Informatieveiligheidsbeleid DUO-organisaties 2025 – 2027

Datum : 5 januari 2025
Versie : Ter vaststelling college van B&W
Zaaknummer : 2024-077175

Managementsamenvatting

In dit document is het ‘Informatiebeveiligingsbeleid 2025-2027 beschreven voor de DUO-organisaties’. In de DUO-organisaties werken drie gemeenten, namelijk Ouder-Amstel, Diemen en Uithoorn en de Duo+ organisatie samen aan één gemeenschappelijke bedrijfsvoering. In dit beleid worden de kaders gesteld waarbinnen, op het gebied van informatiebeveiliging, gewerkt moet worden.

Het doel is om in control te zijn met het beveiligen van (persoons)informatie waarmee binnen de DUO-organisaties wordt gewerkt en waarvoor de gezamenlijke organisaties verantwoordelijk zijn. Het in control zijn en blijven op het gebied van informatiebeveiliging is een traject waar continue aan wordt gewerkt om in te spelen op de veranderende wereld om ons heen en op basis van aanscherping van het normenkader vanuit de Rijksoverheid. Het goed omgaan met informatie is een taak van alle medewerkers van elke individuele organisaties zelf, iedereen heeft hier een verantwoordelijkheid in.

Het informatiebeveiligingsbeleid houdt rekening met:

- De Baseline Informatiebeveiliging Overheid (BIO), en de toekomstige Europese wetgeving, de Network and Information Security directive (NIS2-richtlijn).
- De vertaling van deze Europese richtlijn naar Nederlandse wetgeving middels de NIB2-richtlijn, de Netwerk- en informatiebeveiliging richtlijn) welk naar verwachting effectief zal worden via de Cyberbeveiligingswet (Cbw). Hieruit zal een aanpassing volgen van de huidige BIO naar een nieuwe versie, de BIO2.
- Het twee jaarlijks opgestelde dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten.
- Eisen die voortkomen uit van toepassing zijnde wet- en regelgeving.
- Informatie uit eerdere incidenten, inbreuken op de beveiliging en bevindingen uit diverse audits, zoals het jaarlijkse ENSIA-proces en de Wpg-auditrapporten.
- De wens van de DUO-organisaties om gezamenlijk ook een visie op Informatieveiligheid, in woord en beeld, op te stellen.

De BIO kent een onderscheid in meer zogenoemd ‘’Strategisch (lange termijn) en een Tactische (meer operationele” variant van het informatieveiligheidsbeleid. In dit document wordt het lange termijn ’ Informatieveiligheidsbeleid 2025-2027’ beschreven en is middels dit beleidsstuk de kapstok voor de visie van het bestuur en management van de DUO-organisaties op informatiebeveiliging. Het geeft aan hoe de gestelde inzichten en doelstellingen bereikt gaan worden, inclusief een samenhangende reeks stappen die de continuïteit van Informatieveiligheid borgen in en onderliggende beleidsstukken, processen en procedures op het gebied van informatiebeveiliging en wordt jaarlijks geëvalueerd. De maatregelen worden jaarlijks naar individuele afdelingen/teams vertaald middels een apart jaarplanningsdocument. Hierin staan concrete acties uitgewerkt en vindt er achteraf een toetsing plaats, waarna er een nieuwe jaarplanning wordt gemaakt. Bij significante wijzigingen wordt het beleid aangepast.

In een separaat document, namelijk het “Tactisch informatieveiligheidsbeleid”, wordt aan de hand van de BIO het inhoudelijke normenkader uitgewerkt. Hierin worden alle normen en maatregelen vanuit de BIO, de BIO2, de AVG, de WPG en de NIS2/Cbw nader uitgewerkt, die leidend zullen zijn voor alle organisatieonderdelen van Duo+ en haar partners. Op dit moment, januari 2025, is nog niet bekend wat exact de impact van de nieuwe Europese richtlijn, de NIS2, zal zijn voor de DUO-organisaties. Want hoewel deze Europese richtlijn ingaat per oktober 2024 in is gegaan, is in de vertaling naar Nederlandse wetgeving in de vertraging gekomen. Een volgende stap welke hieruit volgt zal zijn een actualisatie welke specifiek voor

overheidsorganisaties zal gaan gelden: de actualisatie van de huidige BIO naar de BIO2. Er zal een actualisatie van het 'Tactisch informatieveiligheidsbeleid' volgen waarin nader zal worden ingegaan op de wijzigingen.

