaring, vernietiging, verlies of overdracht;
2. De plicht om (vermeende) informatiebeveiligingsincidenten, zoals datalekken en inbreuken op de informatiebeveiliging via een melding aan de helpdesk te melden;
3. Het aanspreken van in- en externe medewerkers, (keten)partners en betrokkene(n) op geconstateerd onzorgvuldig gedrag in relatie tot informatieveiligheid.

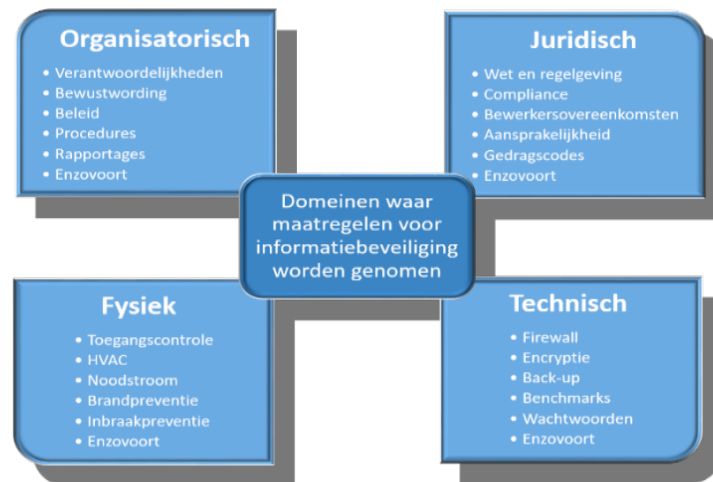
3.6: SCHEMATISCH WEERGAVE VAN DE VERANTWOORDELIJKHEDEN OP HOOFDLIJNEN

Deze verantwoordelijkheden worden hieronder, op hoofdlijnen schematisch weergegeven.



4: DOMEINEN WAAR MAATREGELEN WORDEN GETROFFEN

Om de beschikbaarheid, vertrouwelijkheid en integriteit van de informatievoorziening te waarborgen is het noodzakelijk om een samenhangend pakket van organisatorische, juridische, technische en fysieke informatiebeveiligingsmaatregelen te treffen en te onderhouden. Informatieveiligheid reikt verder dan het implementeren van technische informatiebeveiligingsmaatregelen. Het is een groot misverstand om te denken dat informatiebeveiliging iets technisch is dat centraal geregeld kan of moet worden. Hieronder wordt schematisch weergegeven binnen welke domeinen maatregelen voor informatiebeveiliging worden getroffen en onderhouden. De beschreven maatregelen binnen deze domeinen zijn illustratief en niet limitatief.



5: BELEIDSUITGANGSPUNTEN

Bij het treffen en onderhouden van maatregelen voor de borging van de informatieveiligheid gelden de volgende beleidsuitgangspunten waaraan (vooraf) wordt getoetst:

1. Relevante Europese, landelijke, sectorale wet- en regelgeving en specifieke normenkaders zijn altijd leidend. Denk bij wet- en regelgeving aan de Algemene Verordening Gegevensbescherming (AVG), Wet Basisregistratie Personen (BRP), Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), de archiefwet, enzovoort;
2. De Baseline Informatiebeveiliging Overheid (BIO) wordt gehanteerd als normenkader. De te treffen informatiebeveiligingsmaatregelen worden hieraan (vooraf) getoetst;
3. De te treffen en onderhouden informatiebeveiligingsmaatregelen zijn altijd op een risicoafweging gebaseerd en worden proportioneel getroffen. Deze afweging(en) worden schriftelijk vastgelegd. Een dataclassificatie, Data Protection Impact Assessment⁴ (DPIA) en een risicoanalyse worden daartoe verplicht uitgevoerd;
4. Eventuele (rest) risico's welke niet afgedekt (kunnen) worden met maatregelen of niet proportioneel zijn worden ter acceptatie voorgelegd aan het college van burgemeester en wethouders van de gemeente Ridderkerk;
5. Er is ruimte voor afwijkingen en prioriteringen op basis van het "pas toe of leg uit" principe. Deze afwegingen worden door de proceseigenaar (lijnmanager) schriftelijk vastgelegd, door de Chief Information Security Officer voorzien van een advies en vooraf ter goedkeuring voorgelegd aan de desbetreffende verwerkersverantwoordelijke(n) binnen de gemeente Ridderkerk;
6. Indien van toepassing wordt dit informatiebeveiligingsbeleid verder uitgewerkt c.q. verbijzonderd in onderliggend(e) beleid, informatiebeveiligingsplannen, richtlijnen, procedures, enzovoort. Deze worden getoetst aan de beschikbare operationele producten rondom de Baseline Informatiebeveiliging Overheid;

