gemeente Winterswijk

GEMEENTEBLAD

Officiële uitgave van de gemeente Winterswijk

Nr. 181870

20 april

2026

Informatiebeveiligingsbeleid Winterswijk 2025 - 2028

1. Inleiding

Dit beleidsdocument vormt een volledige uitwerking van het informatiebeveiligingsbeleid voor de Gemeente Winterswijk. Het beleid combineert strategische richting met concrete operationele richtlijnen om consistentie, veiligheid en effectiviteit te waarborgen binnen alle lagen van de organisatie. Hierbij wordt gebruik gemaakt van inzichten uit de Baseline Informatiebeveiliging Overheid (BIO) en andere relevante wet- en regelgeving zoals de Algemene verordening gegevensbescherming (AVG) en de Cyberbeveiligingswet (CBW) NIS2-richtlijn. De focus ligt op het versterken van risicomanagement, compliance met wet- en regelgevingen het verhogen van bewustzijn binnen de organisatie. Dit beleid vormt een kader en wordt aangevuld met specifieke tactische beleidsdocumenten en operationele werkinstructies.

1.1 Leeswijzer

Dit document vormt het strategisch informatiebeveiligingsbeleid van de gemeente Winterswijk voor de periode 2025-2028. Het beleid biedt een kader voor informatieveiligheid en geeft richting aan de tactische en operationele uitvoering.

Hoofdstuk 2 beschrijft de beleidsuitgangspunten, waaronder naleving van wet- en regelgeving, risico gebaseerde maatregelen en de rol van de BIO als verplicht normenkader. Dit hoofdstuk vormt de basis voor verdere uitwerking in tactische en operationele plannen.

Hoofdstuk 3 bevat de strategische stappen die verplicht moeten worden uitgevoerd om informatieveiligheidsrisico's te beheersen. Deze stappen omvatten dataclassificatie, risicoanalyses en waar nodig Data Protection Impact Assessments (DPIA's).

Hoofdstuk 4 richt zich op de organisatie van informatieveiligheid binnen de gemeente. Het beschrijft de verantwoordelijkheidsniveaus volgens het Three Lines of Defence-model en bevat een samenvatting van de verantwoordelijkheden van sleutelrollen zoals de gemeentesecretaris, CIO en CISO.

Hoofdstuk 5 behandelt het gebruik van de PDCA-cyclus (Plan-Do-Check-Act) als continu verbetermechanisme om de effectiviteit van informatieveiligheidsmaatregelen te waarborgen.

De uitvoering van dit strategisch beleid wordt jaarlijks vertaald in een Gemeentelijk Informatiebeveiligingsplan (GIB). Het GIB wordt opgesteld op basis van input van de directie, de CISO, dreigingsbeelden van de IBD en de resultaten van ENSIA-audits. Dit plan specificeert de acties en prioriteiten voor het betreffende jaar en biedt flexibiliteit om in te spelen op actuele risico's en ontwikkelingen.

1.2 Ambitie en visie

De gemeente streeft ernaar een betrouwbare partner te zijn voor inwoners en bedrijven. Door een zero trust-aanpak te hanteren, wordt informatie alleen toegankelijk voor geautoriseerde gebruikers op basis van controle en niet op basis van aannames van vertrouwen.

1.3 Doelstelling

Het beleid heeft als doel:

- Informatiebeveiliging te borgen door duidelijke richtlijnen en verantwoordelijkheden te definiëren.
- Risico's proactief te beheren via structurele evaluaties en aanpassingen.
- Naleving van wet- en regelgeving zoals de AVG, BIO en de NIS2-richtlijn (geïmplementeerd via de Cyberbeveiligingswet - CBW) te waarborgen.
- Bewustwording te vergroten door alle medewerkers actief te betrekken.

2. Beleidsuitgangspunten

Dit beleid omvat alle gemeentelijke processen, systemen en informatie, inclusief gegevens van externe partijen en ketenpartners. Specifieke regelgeving voor kritieke systemen wordt in hieronder beschreven. De strategische uitgangspunten voor informatiebeveiliging worden afgestemd op het algemene beveiligingsbeleid en informatievoorzieningsbeleid van de gemeente Winterswijk.

Naleving van wet- en regelgeving

Europese, landelijke en sectorale wet- en regelgeving, evenals specifieke normenkaders, zijn leidend. Denk hierbij aan: de Baseline Informatiebeveiliging Overheid (BIO 2.0), NEN7510, de Network and Information Security Directive (NIS2-richtlijn), de Algemene Verordening Gegevensbescherming (AVG), de Wet Basisregistratie Personen (BRP), de Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), de Wet politiegegevens (Wpg) en de Archiefwet, (zie bijlage 1 voor een overzicht van alle wet- en regelgeving).

NIS2-richtlijn en Cyberbeveiligingswet (CBW):
De CBW operationaliseert de NIS2-richtlijn en stelt specifieke eisen aan essentiële entiteiten zoals gemeenten.

Verplichting BIO: De BIO is via de Cyberbeveiligingswet verplicht voor alle overheden die vallen onder de sector 'Overheid'.

- **Verantwoordelijkheid bestuurder**: Het college van B&W is verantwoordelijk voor:
  - Het zorgdragen van passende en evenredige technische, operationele en organisatorische maatregelen om de risico's te beheren en afgestemd op de risico's die zich voordoen.
  - Het goedkeuren van te nemen maatregelen voor het beheer van cyberbeveiligingsrisico's.
  - Het toezien op de uitvoering en het beheer ervan.

- **Opleiding**: Het college B&W moet opgeleid zijn en kennis hebben om te kunnen sturen op informatiebeveiligingsrisico's. En college B&W moet ervoor zorgen dat ook hun werknemers regelmatig opleiding/training volgen aangaande het onderwerp. Dit betekent dat de opleiding moet voldoen aan de minimale eisen voor de sector 'Overheid' conform de NIS2-richtlijnen.
- **Meldplicht:** Het college B&W zijn verantwoordelijk voor het tijdig melden van incidenten. Overheden moeten binnen de doorlooptijden 24 uur een melding maken van een meldplichtig incident.
- **Toezicht en verantwoording**: De toezichthouder zal toezicht houden op de invulling van de zorgplicht volgens de Cyberbeveiligingswet. De RDI is als toezichthouder aangewezen voor de sector 'Overheid'.

BIO als verplicht normenkader
De gemeente Winterswijk hanteert verplichte overheid specifieke maatregelen en richtlijnen zoals opgenomen in de BIO 2.0. Deze maatregelen zijn leidend bij de implementatie en uitvoering van informatiebeveiliging binnen alle processen en systemen. De beheersmaatregelen die de gemeente toepast, worden geselecteerd op basis van de NEN-ISO/IEC 27002. Waar nodig worden deze maatregelen aangevuld met normen zoals de NEN 7510 of andere relevante richtlijnen.

Algemene Verordening Gegevensbescherming (AVG)
De invoering van de Algemene Verordening Gegevensbescherming (AVG) heeft geleid tot een grotere focus op de bescherming van persoonsgegevens. Het belang van privacy neemt zowel voor de betrokkenen als voor de gemeente steeds meer toe, evenals de impact van privacy schendingen. De AVG vereist het nemen van "passende" organisatorische en technische maatregelen tegen "ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging". Het begrip" passend" impliceert niet alleen dat er een evenwicht moet zijn tussen de beveiligingsmaatregelen en de aard van de te beschermen gegevens, maar ook dat beveiliging niet statisch kan zijn en moet meebewegen met bedreigingen en de stand van de techniek. De gemeentelijke publieke processen in het sociaal domein kennen hier een extra gevoeligheid en risico op reputatieschade.