Dit nieuwe document 'Informatiebeveiligingsbeleid 2025-2027 beschreven voor de DUO-organisaties' is daarom puur een actualisatie van het oude beleid waarin voornamelijk nieuwe wettelijke bepalingen zijn opgenomen, tekstuele verbeteringen en verbeterende leesbaarheid zijn doorgevoerd. Wel nieuw in dit document is opgenomen de gezamenlijk Visie van de DUO-organisaties op Informatieveiligheid. Deze is 'in woord en in beeld' te vinden in paragraaf 1.4 en in Bijlage II. Verder beschrijft hoofdstuk 5 de zogenoemde 'Assessment-eisen bij gebruik van de DUO-DigiD-aansluitingen'.
In 2022 was er een aparte Annex aan het 'Strategisch Informatieveiligheidsbeleid 2020 -2023' toegevoegd naar aanleiding van veranderende eisen van de toezichthouder Logius. Deze was destijds onder mandatering van de Directeur Duo+ bij de verantwoording over ENSIA 2022 geaccordeerd.

Tenslotte is er specifiek voor de AVG, net als in de vorige versie van het meerjarige Informatiebeveiligings-beleid, een apart document voor de DUO-organisaties opgesteld met hierin hoe de AVG-aanpak binnen de DUO-organisaties, meer op operationeel niveau zal worden uitgevoerd beschreven. Deze documenten samen vormen de basis voor de uitvoering van het beleid voor de komende jaren.

Met instemming van het voorliggende document vervalt het oude 'Strategisch Informatieveiligheidsbeleid 2020 -2023' (zaaknr. 2020 – 103730) alsmede ook de Annex 'Aanvullingen op het Strategisch Informatieveiligheidsbeleid DUO-organisaties 2020 – 2023' (zaaknr. 2022-126112) wordt direct ingestemd met de verdere uitwerking. Met dit aangepaste beleid 'Informatieveiligheidsbeleid 2025-2027 voor de DUO-organisaties' wordt daarnaast bepaald dat de DUO-organisaties bij voorkomende keuzes en vraagstukken ten aanzien van de veiligheid van informatieprocessen de beleidsregels in dit document als uitgangspunt hanteert.