⁴ Een DPIA is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen en vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.

7. Wanneer wetgeving, regelgeving en/of specifieke normenkaders eisen stellen aan taken en verantwoordelijkheden van medewerkers inzake informatieveiligheid dan worden deze opgenomen in aanvullende individuele afspraken op functieniveau tussen de leidinggevende en de medewerker. Immers in de HR21 normfuncties zijn de werkzaamheden met betrekking tot informatiebeveiliging niet expliciet opgenomen. Deze specifieke werkzaamheden passen niet bij het karakter van een generieke functiebeschrijving waarin de werkzaamheden op hoofdlijnen zijn beschreven;
8. Iedere medewerker, zowel vast als tijdelijk, intern of extern, (keten)partner of betrokkene, is verplicht waar nodig gegevens en applicaties te beschermen tegen ongeautoriseerde toegang (naleven informatiebeveiligingsbeleid), gebruik, verandering (manipulatie), openbaring, vernietiging, verlies of ongeautoriseerde overdracht. Bij (vermeende) inbreuken hierop dienen medewerkers dit te melden bij de helpdesk;
9. We gaan uit van de eigen verantwoordelijkheid van medewerkers zowel vast als tijdelijk, intern of extern en overige betrokkene(n) voor hun gedrag binnen het vastgestelde beleid, de basisregels en geldende normenkaders;
10. Het college van burgemeester en wethouders van de gemeente Ridderkerk, de directieraad van de BAR-organisatie, de directie van de NV BAR-afvalbeheer, de Chief Information Security Officer en proceseigenaar (lijnmanager) bevorderen de naleving van dit informatiebeveiligingsbeleid, de algehele communicatie en bewustwording (awareness) rondom informatieveiligheid.

6: VERPLICHT UIT TE VOEREN STAPPEN

De te treffen en onderhouden informatiebeveiligingsmaatregelen zijn altijd op een risicoafweging gebaseerd en worden proportioneel getroffen. Om de informatiebeveiligingsrisico's in beeld te brengen en daarmee te komen tot een zorgvuldige afweging dienen de hieronder vermelde stappen altijd te worden uitgevoerd. Op basis van deze stappen wordt bepaald wat de te treffen en onderhouden informatiebeveiligingsmaatregelen zijn. Dit wordt schriftelijk vastgelegd.

6.1: HET UITVOEREN VAN EEN DATACLASSIFICATIE (STAP 1)

Het uitvoeren van een dataclassificatie is altijd verplicht. Het toekennen van classificatieniveaus aan data en/of informatiesystemen is van groot belang, omdat daarmee het (vereiste) beschermingsniveau wordt geïdentificeerd. Het vormt de basis voor de basisbeveiligingsniveau-toets (BBN-toets). Het beschermingsniveau van gegevens (data) en/of informatiesystemen wordt uitgedrukt in classificatieniveaus voor beschikbaarheid, integriteit en vertrouwelijkheid. Mede aan de hand hiervan kan worden bepaald welke beveiligingseisen gelden en welke maatregelen moeten worden genomen. De eerste stap bij een dataclassificatie is nagaan welke wetgeving, regelgeving en/of specifieke normenkaders mogelijk eisen stellen aan gebruik, distributie en opslag van data. Daarnaast is het van belang om de verantwoordelijkheden t.a.v. de gegevens (data) en/of informatiesystemen goed in beeld te hebben. Bij het uitvoeren van een dataclassificatie worden de daarvoor beschikbare operationele producten van de IBD inzake de Baseline Informatiebeveiliging Overheid (BIO) geraadpleegd en als leidraad gehanteerd.