Privacy beleid
Naast de focus op informatiebeveiliging heeft de gemeente ook een privacy beleid en daaruit voortvloeiende documentatie opgesteld om te voldoen aan de eisen van de AVG. Dit beleid beschrijft de uitgangspunten en maatregelen die de gemeente neemt om de privacy van betrokkenen te waarborgen en persoonsgegevens op een verantwoorde en rechtmatige manier te verwerken.

Wet politiegegevens
Binnen dit beleidskader erkennen wij de bijzondere juridische basis die de Wet politiegegevens (Wpg) biedt voor de verwerking van strafrechtelijke gegevens. Als gemeente zijn wij toegewijd aan het naleven van de Wpg en het waarborgen van de privacy en bescherming van persoonsgegevens in overeenstemming met deze wet. In overeenstemming met de Wpg zullen wij passende maatregelen nemen om de vertrouwelijkheid, integriteit en beschikbaarheid van strafrechtelijke gegevens te waarborgen en ervoor te zorgen dat deze gegevens uitsluitend worden verwerkt voor legitieme doeleinden binnen het kader van de wet.

Forum standaardisatie
Bij aanbestedingen van nieuwe producten en diensten, evenals bij verlenging van bestaande producten en diensten, vraagt de gemeente Winterswijk als overheidsorganisatie naar de relevante open standaar-

den die zijn opgenomen in de 'pas toe of leg uit'-lijst[1] van het Forum Standaardisatie. Deze lijst bevat verplichte standaarden voor de publiekesector, waaronder de normen NEN-ISO/IEC 27001:2022 en NEN-ISO/IEC 27002:2022, die de basis vormen voor de BIO. Als overheidsorganisatie is de gemeente Winterswijk verplicht om te voldoen aan deze standaarden.

DigiD Norm B.01

Integratie van de ICT-beveiligingsrichtlijnen[2] *van het NCSC en de DigiD Norm B.01*[3] *in de Gemeentelijke Webapplicaties*

Als gemeente hebben we de verantwoordelijkheid om de integriteit, vertrouwelijkheid en beschikbaarheid van onze digitale diensten te waarborgen. Deze verantwoordelijkheid strekt zich uit over alle aspecten van onze webapplicaties, inclusief het gebruik van DigiD. We volgen daarom de adviezen op die zijn opgenomen in de ICT-beveiligingsrichtlijnen voor webapplicaties van het Nationaal Cyber Security Centrum (NCSC) en we voldoen aan de DigiD Norm B.01, vastgesteld door de beheerorganisatie van DigiD. Toepassing en Implementatie Gemeente Winterswijk streeft ernaar om de adviezen van de NCSC ICT-beveiligingsrichtlijnen op te volgen en zal de eisen van de DigiD Norm B.01 toe passen in haar gemeentelijke webapplicaties. Dit geldt voor alle fasen, van de selectie van applicaties, de configuratie, de implementatie tot het doorlopend onderhoud ervan. Het personeel wordt getraind en ondersteund om te zorgen voor naleving van deze richtlijnen en normen bij het werken met externe leveranciers en bij het beheer van de webapplicaties.

Bewaking en herziening
Gemeente Winterswijk zal regelmatig de procedures en prestaties evalueren om ervoor te zorgen dat ze in lijn blijven met de adviezen van de NCSC ICT-beveiligingsrichtlijnen en voldoen aan de DigiD Norm B.01. Eventuele afwijkingen of lacunes zullen worden geïdentificeerd en worden gecorrigeerd. We streven ernaar om de veiligheidsnormen voortdurend te verbeteren in lijn met deze richtlijnen en norm.

Verantwoordelijkheid en aansprakelijkheid
De verantwoordelijkheid voor het volgen van de adviezen van de NCSC ICT-beveiligingsrichtlijnen en het naleven van de DigiD Norm B.01 ligt bij iedereen die betrokken is bij het selecteren, implementerenen het beheren van de webapplicaties. We streven ernaar een cultuur van beveiligingsbewustzijn en integriteit te bevorderen, zowel binnen de gemeente als in de interacties met externe leveranciers.

Risicogebaseerde maatregelen
Alle maatregelen worden gebaseerd op een risicoafweging en proportioneel toegepast. Deze afweging wordt schriftelijk vastgelegd.

- Dataclassificatie is verplicht.
- Indien wettelijk vereist, wordt een Data Protection Impact Assessment (DPIA) uitgevoerd.
- Elke informatiestroom en systeem heeft een toegewezen eigenaar die verantwoordelijk is voor de naleving en beveiliging ervan.
- Informatiesystemen en processen worden ontworpen om essentiële functies te garanderen, ook tijdens incidenten of storingen.

Beoordeling en acceptatie van risico's
Rest- en restrisico’s die niet volledig kunnen worden afgedekt of niet proportioneel zijn, worden door de Chief Information Security Officer (CISO) beoordeeld en voorzien van advies. Acceptatie vindt plaats op een directieniveau.

Zero trust en multi-factor authenticatie (MFA)
Toegang vanuit een onvertrouwde naar een vertrouwde zone is uitsluitend toegestaan op basis van een zero trust-aanpak en gebruik van multi-factor authenticatie. [9.4.2.1] [6.2.1.1]

Afwijkingen en prioritering
Afwijkingen en prioriteringen worden toegestaan onder het “pas toe of leg uit”-principe. Deze beslissingen worden door de proceseigenaar schriftelijk vastgelegd, voorzien van advies door de CISO en ter goedkeuring voorgelegd aan het directieniveau.

Beveiligingsbewustzijn

1) https://www.forumstandaardisatie.nl/open-standaarden/verplicht
2) https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties
3) https://www.logius.nl/domeinen/toegang/digid/ict-beveiligingsassessments-digid/documentatie/norm-ict-beveiligingsassessments-digid

De gemeente bevordert beveiligingsbewustzijn op alle niveaus door middel van periodieke training, communicatie en evaluatie van beveiligingsgedrag binnen de organisatie.

Uitwerking van beleid
Het strategisch beleid wordt vertaald naar praktische procedures en richtlijnen die voldoen aan de verplichte normen en maatregelen uit de BIO 2.0. Deze implementatie wordt ondersteund door het gebruik van de NEN-ISO/IEC 27002 als referentiekader.

2.1 Van beleid naar uitvoering
Deze normenkaders worden vertaald naar praktische procedures en richtlijnen om de naleving en implementatie binnen alle gemeentelijke processen te waarborgen. De gemeente hanteert gemeenschappelijke betrouwbaarheidseisen gebaseerd op beschikbaarheid, integriteit en vertrouwelijkheid, afgestemd op de BIO 2.0 en NEN-ISO/IEC 27001.

Deze BIO stelt normen voor de volgende onderwerpen:
- Informatiebeveiligingsbeleid;
- Organiseren van informatiebeveiliging;
- Veilig personeel;
- Beheer van bedrijfsmiddelen;
- Toegangsbeveiliging;
- Cryptografie;
- Fysieke beveiliging en beveiliging van de omgeving;
- Beveiliging bedrijfsvoering;
- Communicatiebeveiliging;
- Acquisitie, ontwikkeling en onderhoud van informatiesystemen;
- Leveranciersrelaties;
- Beheer van informatiebeveiligingsincidenten;
- IB-aspecten van bedrijfscontinuïteitsbeheer;
- Naleving.