Inhoudsopgave

Managementsamenvatting **2**

Inhoudsopgave **4**

1 Inleiding **7**

1.1 Aanleiding tot informatiebeveiliging 7

1.2 Leeswijzer 7

1.3 Wat is informatiebeveiliging? 7

1.4 Visie op informatiebeveiliging 8

1.5 De informatieveiligheidspiramide 9

1.6 Verantwoordelijkheid en bevoegdheid informatieveiligheidsbeleid 11

1.7 Algemene oriëntatie en positionering 11

1.8 Geldigheid en evaluatie 11

2 Lange termijn beleid **13**

2.1 Doel 13

2.2 Ontwikkelingen 13

2.2.1 De Baseline Informatiebeveiliging Overheid (BIO) en de BIO2 13

2.2.2 De 10 principes voor informatiebeveiliging 13

2.2.3 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 14

2.3 Speerpunten voor de komende beleidsperiode 14

2.3.1 Speerpunt 1: Het belang voor informatiebeveiliging is duidelijk voor iedereen 14

2.3.2 Speerpunt 2: Technische maatregelen groeien mee met het cyberdreigingsbeeld 15

2.3.3 Speerpunt 3: P&C-cyclus voor informatiebeveiliging is ingericht voor alle afdelingen 15

2.3.4 Informatie uit incidenten, en bevindingen uit audits / testen 15

2.3.5 Wetgeving 15

2.4 Standaarden van informatiebeveiliging 16

2.5 Informatieveiligheidsbeleid 17

2.6 Beleidsdocument voor Informatieveiligheid 17

2.7 Plaats van het langere termijn beleid 17

2.8 Scope informatiebeveiliging 17

2.9 Informatiebeveiliging in relatie tot privacy 18

2.10 Logging 19

2.11 Informatieveiligheidsanalyse 19

2.12 Aanvullende maatregelen 19

2.12.1 Afwijkend beveiligingsniveau 19

2.12.2 Persoonsgegevens 20

2.13 Borging van het informatieveiligheidsbeleid 20

2.14 Eenduidige Normatiek Single Information Audit (ENSIA) 21

2.15 Uitgangspunten lange termijn informatiebeveiligingsbeleid 21

2.15.1 Risk Management 22

2.15.2 Lange termijn doelen 22

2.15.3 Belangrijkste uitgangspunten 22

2.15.4 Invulling van de uitgangspunten 23

2.15.5 Randvoorwaarden 24

3 Organisatie, taken & verantwoordelijkheden 25
3.1 Doel 25
3.2 Verantwoordelijkheidsniveaus binnen Duo+ 25
3.3 Beleidsbepalende, regisserende en coördinerende verantwoordelijkheden 25
3.4 Verantwoordelijkheden en taken van leidinggevenden 26
3.5 Betrokken partijen 26
3.5.1 Het College van B&W en de gemeenteraad 26
3.5.2 Directieteam en gemeentesecretaris 26
3.5.3 Teammanagers / -leiders 27
3.5.4 Chief Information Security Officer (CISO) 27
3.5.5 Functionaris Gegevensbescherming (FG) 28
3.5.6 De teamleider Informatisering en Automatisering 29
3.5.7 De teamleider Interne Dienstverlening Duo+ 29
3.5.8 De teamleider Interne Dienstverlening Diemen 30
3.5.9 De teamleider Personeel en Organisatie 30
3.5.10 Team Informatieveiligheid en Privacy 30
3.5.11 Privacy Officer (PO) 30
3.5.12 Specialist informatiebeveiliging per team 31
3.5.13 De Gegevensbeheerders 31
3.5.14 De Medewerkers 31
3.6 Rapporteren beveiligingsincidenten en datalekken 31
3.7 Controle en verantwoording 32
3.8 Overlegvormen 32
3.9 Afstemming met portefeuillehouder 32
3.10 ICT-crisisbeheersing (Business Continuity) 32
3.11 Coordinated vulnerability disclosure / responsible disclosure 33
3.12 Verantwoordelijkheden afdelingsoverstijgende (informatie)systemen 34
3.13 Contracten met derden 34
3.13.1 Servicelevel agreement (niveau van dienstverlening) 34
3.13.2 (ICT-)overeenkomsten met een derde partij 34
3.13.3 Verwerkers van persoonsgegevens 35
3.13.4 Toegang derden tot systemen 35
3.13.5 Specialistische Inhuur derden 35
4 Inventarisatie en beheer van informatie en bedrijfsmiddelen 37
4.1 Inleiding 37
4.2 Inventarisatie van informatie en (informatie) bedrijfsmiddelen 37
4.3 Eigendom van informatie en bedrijfsmiddelen 37
4.4 Aanvaardbaar gebruik van bedrijfsmiddelen 37
5 Assessment bij gebruik van DigiD-aansluitingen 39
5.1 Inleiding 39
5.2 DigiD-audit en Third Party Mededeling SaaS-diensten 39
5.3 Randvoorwaarden DigiD-aansluiting 39
5.4 Taken en verantwoordelijkheden proceseigenaar 40
6 Uitzonderingen op dit informatiebeveiligingsbeleid 41
7 Slot 41

Bijlage I. Huidige DigiD-aansluitingen 42

Bijlage II. Visie op Informatieveiligheid in beeld 43

Bijlage III. Overzicht BIO normenkader 44

Bijlage IV. Overzicht BIO-overheidsmaatregelen 45

Bijlage V. Aandachtsgebieden AVG 50

Bijlage VI. Afkortingen, wet- en regelgeving, richtlijnen en normenkaders 52

1 Inleiding

1.1 Aanleiding tot informatiebeveiliging

Deze beleidsnota beschrijft het Informatiebeveiligingsbeleid van de DUO-organisaties voor de jaren 2025 tot 2027 en vervangt het in 2020 vastgestelde 'Strategisch Informatiebeveiligingsbeleid 2020-2023'. Deze nota is richtinggevend en kader stellend en wordt aangevuld met onderwerp specifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau.

Met dit aangepaste 'Informatiebeveiligingsbeleid Duo-organisaties 2025-2027' zetten de DUO-organisaties een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente te continueren en voort te gaan op de stappen die in de voorgaande jaren gezet zijn. De basis voor dit beleid is de NEN-ISO/IEC 27002 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO). De principes zijn gebaseerd op de 10 principes[1] voor informatiebeveiliging zoals uitgewerkt door de VNG.