6.2: HET UITVOEREN VAN EEN DATA PROTECTION IMPACT ASSESSMENT (STAP 2)

Een Data Protection Impact Assessment (DPIA) is een instrument om vooraf de privacy risico's van een gegevensverwerking in kaart te brengen en om op basis van de geïdentificeerde risico's de te treffen maatregelen te bepalen om deze risico's af te dekken/mitigeren. Het uitvoeren van een Data Protection Impact Assessment (DPIA) is op basis van het beleidsuitgangspunt 3 verplicht en kan in sommige situaties zelfs bij wet⁵ verplicht zijn. Bij het uitvoeren van een DPIA worden de daarvoor beschikbare operationele producten van de IBD inzake de Baseline Informatiebeveiliging Overheid (BIO) geraadpleegd en als leidraad gehanteerd.

6.3: UITVOEREN VAN BBN-TOETS EN (DIEPGAANDE) RISICOANALYSE (STAP 3)

De aanpak van onze informatieveiligheid is risico gebaseerd. Dat wil zeggen dat beveiligingsmaatregelen worden getroffen en onderhouden op basis van een (actuele) risicoanalyse en een basisbeveiligingsniveau-toets (BBN-toets). Wanneer de beschikbaarheid en/of integriteit en/of vertrouwelijkheid, of onderdelen van het informatiesysteem een BBN3-niveau behoeft dan dient een aanvullende diepgaande risicoanalyse te worden uitgevoerd. In de overige situaties vormen de uitgevoerde dataclassificatie (stap 1) en het uitgevoerde Data Protection Impact Assessment (DPIA) (stap 2) te samen de risicoanalyse op basis waarvan de te treffen en onderhouden informatiebeveiligingsmaatregelen worden bepaald. Bij het uitvoeren van de BBN-toets en de diepgaande risicoanalyse worden de daarvoor beschikbare operationele producten van de IBD inzake de Baseline Informatiebeveiliging Overheid (BIO) geraadpleegd en als leidraad gehanteerd.

7: HET DOEL VAN HET INFORMATIEVEILIGHEID

Informatiebeveiliging heeft betrekking op het treffen en onderhouden van een samenhangend pakket van maatregelen teneinde de betrouwbaarheid van de informatievoorziening te waarborgen. De informatievoorziening omvat het geheel van beleid, organisatie, procedures, apparatuur, programmatuur, gegevens en mensen dat betrokken is bij de ontwikkeling, implementatie en instandhouding van de informatiehuishouding. Hierbij wordt onderscheid gemaakt tussen beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid.

7.1: BESCHIKBAARHEID

Beschikbaarheid is het zorgdragen voor het beschikbaar hebben van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor gebruikers. Hierdoor hebben burgers en bedrijven toegang tot voor hen relevante informatie en hebben medewerkers toegang tot relevante informatie om hun werk en de dienstverlening voor onze burgers en bedrijven ongestoord voort te zetten.

7.2: INTEGRITEIT

Integriteit is het waarborgen van de correctheid, volledigheid en tijdigheid (actualiteit) van informatie en informatieverwerking. Voor een efficiënte en effectieve bedrijfsvoering

⁵ Artikel 35 van de Algemene Verordening Gegevensbescherming (AVG)

is het voor de gemeente Ridderkerk van belang dat de correcte informatie tijdig aanwezig is in de informatiesystemen en processen.

7.3: **VERTROUWELIJKHEID**

Vertrouwelijkheid is het beschermen van informatie tegen kennisname, mutatie (manipulatie) en/of verwijderen door onbevoegden. Oftewel informatie is alleen toegankelijk voor degenen die hiertoe zijn geautoriseerd.

7.4: **CONTROLEERBAARHEID**

De mogelijkheid om vast te kunnen stellen of wordt voldaan aan de eisen ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid.

BIJLAGEN

Geen