3. Verplicht uit te voeren stappen

Het vaststellen en onderhouden van informatiebeveiligingsmaatregelen is altijd gebaseerd op een zorgvuldige risicoafweging en wordt proportioneel uitgevoerd. Om informatiebeveiligingsrisico's in kaart te brengen en weloverwogen beslissingen te nemen over passende maatregelen, dienen de onderstaande stappen altijd te worden doorlopen. De gemaakte afwegingen en genomen maatregelen worden schriftelijk vastgelegd voor verantwoording en naleving.

3.1 Dataclassificatie
Alle gegevens en systemen worden geclassificeerd op basis van beschikbaarheid, integriteit en vertrouwelijkheid. Deze classificatie vormt de basis voor het vaststellen van het Basisbeveiligingsniveau (BBN).

3.2 Risicoanalyse
Bij verhoogde beveiligingseisen (vanaf BBN2) worden aanvullende risicoanalyses uitgevoerd om passende maatregelen te identificeren. Deze analyses helpen om kwetsbaarheden te minimaliseren en beveiliging proportioneel te implementeren.

3.3 Privacy-impactbeoordeling (DPIA)
Waar wettelijk vereist, worden DPIA's uitgevoerd om de privacyrisico's van gegevensverwerking vooraf in kaart te brengen. Dit waarborgt naleving van de AVG en andere privacyregelgeving.

3.4 Statement of Applicability (SoA):
Bij het vaststellen van beheersmaatregelen stelt de gemeente een verklaring van toepasselijkheid (SoA) op, waarin wordt vastgelegd welke maatregelen worden toegepast en waarom. Deze verklaring vormt een belangrijk document voor transparantie en naleving van de BIO 2.0.

3.5 ISMS-processen:
De gemeente implementeert en onderhoudt een managementsysteem voor informatiebeveiliging (ISMS) dat voldoet aan de NEN-ISO/IEC 27001. Dit omvat het bepalen van de scope, het uitvoeren van risicoanalyses, en het continu verbeteren van beveiligingsmaatregelen.

4. Organisatie, taken en verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot de informatiebeveiliging op welke plaats belegd zijn binnen gemeente Winterswijk. Eigenaarschap van bedrijfsprocessen en informatieprocessen/systemen benoemen en verantwoordelijkheden vaststellen [8.1.2].

Resultaat: Verankering van verantwoordelijkheden, taakomschrijvingen en coördinatie- en rapportagemechanismen voor informatiebeveiliging in de gemeentelijke organisatie.

Het volgt de bekende methode van de Three Lines of Defence (3LoD) in de bedrijfsvoering. In dit model is het lijnmanagement de eerste lijn, verantwoordelijk voor de eigen processen, inclusief informatiebeveiliging. De tweede lijn (CISO, security officers) ondersteunt, adviseert, coördineert en controleert of het managementteam hun verantwoordelijkheden nakomt. De derde lijn voorziet het geheel van een objectief oordeel en mogelijkheden tot verbetering via een interne auditor. In sommige gevallen kan er nog een vierde lijn worden toegevoegd in de vorm van een externe audit, die op bepaalde aspecten verplicht is.

4.1 Verantwoordelijkheidsniveaus binnen de gemeente Winterswijk

Binnen de gemeente Winterswijk worden, in overeenstemming met de geldende wet- en regelgeving, de volgende verantwoordelijkheids- en takenniveaus onderscheiden met betrekking tot informatiebeveiliging [6.1.1.2].

4.1.1 Controle en toetsing door de gemeenteraad

De gemeenteraad heeft een specifieke bevoegdheid om het beleid en de werking ervan binnen de gemeente Winterswijk te controleren en te toetsen, inclusief informatiebeveiliging. Het college B&W stelt het informatiebeveiligingsbeleid vast. Het college legt jaarlijks verantwoording af aan de gemeenteraad over de stand van zaken van informatiebeveiliging, in lijn met de P&C-cyclus. Dit gebeurt via een collegeverklaring waarop een auditor Assurance afgeeft en in het jaarverslag met een passage over informatiebeveiliging in de paragraaf bedrijfsvoering [18.2.2.1].

4.1.2 Conformering van de griffie aan dit beleid

Als apart orgaan binnen de ambtelijke organisatie is de griffie verantwoordelijk voor de eigen processen, systemen en gegevens, inclusief de staat van informatiebeveiliging binnen deze processen. De griffie conformeert zich aan het informatiebeveiligingsbeleid en hanteert hetzelfde kader als de ambtelijke organisatie.

4.1.3 Beleidsbepalende, regisserende en coördinerende verantwoordelijkheden op organisatieniveau

Als eigenaar van gemeentelijke informatieprocessen en -systemen draagt het college de eindverantwoordelijkheid voor een passend niveau van informatiebeveiliging. Het college stelt met het voorliggende beleidsdocument de kaders voor informatiebeveiliging vast op basis van landelijke en Europese wet- en regelgeving. De gemeenteraad wordt geïnformeerd over de informatiebeveiliging van de gemeente via P&C-cyclus. Hierin worden de stand van zaken, uitgevoerde plannen van het afgelopen jaar, de tijdsplanning en plannen voor het volgende jaar gepresenteerd. Bovendien wordt de CISO aangesteld door het college, op basis van een vastgesteld functieprofiel [6.1.1.2; 6.1.1.3; 6.1.1.4].

4.1.4 Verantwoordelijkheden en taken op organisatieniveau

Gemeentesecretaris

De gemeentesecretaris is eindverantwoordelijk voor de borging van informatieveiligheid binnen de gemeente en heeft de volgende verantwoordelijkheden:

- Het stellen van **strategische en operationele kaders** en het geven van sturing aan informatiebeveiliging.
- Het beheren en beheersen van i**nformatiebeveiligingsrisico's** binnen de gemeente.
- Het **periodiek evalueren en bijstellen** van het beleid om te voldoen aan veranderende wet- en regelgeving of risico's.
- Het **controleren van beveiligingsmaatregelen** om te waarborgen dat deze voldoen aan betrouwbaarheidseisen en voldoende bescherming bieden.
- Het toewijzen van **verantwoordelijkheden** voor specifieke informatiebeveiligingscomponenten en -systemen.
- Het scheiden van **uitvoerende, controlerende en beleidsbepalende taken** op het gebied van informatiebeveiliging om fraude en fouten te voorkomen.

Chief Information Officer (CIO)

De CIO is verantwoordelijk voor de algehele informatievoorziening binnen de gemeente. Dit omvat:

- Het zorgen dat de strategische doelen op het gebied van informatiebeveiliging en -voorziening worden gerealiseerd.
- Het afstemmen van informatiebeleid op de bredere organisatorische doelen.
- Het waarborgen van de integratie van informatiebeveiliging binnen de gemeentelijke informatievoorziening.
- **Het ontwikkelen en beheren van het Business Continuity Plan (BCP):** Het BCP richt zich op het waarborgen van de continuïteit van kritieke processen en systemen tijdens verstoringen of calamiteiten. Hierbij houdt de CIO toezicht op:
  - Identificatie en prioritering van kritieke bedrijfsprocessen en afhankelijkheden.
  - Samenwerking met de CISO en lijnmanagers om risico's en beveiligingsmaatregelen te integreren in het continuïteitsplan.
  - Periodieke evaluatie, testen en actualisatie van het BCP.