1.2 Leeswijzer

In hoofdstuk 2 wordt de kern van het beleid uiteengezet en bevat de basisprincipes voor informatiebeveiliging. Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn. In Hoofdstuk 4 staan de Classificaties en beheer van informatie en bedrijfsmiddelen beschreven. In Hoofdstuk 5 staat informatie beschreven over hoe om te gaan met de digitale persoons identificatie rond DigiD. In de bijlagen is nadere informatie te vinden met betrekking tot de toetsing onderwerpen die de AVG en de BIO beschrijven. En is in beeld weergeven wat de Visie op Informatieveiligheid is van de DUO-organisaties.

1.3 Wat is informatiebeveiliging?

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van persoonsgegevens en andere informatie.

- Beschikbaarheid: Het zorgdragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers.
- Integriteit: het waarborgen van de juistheid, volledigheid, en controleerbaarheid van informatie en informatieverwerking.
- Vertrouwelijkheid: de mate waarin informatie alleen toegankelijk is of wordt gemaakt voor degenen die hiervoor gerechtigd zijn.

[1] De 10 bestuurlijke principes voor informatiebeveiliging'. https://vng.nl/files/vng/de-10-bestuurlijke-principes-voor_20190109.pdf

1.4 Visie op informatiebeveiliging

Dat de samenwerkende DUO-organisaties Informatieveiligheid belangrijk vinden onderstreept dat men gezamenlijk een aparte visie op Informatieveiligheid heeft opgesteld. Hieronder is deze tekst weergeven. Daarnaast is deze visie ook visueel vertaald. In Bijlage II is deze te vinden.

De gemeente Uithoorn/Diemen/Ouder-Amstel/ Uitvoeringsorganisatie Duo+ is een openbare organisatie die zich inzet voor de leefbaarheid en de veiligheid van haar inwoners. De gemeente verwerkt zelf maar soms ook samen met de DUO-partners persoonsgegevens en andere informatie van haar inwoners, bedrijven, personeel en bezoekers. Deze gegevens zijn vertrouwelijk en moeten beschermd worden tegen ongeoorloofde toegang, gebruik, wijziging of vernietiging.

Als college erkennen wij eindverantwoordelijk te zijn voor de informatiebeveiliging binnen onze DUO-samenwerking en dit hebben wij ook bekrachtigd in onze eigen afzonderlijke gemeente. Wij zullen er dan ook voor zorgen dat er voldoende middelen beschikbaar zijn om informatiebeveiliging op de juiste wijze te waarborgen. Wij zorgen voor een goede beschikbaarheid van onze systemen en beschermen onze data op een adequate wijze. Adequaat wil zeggen dat we kijken naar de stand van de techniek, het risico en de kosten die de maatregelen met zich meenemen. Deze zaken moeten met elkaar in balans zijn.

Wij hanteren een integrale risicomanagementbenadering om onze informatiebeveiliging op peil te houden. Door in te spelen op risico's kunnen wij de middelen efficiënt en effectief inzetten. We identificeren en analyseren risico's en nemen de nodige maatregelen om deze risico's te mitigeren of te elimineren. Wij nemen hierbij informatiebeveiligingsmaatregelen vanaf het begin mee bij aanpassingen van processen en systemen. Hierbij besteden wij extra aandacht aan de bescherming van persoonsgegevens en de bescherming van vitale infrastructuur. We realiseren ons ook dat 100% veilig nooit haalbaar is maar we doen wel onze uiterste best om zo veilig mogelijk te zijn. Wij zorgen er minstens voor dat onze gemeente voldoet aan alle relevante wet- en regelgeving op het gebied van informatiebeveiliging, waaronder maar niet uitsluitend de Baseline Informatiebeveiliging Overheid (BIO), de Algemene Verordening Gegevensbescherming (AVG), de Wet politiegegevens (Wpg) en de Network and Information Security directive (NIS2-richtlijn). Compliance is voor ons een belangrijk uitgangspunt.

Als college staan we midden in de samenleving en werken we zowel intern als extern samen. We erkennen de noodzaak van samenwerking en informatie-uitwisseling met de onderlinge DUO-partners en relevante (externe) partijen op het gebied van informatiebeveiliging. We streven naar een gezamenlijke aanpak om gemeenschappelijke dreigingen aan te pakken en best practices te delen. We realiseren ons hierbij dat wij ook verantwoordelijk zijn voor verwerkingen van informatie die we door derden laten uitvoeren.

Het waarborgen van de continuïteit van de informatievoorziening bij calamiteiten of storingen is voor ons van groot belang. Dit onder het motto van Benjamin Franklin “Failing to Prepare. Is Preparing to Fail”.
Als college hechten we veel waarde aan de eigen verantwoordelijkheid van het management en de medewerkers op het gebied van informatiebeveiliging. We zorgen voor adequate training en bewustwording van medewerkers, waarbij we hen voorzien van de nodige kennis en vaardigheden om informatiebeveiliging te waarborgen. Deze trainingen zijn niet vrijblijvend. Daarnaast zorgen we voor een open en veilige werkomgeving waarin medewerkers worden aangemoedigd om risico's te signaleren en veiligheidsincidenten te melden en bij te dragen aan het verbeteren van onze informatiebeveiligingspraktijken. Hiermee creëren wij als bestuurders gemeente een cultuur van veiligheid en bewustzijn op het gebied van informatiebeveiliging. Zo kunnen wij de privacy en veiligheid van onze inwoners, personeel en andere belanghebbenden optimaal waarborgen.

Wij streven naar transparantie en openheid over de informatiebeveiligingsmaatregelen die wij nemen. Wij vinden het belangrijk dat inwoners, personeel en andere stakeholders vertrouwen hebben in onze aanpak, dat zij op ons kunnen vertrouwen en dat zij weten hoe wij omgaan met informatiebeveiliging. Dit draagt bij aan het behoud en versterken van de fundamentele vrijheden die horen bij onze democratische rechtstaat.

Informatisering speelt een steeds prominentere rol in de gemeentelijke organisatie en samenwerkings-verbanden op het lokale niveau. Deze rol wordt in het kader van het stelsel van basisregistraties en de toenemende complexiteit van het digitale dienstverleningskanaal steeds belangrijker. De DUO-organisaties richten zich op het koppelen van systemen waardoor grote gegevensverzamelingen ontstaan die vervolgens weer specifieke informatie opleveren voor interne en externe afnemers.

Daarnaast zijn de DUO-organisaties steeds afhankelijker van goed werkende informatievoorziening en -systemen. Dit betekent dat de organisaties alert zijn op mogelijke verstoringen van of bedreigingen gericht op informatiesystemen, mede omdat veel informatiesystemen niet primair zijn ontworpen met het oog op veiligheid. De veiligheid die met de technische middelen kan worden bereikt is begrensd en wordt al vanouds ondersteund met passende beheerprocessen en procedures. Ook speelt de menselijke factor (het menselijk gedrag) een steeds grotere rol in het daadwerkelijk realiseren van de veiligheid van informatie in de praktijk. Deze factor speelt, door de steeds complexer wordende informatieprocessen, veelal zelfs een doorslaggevende rol.

Informatie komt in verschillende vormen voor. Het kan zijn geschreven, gesproken, gedrukt of digitaal zijn verwerkt en-/of opgeslagen. Al deze verschijningsvormen van informatie vragen voor een deel eenzelfde generieke aanpak, maar kennen ook verschillen. Dit document besteedt hier aandacht aan.

De veiligheid van informatie speelt binnen een groot aantal gebieden van de DUO-organisaties een rol. Om te voorkomen dat binnen elk van die gebieden (bijvoorbeeld rondom Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), de Basisregistratie Personen (BRP) en Waardedocumenten (WD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Ondergrond (BRO) of Basisregistratie Grootschalige Topografie (BGT) separaat beleid ontwikkeld en geïmplementeerd wordt, is de keuze gemaakt dit voor de DUO-organisaties een breed informatieveiligheidsbeleid op te stellen voor alle organisatie onderdelen.