Chief Information Security Officer (CISO)
De CISO voert namens het college activiteiten uit op het gebied van informatiebeveiliging en is verantwoordelijk voor de volgende taken [8.1.2]:

- **Beveiligingsniveau bepalen:** De gemeentesecretaris besluit het niveau en het directieteam stelt het gewenste niveau van informatiebeveiliging vast.
- **Beveiligingseisen per bedrijfsproces:** Het vaststellen van beveiligingseisen voor specifieke bedrijfsprocessen en informatiesystemen.
- **Implementatie van beveiligingsmaatregelen:** Zorgen voor de juiste implementatie van beveiligingsmaatregelen in interne en externe (informatie)systemen.
- **Toezicht en rapportage:** Het bewaken van de naleving van het informatiebeveiligingsbeleid en het rapporteren aan de gemeentesecretaris en het college.
- **Aansturing van systeemeigenaren:** Voor elk informatiesysteem wordt door de gemeentesecretaris een procesverantwoordelijke of systeemeigenaar aangesteld. De CISO coördineert dat deze personen voldoen aan de eisen die voortvloeien uit het beleid en de relevante wetgeving.

Overzicht van Verantwoordelijkheden

Rol	Hoofdverantwoordelijkheden
Gemeentesecretaris	Strategisch beleid, risico's beheren, beveiligingskaders stellen, eindverantwoordelijkheid.
Adjunct Gemeentesecretaris	Continuïteit waarborgen bij afwezigheid van de gemeentesecretaris.
CIO	Algehele informatievoorziening en integratie van informatiebeveiliging in gemeentelijke processen.
CISO	Implementatie, toezicht en advisering over informatiebeveiligingsmaatregelen.

4.1.5 Verantwoordelijkheden en taken op eenheidsniveau

De domeinmanagers en de griffier (proceseigenaren) zijn eigenaar van en integraal verantwoordelijk voor de (informatie)beveiliging van de informatieprocessen en -systemen binnen hun organisatieonderdeel.

De domeinmanagers en griffier hebben onder andere de volgende **verantwoordelijkheden**:

- Het borgen van de verantwoordelijkheid voor het classificeren van opgeslagen data in applicaties en gegevensverzamelingen, waarbij de uitvoering kan worden gedelegeerd.
- Verantwoordelijk voor het vaststellen van betrouwbaarheidseisen voor de afdelingsinformatiesystemen, met de mogelijkheid om de uitwerking te laten uitvoeren door bevoegde medewerkers.
- Verantwoordelijk voor het aansturen en goedkeuren van de keuze, implementatie en communicatie van maatregelen die voortvloeien uit de betrouwbaarheidseisen.
- Het dragen van de verantwoordelijkheid voor het laten uitvoeren van risicoscans voor informatiebeveiliging, ter ondersteuning van risicoafwegingen.
- Verantwoordelijk voor het realiseren en waarborgen van informatiebeveiliging binnen de processen waarvoor zij verantwoordelijk zijn, inclusief uitbestede delen en samenwerkingsverbanden, met de mogelijkheid om taken te delegeren.
- Verantwoordelijk voor het stimuleren van bewustwording bij medewerkers over hun verantwoordelijkheid voor informatiebeveiliging in hun dagelijkse werkprocessen.
- Het bevorderen van beveiligingsbewustzijn, bedrijfscontinuïteit en naleving van regels en richtlijnen, door het aansturen en faciliteren van relevante initiatieven.

- Verantwoordelijk voor het laten coördineren van de afhandeling van beveiligingsincidenten die de betrouwbaarheid, beschikbaarheid of vertrouwelijkheid van de informatievoorziening verstoren [16.1.2.5].
- Verantwoordelijk voor het vaststellen van relevante wettelijke, statutaire, regelgevende en contractuele eisen, en voor het aansturen van de implementatie van de benodigde aanpak om aan deze eisen te voldoen voor elk informatiesysteem en de organisatie [18.1.1].
- Verantwoordelijk voor het waarborgen van privacy en bescherming van persoonsgegevens conform de relevante wet- en regelgeving [18.1.4], waarbij de uitvoering kan worden gedelegeerd.
- Verantwoordelijk voor het toezien op de controle van het verwerken van persoonsgegevens om vast te stellen dat alleen geautoriseerde medewerkers de juiste persoonsgegevens hebben ingezien en verwerkt.
- Verantwoordelijk voor het opdracht geven aan en het toezien op periodieke beveiligingsaudits.
- Verantwoordelijk voor het waarborgen van rapportages, via de CISO, over de naleving van wet- en regelgeving en het algemene beleid van de gemeente met betrekking tot informatiebeveiliging in de Planning & Control-rapportages.
- Lijnmanagers zijn verantwoordelijk voor de continuïteit van taakuitvoering (BCM) binnen hun processen en systemen, inclusief de samenhang met ketens van informatiesystemen, waarbij de uitvoering kan worden belegd bij bevoegde medewerkers.

4.1.6 Chief Information Security Officer (CISO)

Een Chief Information Security Officer (CISO) is aangewezen door het college op basis van een vastgesteld profiel [6.1.1.2; 6.1.1.3; 6.1.1.4]. In deze rol is de CISO namens de directie verantwoordelijk voor het actueel houden van het informatieveiligheidsbeleid op strategisch en organisatieniveau. De CISO coördineert de uitvoering van het beleid, beheerst risico's volgens de behoeften van de gemeente en rapporteert aan het college en directie.

De taken en verantwoordelijkheden van de CISO omvatten het volgende:

- Direct rapporteren aan de gemeentesecretaris en de portefeuillehouder.
- Coördineren van de ontwikkeling van het informatiebeveiligingsbeleid.
- Coördineren van de uitvoering van de informatiebeveiligingsanalyse en zorgen voor regelmatige updates.
- Prioriteren van informatiebeveiligingsmaatregelen op basis van de informatiebeveiligingsanalyse en leiden van de uitvoering van het actieplan informatiebeveiliging.
- Bewaken van de uitvoering van het actieplan informatiebeveiliging en naleving van het beleid.
- Opstellen van een plan voor overleg en rapportage met betrekking tot informatiebeveiliging.
- Ondersteunen van de gemeentesecretaris, de adjunct gemeentesecretaris en het managementteam met kennis over informatiebeveiliging, zodat zij hun verantwoordelijkheid voor de betrouwbaarheid van de informatievoorziening kunnen vervullen.
- Fungeren als aanspreekpunt voor medewerkers van de gemeente Winterswijk met vragen over informatiebeveiliging.
- Volgen van externe invloeden die van invloed zijn op het informatiebeveiligingsbeleid en de informatiebeveiligingsanalyse.
- Geven van gevraagd en ongevraagd advies over informatiebeveiliging aan de gehele organisatie.
- Bevorderen van het bewustzijn van beveiliging binnen de organisatie.
- Ondersteunen van het college bij het opstellen van de rapportage over informatiebeveiliging van de gemeente in het jaarverslag.
- Onderhouden van contacten met relevante overheidsinstanties.
- Ondersteunen van de organisatie vanuit een onafhankelijke centrale positie bij het bewaken en verbeteren van de betrouwbaarheid van de informatievoorzieningen hierover rechtstreeks rapporteren aan het directieteam vóór de P&C-gesprekken.
- De CISO rapporteert bevindingen aan het college en directie.
- Waarborgt dat de juiste maatregelen en processen worden geïmplementeerd om te voldoen aan de ENSIA-normen.

4.1.7 Information Security Officer (ISO)

De CISO wordt ondersteund door de Information Security Officer (ISO). Deze rol heeft op tactisch niveau de verantwoordelijkheid voor het up-to-date houden van het informatieveiligheidsbeleid, het coördineren van de uitvoering ervan, het verstrekken van advies bij projecten.

De taken en verantwoordelijkheden van de ISO omvatten het volgende:

- *Periodieke toetsing van de juiste naleving, werking, effectiviteit en kwaliteit van de maatregelen met betrekking tot informatiebeveiliging, in samenwerking met de beveiligingsbeheerders.*

- *Controle van de voortgang van de uitvoering van maatregelen uit de informatiebeveiligingsanalyse en het actieplan informatiebeveiliging.*
- *Toezicht houden op de periodieke actualisatie van het informatiebeveiligingsbeleid en de informatiebeveiligingsanalyse.*
- *Bewaking van het niveau van informatiebeveiliging.*
- *Toetsing van het evaluatieproces van beveiligingsincidenten.*
- *Rapportage van bevindingen aan de ISO.*
- *Uitvoering van operationele activiteiten met betrekking tot informatiebeveiliging, zoals het implementeren en monitoren van beveiligingsmaatregelen.*
- *Het ontwikkelen en onderhouden van informatiebeveiligingsbeleid, procedures en richtlijnen.*
- *Identificeren van kwetsbaarheden en risico's op operationeel niveau en het implementeren van passende maatregelen.*
- *Rapportage van informatiebeveiligingsincidenten en het coördineren van de respons en de afhandeling ervan.*
- *Het bevorderen van bewustzijn en training van medewerkers over informatiebeveiliging.*
- *Bijhouden van een register van informatiebeveiligingsincidenten en verantwoordelijkheid dragen voor de juiste afhandeling en evaluatie ervan.*
- *De ISO heeft de operationele verantwoordelijkheid voor de uitvoering van de ENSIA-audit en coördineert de auditactiviteiten, verzamelt relevante informatie en werkt samen met interne en externe auditors.*
- *Zorgt ervoor dat de vereiste documentatie en bewijsmaterialen worden verzameld.*

4.1.8 Beveiligingsfunctionaris

De rol van Beveiligingsfunctionaris omvat het beheer, de coördinatie en het advies met betrekking tot informatiebeveiliging binnen een specifiek deelgebied. In dit beleidsdocument worden verschillende benamingen gegeven aan rollen die veelal dezelfde taken en verantwoordelijkheden hebben met betrekking tot specifieke gegevensverzamelingen. Om duidelijkheid te scheppen in de naamgeving, wordt in dit beleidsdocument de verantwoordelijkheid voor beveiliging met betrekking tot een specifieke gegevensverzameling toegewezen aan de Beveiligingsfunctionaris.

Specifiek verplichte beveiligingsfunctionarisrollen:

- Autorisatiebevoegde Reisdocumenten/Aanvraagstations: verantwoordelijk voor het beheer van de autorisaties (het toekennen van rechten in informatiesystemen aan personen of groepen) voor de reisdocumentenmodules (RAAS en aanvraagstations).
- Autorisatiebevoegde Rijbewijzen: verantwoordelijk voor het beheer van de autorisaties voor rijbewijzen, inclusief aanmelding bij de RDW.
- Daarnaast worden, indien mogelijk, Beveiligingsfunctionarissen aangewezen voor verschillende aspecten van de gemeentelijke bedrijfsvoering (zoals facilitaire zaken, DIV (archivering) en personeelszaken), evenals de primaire processen (bijvoorbeeld sociaal domein, financiën, beveiliging, handhaving, publieksdiensten (eventueel gecombineerd met BRP en waarde documenten), ruimte/omgeving).

4.1.9. Technical Information Security Officer

De TISO is verantwoordelijk voor de technische aspecten van informatiebeveiliging binnen gemeente Winterswijk waaronder het beoordelen, bewaken, inrichten en implementeren van de informatieveiligheid en fungeert als verbindende factor tussen de CISO en de beheerorganisatie op het gebied van informatieveiligheid. Bovendien speelt de TISO een belangrijke rol bij het coördineren van uitwijk, backup en penetratietesten, het beoordelen van nieuwe initiatieven en wijzigingen op het gebied van technische veiligheid.

De taken en verantwoordelijkheden van de TISO omvatten onder andere het volgende:

- *Beoordelen, bewaken, inrichten en implementeren van de architectuur op informatieveiligheid.*
- *Coördineren en prioriteren van te nemen maatregelen die voortvloeien uit security incidenten.*
- *Rapporteert aan de CISO en CIO.*
- *(Mede) opstellen van informatieveiligheidsbeleid, ICT-richtlijnen, beveiligingsplannen en het toetsen en inrichten hiervan.*
- *Uitvoeren van risico- en kwetsbaarheid analyses op de techniek en/of processen en implementatie van verbeteringen hierop.*
- *Beheer van het technisch continuïteitsmanagement, waaronder de coördinatie van uitwijk, backup en penetratietesten.*
- *Vertegenwoordiging van de technische aspecten bij externe (IT) audit.*

4.1.10 Functionaris Gegevensbescherming (FG)

De Functionaris voor Gegevensbescherming (FG) is de interne toezichthouder op de verwerking van persoonsgegevens binnen de gemeente, in overeenstemming met de Algemene Verordening Gegevensbescherming (AVG). [18.1.4.1]

De FG heeft de volgende wettelijke taken (art. 39 lid 1 AVG), aangepast aan de situatie binnen de gemeente:

- Informeren en adviseren van de gemeenteraad, het college, het directieteam, het managementteam en de medewerkers over hun verplichtingen met betrekking tot gegevensbescherming.
- Toezien op de naleving van zowel de AVG als andere wetten met betrekking tot gegevensbescherming, evenals het beleid met betrekking tot de bescherming van persoonsgegevens van de verwerkingsverantwoordelijke of de verwerker. Dit omvat het bewustmaken en opleiden van het personeel dat betrokken is bij de verwerking en het uitvoeren van audits.
- Toezicht houden op de registratie van beveiligingsincidenten waarbij persoonsgegevens betrokken zijn en toezicht houden op het melden van datalekken bij de Autoriteit Persoonsgegevens en betrokkenen.
- Samenwerken met en fungeren als contactpunt voor de Autoriteit Persoonsgegevens.
- Rekening houden met risico's in relatie tot de aard, omvang en context van de verwerking van persoonsgegevens.
- Fungeren als contactpersoon binnen de organisatie.
- Rapporteren aan de hoogste leidinggevende van de verwerkingsverantwoordelijke, meestal het college of de burgemeester en in sommige gevallen de gemeenteraad.
- De FG heeft een toezichthoudende en adviserende taak op het gebied van privacy.

4.1.11 Privacy Officer (PO)

Deze functie is gericht op de uitvoering en naleving van de Algemene Verordening Gegevensbescherming (AVG). Daarnaast adviseert de medewerker over privacybescherming en activiteiten ter bescherming van persoonsgegevens.