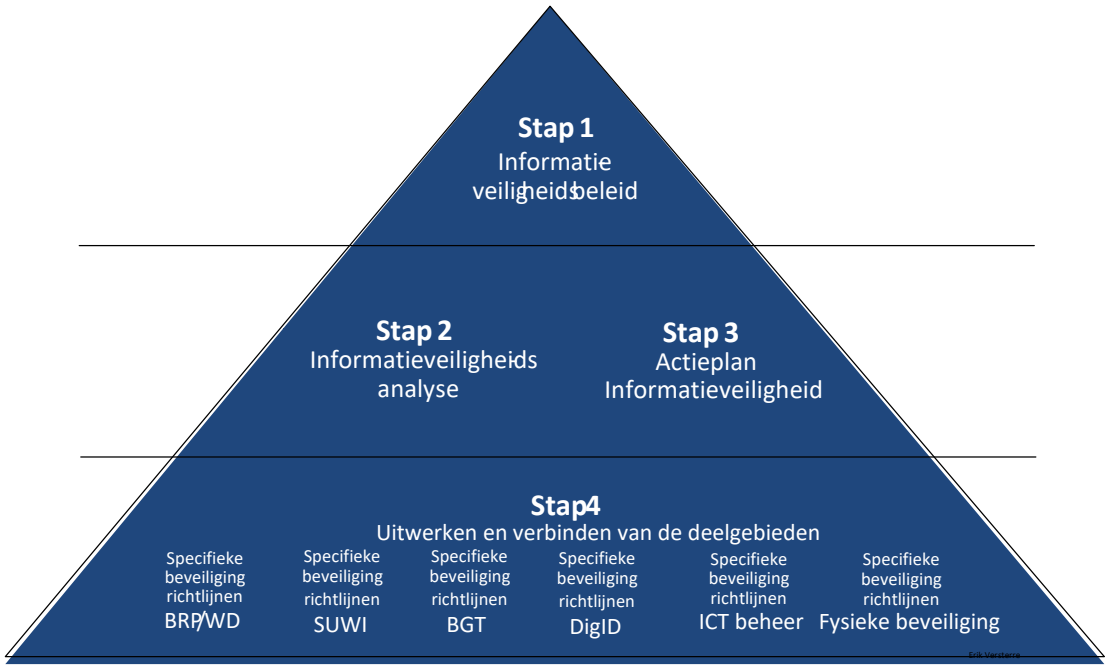
De DUO-organisaties stellen gezamenlijk een organisatie breed informatieveiligheidsbeleidskader vast. Daarin wordt op lange en korte termijn (hoog over en meer operationeel werk/afdelingsniveau) beschreven welke uitgangspunten er gelden ten aanzien van de Informatieveiligheid. Voor alle DUO-organisaties gelden derhalve dezelfde uitgangspunten. Dit document zal samen met het meer operationeel Informatieveiligheidsbeleid, de technische beveiligingsmaatregelen en de procedures een adequaat niveau van beveiliging voor de organisatie opleveren waardoor de kwaliteitskenmerken van informatie, te weten de beschikbaarheid, de integriteit, de vertrouwelijkheid en de controleerbaarheid van de informatie binnen alle domeinen van de DUO-organisaties zijn gewaarborgd.
Informatiebeveiliging is een proces waarbij het continue leren op de eerste plaats staat en is ook niet bedoeld voor het winnen op de korte termijn. Het is een lange termijnstrategie met vallen en opstaan. Dat vergt een mind-set en maakt dat het onderwerp Informatieveiligheid een vast onderdeel moet zijn op de bestuurstafel.

1.5 De informatieveiligheidspiramide

De centrale overheid heeft veel aandacht voor de veiligheid van informatie binnen de verschillende overheidslagen. Naast het ontwikkelen van nieuwe wet- en regelgeving op dit gebied uit zich deze aandacht ook in bewustwordingscampagnes en ondersteuning van gemeentelijke overheden en samenwerkingsverbanden bij hun inspanningen om de veiligheid van overheidsinformatie te verhogen. De toenemende complexiteit en intensiteit van de informatieprocessen bieden een helder motief voor overheden om hun aandacht nog meer te richten op de veiligheid voor overheidsinformatie.

Teneinde de scope van dit document te verduidelijken, is in Figuur 1 aangegeven welke niveaus van Informatieveiligheid zijn te onderkennen.

Bovenaan de piramide treffen we het informatieveiligheidsbeleid aan. Dit is een organisatie breed beleid dat de uitgangspunten, de normen en de kaders biedt voor de veiligheid van alle onderliggende gemeentelijke informatieprocessen. Uitzonderingen hierop zijn toegestaan, maar dan wel duidelijk gemotiveerd én verifieerbaar.