De Privacy Officer heeft de volgende verantwoordelijkheden:

- Beoordelen van de verwerking van persoonsgegevens in overeenstemming met de privacywetgeving. Advies verstrekken aan het directieteam en managementteam bij wijzigingen in procesuitvoering, bedrijfsvoering en de toepassing van een data protection impact assessment (DPIA).
- Als adviserend lid deelnemen aan programma's en projecten die mogelijk invloed hebben op de verwerking van persoonsgegevens.
- Uitleg geven over de privacy voorschriften in de AVG en sectorale wetgeving.
- Coördineren van privacy werkzaamheden, inclusief het informeren en melden bij de Functionaris voor Gegevensbescherming (FG).
- Coördineren, samenvoegen en openbaar maken van overzichten van gegevensverwerkingen van de verschillende organisatieonderdelen binnen de gemeente.
- Coördineren van verzoeken met betrekking tot inzage, correctie en verzet met betrekking tot persoonsgegevens en adviseren over de afhandeling ervan.
- Rapporteren aan het directieteam.
- Ontwikkelen van procedures voor de afhandeling van datalekken waarbij persoonsgegevens betrokken zijn.
- Beheer en onderhoud van standaarddocumenten voor verwerkersovereenkomsten, convenanten en reglementen.
- Adviseren en ondersteunen bij het besluitvormingsproces en het afsluiten van verwerkersovereenkomsten, convenanten en de vaststelling van reglementen.

4.1.12 Applicatiebeheer

Het beheer van applicaties is een belangrijk aspect in de beveiliging van gemeentelijke informatie, zowel op functioneel als technisch gebied. Het gebruik van applicaties blijft toenemen en in de loop der tijd is er binnen de gemeente een diversiteit aan vak- en back-officeapplicaties ontstaan. Het configureren, beveiligen (updates/patches), toegangsbeheer en algemeen beheer van deze applicaties zijn enkele aspecten die bij een gestructureerde uitvoering de risico's kunnen verminderen.

Functioneel applicatiebeheer omvat taken zoals:

- Analyseren van functionele behoeften.
- Configureren en aanpassen van applicaties.
- Bieden van gebruikersondersteuning.

- Uitvoeren van functionele tests en kwaliteitsborging.
- Technisch applicatiebeheer omvat taken zoals:
- Installeren en configureren van applicaties.
- Zorgen voor beveiliging en updates.
- Optimaliseren van applicatieprestaties.
- Oplossen van technische problemen.
- Functioneel en technisch applicatiebeheer werken samen om applicaties goed te laten functioneren en te voldoen aan de behoeften van de gebruikers en de organisatie.

4.1.13 De medewerkers

Medewerkers zijn verantwoordelijk voor de beveiliging van hun functie en taken. Ze hanteren zorgvuldigheid en discipline bij het omgaan met informatie en systemen. Ze begrijpen de eisen voor betrouwbaarheid, integriteit, beschikbaarheid en
controleerbaarheid van de informatieprocessen waaraan ze deelnemen. Het tactisch informatiebeveiligingsbeleid bevat gedragsregels die medewerkers dienen te kennen en te volgen in hun functie.

5. Informatiebeveiliging in de PDCA-cyclus

5.1 Plan

In de planningsfase formuleren verantwoordelijke functionarissen het informatiebeveiligingsbeleid en richten ze de beveiligingsorganisatie in. Het beleid is zoals eerder beschreven gebaseerd op verschillende bronnen, zoals wet- en regelgeving, de missie en visie van de gemeente Winterswijk. De BIO, externe factoren, best practices, risico beoordelingen en auditresultaten. Het informatiebeveiligingsbeleid en eventuele wijzigingen wordt vastgesteld door het college. Het beleid bestaat uit richtlijnen en een basisniveau van beveiliging. Elk jaar worden in het jaarplan van de directies speerpunten voor informatiebeveiliging opgenomen, die worden vertaald naar concrete acties. De CISO adviseert de gemeente om deze speerpunten en acties te realiseren.

ISMS als strategisch fundament:
Het informatiebeveiligingsbeleid is onderdeel van een breder managementsysteem voor informatiebeveiliging (ISMS), dat is opgezet conform de NEN-ISO/IEC 27001. Het ISMS vormt het strategisch fundament voor het continu beheren, verbeteren en monitoren van informatieveiligheid binnen de gemeente.

Strategisch kader voor continuïteit
Continuïteitsbeheer vormt een integraal onderdeel van het strategische informatiebeveiligingsbeleid. Het beleid stelt dat:

- De gemeente robuuste maatregelen treft om de continuïteit van kritieke processen en informatiesystemen te waarborgen.
- Risico’s op uitval en verstoring systematisch worden geanalyseerd en geprioriteerd.
- Periodieke evaluaties en tests worden uitgevoerd om de effectiviteit van de continuïteitsmaatregelen te waarborgen.

De verantwoordelijkheid voor de strategische aansturing van continuïteitsbeheer ligt bij de CIO, met input van de CISO voor risico-inschattingen. Resultaten van evaluaties worden opgenomen in de jaarlijkse rapportage aan de gemeenteraad.

5.2 Do

Om risico's met betrekking tot informatiebeveiliging te verminderen en het basisniveau van beveiliging te implementeren, kiest de gemeente Winterswijk de volgende aanpak: het nemen van risicogebaseerde maatregelen om te voldoen aan het basisniveau van beveiliging. Minstens één keer per jaar, of bij belangrijke veranderingen in bedrijfsprocessen of informatiesystemen, voeren de CISO, ISO en TISO risicoanalyses uit binnen de aangewezen beveiligingsdomeinen. In overleg met de lijnmanagers bepalen zij op basis van deze risico's de prioriteiten en beslissen ze welke maatregelen gedurende het jaar geïmplementeerd moeten worden. De lijnmanagers stellen hiervoor de benodigde middelen en personeel beschikbaar.

De te nemen maatregelen kunnen afkomstig zijn van het basisniveau van beveiliging of zelfstandig bepaald worden. Daarnaast wordt op basis van de risicoanalyse het basisniveau van beveiliging bepaald voor elk proces of informatiesysteem. De CISO geeft inzicht in de reeds geïmplementeerde maatregelen van het basisniveau en geeft aan waar het gewenste beveiligingsniveau nog niet wordt bereikt. In samenwerking met de directie wordt bepaald hoe het basisniveau van beveiliging bereikt kan worden. Afwijkingen worden centraal geregistreerd in het Information Security Management System (ISMS) en gerapporteerd aan de directie. Naast het verminderen van risico's door het implementeren van maatregelen, is het ook belangrijk om incidenten goed te beheren. Medewerkers kunnen security incidenten

melden volgens bestaande procedures, de CISO rapporteert periodiek over de opgetreden security incidenten aan de directie.

Uitvoering van ISMS-processen:
Bij het implementeren van maatregelen wordt het ISMS gebruikt als leidend mechanisme. Dit omvat processen zoals het vaststellen van de scope van het ISMS, het uitvoeren van risicoanalyses, en het bewaken van de implementatie en effectiviteit van maatregelen.

5.3 Check
Het informatiebeveiligingsproces is niet compleet zonder controle op de naleving van het beleid en de richtlijnen. Binnen de gemeente Winterswijk wordt een drielaags-model gehanteerd om de effectiviteit van beveiligingsmaatregelen te beoordelen:

Directie: De CISO is verantwoordelijk voor de werking van geïmplementeerde maatregelen. De CISO rapporteert de directie over de effectiviteit van genomen maatregelen.

Interne controle, eventueel aangevuld met externe expertise: Naast de controle door de CISO worden onafhankelijke interne audits uitgevoerd door interne controllers of beveiligingsfunctionarissen, mogelijk met ondersteuning van een externe partij. De bevindingen worden via de directeur gerapporteerd aan het college.

Externe accountant: Naast de interne controle beoordeelt een externe accountant jaarlijks bepaalde aandachtsgebieden binnen het informatiebeveiligingsdomein. De bevindingen worden via de directeur gerapporteerd aan het college.

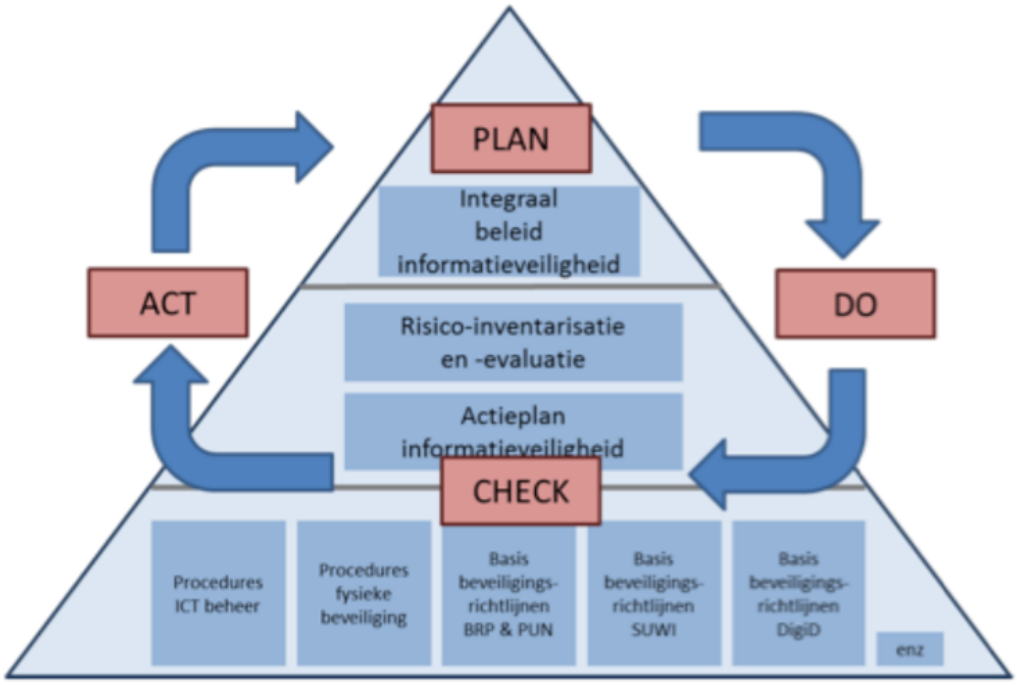
Monitoring van ISMS-prestaties:
Het ISMS wordt gemonitord door het regelmatig evalueren van prestaties via interne en externe audits. De resultaten worden gebruikt om verbeterpunten te identificeren en de effectiviteit van de maatregelen te waarborgen.

Risicoanalyses en meldingen van incidenten worden periodiek beoordeeld om de voortgang van het ISMS te monitoren en bij te sturen waar nodig.

5.4 Act
Het informatiebeveiligingsbeleid wordt minimaal één keer per twee jaar geëvalueerd en indien nodig bijgesteld om te blijven voldoen aan wet- en regelgeving en veranderende risico's. Op basis van de evaluatie bepaalt de CISO samen met de lijnmanagers de vervolgacties.

Continu verbeteren via ISMS:
De evaluatieresultaten van het ISMS worden gebruikt om verbeteracties te plannen. Deze acties richten zich op het versterken van zwakke punten in de beveiliging, het aanpassen van maatregelen aan nieuwe dreigingen, en het waarborgen van naleving van de BIO 2.0.

De verklaring van toepasselijkheid (SoA) wordt jaarlijks herzien om ervoor te zorgen dat de toegepaste maatregelen blijven aansluiten op de actuele risico’s en wettelijke eisen.


PLAN
Integraal beleid informatieveiligheid
ACT
DO
Risico-inventarisatie en -evaluatie
Actieplan informatieveiligheid
CHECK
Procedures ICT beheer
Procedures fysieke beveiliging
Basis beveiligings-richtlijnen BRP & PUN
Basis beveiligings-richtlijnen SUWI
Basis beveiligings-richtlijnen DigiD
enz

gemeente Winterswijk

Bijlage 1:

Overzicht van wet- en regelgeving onderliggend aan informatiebeveiliging (niet uitputtend)

1. Auteurswet
2. Telecommunicatiewet
3. Ambtenarenwet
4. Wet computercriminaliteit
5. Algemene verordening gegevensbescherming (AVG)
6. Archiefwet / Archiefregeling
7. Beveiligingsnorm DigiD B.01
8. Databankenwet
9. Wet elektronisch bestuurlijk verkeer
10. Wet elektronische handtekeningen
11. Wet algemene bepalingen Burgerservicenummer (Wabb)
12. Paspoortwet
13. Paspoortuitvoeringsregeling Nederland (PUN)
14. Reglement Rijbewijzen
15. Wet basisregistratie personen (Wet BRP)
16. Wet open overheid (Woo)
17. Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI)
18. Wet Basisregistratie Adressen en Gebouwen (BAG)
19. Wet Basisregistratie Grootschalige Topografie (BGT)
20. Wet Basisregistratie Ondergrond (BRO)
21. Wet kenbaarheid publiekrechtelijke beperkingen (WKPB)
22. Wet politiegegevens (Wpg)
23. Wet ruimtelijke ordening (Wro)
24. Cyberbeveiligingswet (CBW) – nationale implementatie van de NIS2-richtlijn.
25. Wet modernisering elektronisch bestuurlijk verkeer (Wmebv) – eventueel relevant bij digitale interacties.
26. Wet digitale overheid (Wdo) – nieuwe wet die richtlijnen geeft voor digitale dienstverlening door de overheid.
27. Wet gemeenschappelijke regelingen (Wgr) – relevant bij samenwerking met andere gemeenten.

gemeente Winterswijk

Bijlage 2:

Classificatietabel voor informatiebeveiliging
De basisbeveiligingsniveaus zijn uitgewerkt langs de lijnen beschikbaarheid, integriteit en vertrouwelijkheid. De BBN-toets helpt bij het kiezen van het best passende niveau. De beschikbaarheidsniveaus zijn gebaseerd op de geldende beschikbaarheidsniveaus die door de grote interne dienstenleveranciers worden gehanteerd. De vertrouwelijkheidsniveaus zijn in lijn gebracht met de schadescenario's die gelden voor de **te beschermen belangen**. De onderverdeling is als volgt:
BBN1: beschikbaarheid = Laag integriteit = Laag vertrouwelijkheid = Laag
BBN2: beschikbaarheid = Midden integriteit = Midden vertrouwelijkheid = Midden
BBN3: beschikbaarheid = Midden integriteit = Midden vertrouwelijkheid = Hoog