Figuur 1 De informatieveiligheidspiramide

Het tactische niveau van de piramide is gericht op het tactische implementatietraject. De implementatiefase begint met het uitvoeren van een GAP-analyse. Tijdens deze GAP-analyse worden de uitgangspunten uit het organisatie brede informatiebeveiligingsbeleid getoetst aan de praktijksituatie. Hierin worden niet alleen de ‘harde aspecten’ onderzocht. Dat wil zeggen de techniek, de regels en de procedures. Maar worden ook de ‘zachte aspecten’ meegenomen. Deze richten zich op het menselijk handelen, cultuuraspecten en daarnaast op de sociale en fysieke inrichting van de organisatie. Na de GAP-analyse vindt als slot nog een risicoweging, prioritering en planning van te nemen maatregelen plaats. Tijdens deze stap worden risico’s die zijn geconstateerd, gewogen en eventueel van maatregelen voorzien, zodat een compact overzicht ontstaat van risico’s en te treffen maatregelen.

Op het laagste niveau wordt een complete set aan maatregelen opgeleverd die gericht is op de specifieke eisen van een onderdeel. Een onderdeel kan een applicatie zijn zoals de BRP, de BAG, BGT, BRO of het financiële systeem, maar kan ook gericht zijn op de ICT-beheerprocessen, de inrichting van de ICT-platformen of de juistheid van de crediteurenadministratie.

De voorstellen van de te nemen maatregelen zullen mogelijk worden besproken in de verschillende OGON-overleggen van de DUO-organisaties.

1.6 Verantwoordelijkheid en bevoegdheid informatieveiligheidsbeleid

Het 'lange termijn' beleid rondom Informatieveiligheid van de bedrijfsvoeringsorganisatie Duo+ sluit aan op het 'lange termijn' beleid van de DUO-gemeenten. De gemeenteraden van de partners van Duo+ dragen de specifieke bevoegdheid voor de controle en de toetsing op de werking van beleid binnen de gemeente, [2] zo ook voor Informatieveiligheid.

De eindverantwoordelijkheid voor Informatieveiligheid ligt op bestuurlijk niveau bij het College (accountable), het hoofd Staf van Duo+ is voor de dagelijkse uitvoering verantwoordelijk (responsible). Indien een taakgebied niet is overgedragen aan Duo+ is de gemeentesecretaris van de desbetreffende gemeente verantwoordelijk (responsible).

De eindverantwoordelijkheid bestaat uit vaststelling en implementatie van de informatieveiligheidsstructuur [3] en de organisatie brede beleidsnormen. Voor het nemen van operationele maatregelen op het gebied van Informatieveiligheid is de directeur Duo+ gemandateerd. Dit betekent dat de directeur Duo+ toeziet op ontwikkeling en beheer van geschikt instrumentarium om Informatieveiligheid te kunnen waarborgen. Dit geldt ook in geval van ketenafhankelijkheid en bij cluster overstijgende (informatie)systemen. Per instrument is het afhankelijk van het taakgebied of de verantwoordelijkheid ligt bij het hoofd Staf Duo+ of de gemeente-secretaris van de desbetreffende gemeente.

Voor de informatiesystemen zijn de leidinggevenden/ proceseigenaren, verdeeld over de DUO-organisaties, verantwoordelijk. Zij dragen er zorg voor dat de informatiesystemen geclassificeerd en ingericht worden naar Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV), zodat er adequate maatregelen kunnen worden getroffen om de veiligheidsrisico's te beheersen. Een belangrijk aspect van deze verantwoordelijkheid is om de medewerkers mee te nemen in hun verantwoordelijkheid ten aanzien van de veiligheid van informatie in hun dagelijkse werkprocessen.

1.7 Algemene oriëntatie en positionering

Informatieveiligheid maakt onlosmakelijk deel uit van de bedrijfsvoering en de primaire processen van de organisatie en haar omgeving. In de uitwerking vormt het een samenhangend geheel van maatregelen van procedurele, organisatorische, fysieke, technische, personele en juridische aard.

Het doel van Informatieveiligheid is het behoud van:

- Beschikbaarheid / continuïteit (voorkomen van uitval van systemen)
- Integriteit / betrouwbaarheid (gegevens zijn juist, actueel en volledig)
- Vertrouwelijkheid / exclusiviteit (onbevoegden kunnen geen kennisnemen van gegevens die niet voor hen bestemd zijn)
- Controleerbaarheid (de mogelijkheid te kunnen achterhalen welke handelingen met de informatiesystemen zijn uitgevoerd)

1.8 Geldigheid en evaluatie

Het informatiebeveiligingsbeleid blijft van kracht tot nieuw informatiebeveiligingsbeleid is vastgesteld. Daarbij is het uitgangspunt dat jaarlijks wordt geëvalueerd en na drie jaar nieuw beleid wordt opgesteld en

[2] In hoofdstuk 2 worden de verantwoordelijkheden en bevoegdheden ten aanzien van informatieveiligheid uitgebreider beschreven.