BBN1	
Beschikbaarheid = Laag	Het informatiesysteem mag incidenteel uitvallen voor maximaal twee weken (ook in piekperiodes) en dit heeft nauwelijks of geen gevolgen voor burgers/gebruikers. Uitval kan leiden tot beperkte schade, bijvoorbeeld: – financiële gevolgen; op te vangen binnen de vastgestelde ruimte binnen de begroting van de organisatie of uitvoeringsorganisatie; leidt nog niet tot het niet krijgen van een accountantsverklaring; – beperkt verlies van management control; – irritatie en ongemak bij burgers geventileerd in de media; – interne negatieve publiciteit (imagoschade). Deze gevolgen worden als volgt gekwantificeerd: – Kantoorautomatisering en organisatiespecifieke systemen hebben tijdens openingstijden een beschikbaarheid van minimaal 98% op maandbasis ook in piekperiodes. – Maximaal dataverlies 28 uur. – Maximale hersteltijd in geval van incidenten is binnen 40 werkuren (vijf werkdagen van 8 uur) in 85% van de gevallen.
Integriteit = Laag	Er zijn geen bijzondere maatregelen noodzakelijk om de juistheid, tijdigheid en volledigheid van informatie te waarborgen. Het verlies van integriteit kan leiden tot beperkte schade, bijvoorbeeld: – financiële gevolgen; op te vangen binnen de vastgestelde ruimte binnen de begroting van de organisatie of uitvoeringsorganisatie; leidt nog niet tot het niet krijgen van een accountantsverklaring; – beperkt verlies van management control; – irritatie en ongemak bij burgers geventileerd in de media; – interne negatieve publiciteit (imagoschade).
Vertrouwelijkheid = Laag	Kennisname van informatie door ongeautoriseerden (buitenstaanders) is niet gewenst, maar leidt niet tot schade van enige omvang. Het gaat hier om ongerubriceerde informatie. Het openbaar worden van deze informatie kan leiden tot: – financiële gevolgen: op te vangen binnen de begroting van de organisatie of uitvoeringsorganisatie; – irritatie en ongemak bij burgers geventileerd in de media; – interne negatieve publiciteit (imagoschade).

BBN2	
Beschikbaarheid = Midden	Het informatiesysteem mag beperkt korte tijd uitvallen voor maximaal één week (ook in piekperiodes) en dit heeft voelbare gevolgen voor burgers/gebruikers. Uitval kan leiden tot beperkte schade, bijvoorbeeld: – politieke schade aan een bestuurder: bestuurder moet zich verantwoorden naar aanleiding van verantwoordingsvragen; – diplomatieke schade te herstellen door ambtelijke opschaling; – financiële gevolgen: niet meer op te vangen binnen de vastgestelde ruimte binnen de begroting van de (uitvoerings)organisatie; geen accountantsverklaring afgegeven; – belangrijk verlies van management control; – verlies van publiek respect; klachten van burgers;

	– organisatiebrede negatieve publiciteit (imagoschade) of significant verlies van motivatie van medewerkers. De beschikbaarheid wordt als volgt gekwantificeerd: – Kantoorautomatisering en organisatiespecifieke systemen hebben tijdens openingstijden een beschikbaarheid van minimaal 98% op maandbasis ook in piekperiodes. – Maximaal dataverlies 24 uur. – Maximale hersteltijd in geval van incidenten is binnen 16 werkuren (twee dagen van 8 uur).
Integriteit = Midden	Er zijn passende maatregelen noodzakelijk om de juistheid, tijdigheid en volledigheid (VIR-definitie) te waarborgen. Het verlies van integriteit kan leiden tot forse schade, bijvoorbeeld: – politieke schade aan een bestuurder: bestuurder moet zich verantwoorden naar aanleiding van verantwoordingsvragen; – diplomatieke schade te herstellen door ambtelijke opschaling; – financiële gevolgen: niet meer op te vangen binnen de vastgestelde ruimte binnen de begroting van de (uitvoerings)organisatie; geen accountantsverklaring afgegeven; – belangrijk verlies van management control; – verlies van publiek respect; klachten van burgers; – organisatiebrede negatieve publiciteit (imagoschade) of significant verlies van motivatie van medewerkers.
Vertrouwelijkheid = Midden	Bescherming van gegevens en andere te beschermen belangen in de processen van de overheid, waar onder andere vertrouwelijkheid aan de orde is, omdat het om gevoelige informatie gaat. Het openbaar worden van de gegevens kan leiden tot: – politieke schade aan een bestuurder: bestuurder moet zich verantwoorden naar aanleiding van verantwoordingsvragen; – diplomatieke schade te herstellen door ambtelijke opschaling; – financiële gevolgen: niet meer op te vangen binnen de begroting van de (uitvoerings)organisatie; geen accountantsverklaring afgegeven; – verlies van publiek respect; klachten van burgers of significant verlies van motivatie van medewerkers; – bindende aanwijzing van de AP in verband met schending van de privacy; – directe imagoschade, bijvoorbeeld door negatieve publiciteit.

BBN3	
Beschikbaarheid = Midden	Het informatiesysteem mag beperkt korte tijd uitvallen voor maximaal één week (ook in piekperiodes) en dit heeft voelbare gevolgen voor burgers/gebruikers. Uitval kan leiden tot beperkte schade, bijvoorbeeld: – politieke schade aan een bestuurder: bestuurder moet zich verantwoorden naar aanleiding van verantwoordingsvragen; – diplomatieke schade te herstellen door ambtelijke opschaling; – financiële gevolgen: niet meer op te vangen binnen de vastgestelde ruimte binnen de begroting van de (uitvoerings)organisatie; geen accountantsverklaring afgegeven; – belangrijk verlies van management control; – verlies van publiek respect; klachten van burgers; – organisatiebrede negatieve publiciteit (imagoschade) of significant verlies van motivatie van medewerkers. De beschikbaarheid wordt als volgt gekwantificeerd: – Kantoorautomatisering en organisatiespecifieke systemen hebben tijdens openingstijden een beschikbaarheid van minimaal 98% op maandbasis ook in piekperiodes. – Maximaal dataverlies 24 uur. – Maximale hersteltijd in geval van incidenten is binnen 16 werkuren (twee dagen van 8 uur).

Integriteit = Midden	Er zijn passende maatregelen noodzakelijk om de juistheid, tijdigheid en volledigheid (VIR-definitie) te waarborgen. Het verlies van integriteit kan leiden tot forse schade, bijvoorbeeld: – politieke schade aan een bestuurder: bestuurder moet zich verantwoorden naar aanleiding van verantwoordingsvragen; – diplomatieke schade te herstellen door ambtelijke opschaling; – financiële gevolgen: niet meer op te vangen binnen de vastgestelde ruimte binnen de begroting van de (uitvoerings)organisatie; geen accountantsverklaring afgegeven; – belangrijk verlies van management control; – verlies van publiek respect; klachten van burgers; – organisatiebrede negatieve publiciteit (imagoschade) of significant verlies van motivatie van medewerkers.
Vertrouwelijkheid = Hoog	Verlies van informatie heeft een grote impact, waarvan niet uit te leggen is als deze niet gerubriceerd is en beschermd wordt op het niveau van BBN3: – informatie wordt door derden geleverd met een rubricering (niet zijnde BBN2); – aansluiting op een infrastructuur vereist BBN3 (bijvoorbeeld om al op de infrastructuur aanwezige gerubriceerde informatie niet in gevaar te brengen) om informatie te kunnen verwerken op deze infrastructuur; – weerstand tegen statelijke actoren is noodzakelijk.