[3] Onder het begrip informatieveiligheidsstructuur wordt in dit verband de complete beheercyclus van het informatieveiligheidsproces verstaan (beleidsvorming, implementatie, verantwoording, controle en bijstelling). Informatieveiligheid wordt gedefinieerd als een verzamelbegrip voor de kwaliteitsaspecten beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid.

vastgesteld. Bij belangrijke wijzigingen van bijvoorbeeld landelijke wet- en regelgeving zal het beleidsstuk eerder worden aangepast of middels addendum aangevuld.

2 Lange termijn beleid

2.1 Doel

Het doel van deze beleidsnota is het presenteren van het 'Informatiebeveiligingsbeleid voor de wat meer langere termijn, de jaren 2025 tot 2027 voor de DUO-organisaties'. De uitwerking van dit beleid in concrete maatregelen vindt plaats in de jaarlijks vast te stellen "Jaarplanning over Gegevensbescherming en Informatieveiligheid".

2.2 Ontwikkelingen

De ontwikkelingen die van belang zijn voor de actualisering van het informatiebeveiligingsbeleid zijn de volgende:

2.2.1 De Baseline Informatiebeveiliging Overheid (BIO) en de BIO2

De BIO (Baseline Informatiebeveiliging Overheid) en haar verwachte opvolger de BIO2 vormt het normenkader voor de gehele overheid. De werkwijze van deze BIO is meer gericht op risicomanagement. Dat wil zeggen dat de teammanagers of afdelingsmanagers nu meer dan vroeger moeten werken volgens de aanpak van de ISO-27001 en daarbij is risicomanagement van belang. Dit houdt voor het (team-)management in, dat men op voorhand keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen adequaat beveiligd zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid. Informatieveiligheid dient dus vanuit het primaire proces gestuurd te worden, daar waar het eigenaarschap van de informatie ligt. De teammanager kent het te beveiligen informatiesysteem en de te beschermen informatie uiteindelijk het best.

2.2.2 De 10 principes voor informatiebeveiliging

De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader [4] BIO en gaan over de waarden die de bestuurder zichzelf oplegt. De principes zijn als volgt:

1. Bestuurders bevorderen een veilige cultuur
2. Informatiebeveiliging is van iedereen
3. Informatiebeveiliging is risicomanagement
4. Risicomanagement is onderdeel van de besluitvorming
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking
6. Informatiebeveiliging is een proces
7. Informatiebeveiliging kost geld
8. Onzekerheid dient te worden ingecalculeerd
9. Verbetering komt voort uit leren en ervaring
10. Het bestuur controleert en evalueert

De principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging in de gemeentelijke organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de gemeentelijke processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van

[4] Deze principes worden gelijk met de BIO van kracht, zie besluitvorming Informatiebeveiligingsdienst (IBD) en Verenigde Nederlandse Gemeenten (VNG). Zie ook Bijlage IV - Overzicht BIO normenkader

de gemeente. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst als regelmatig terugkerend agendapunt bij de bestuurders.

2.2.3 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten van het Nationaal Cyber Security Center (NCSC) en de Informatie Beveiligingsdienst (IBD), geeft een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dit dreigingsbeeld is daarmee het ideale document om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging.

De DUO-gemeenten zijn aangesloten bij de InformatieBeveiligingsdienst (IBD) van de VNG. Jaarlijks publiceren zij in samenwerking met het National Cyber Security Center (NCSC) een zogenaamd ‘dreigingsbeeld’ op het terrein van cybersecurity. In het dreigingsbeeld 2023/2024 [5] zijn de drie belangrijkste risico’s voor gemeenten geïdentificeerd:

1. Uitval van dienstverlening en bedrijfsvoering
2. Vertrouwelijke informatie in verkeerde handen
3. Fouten in de dienstverlening

De DUO-organisaties onderkennen deze risico’s en de organisaties hebben in de afgelopen beleidsperiode gewerkt aan een basis die de DUO-gemeenten in staat stellen om op alle risicogebieden door te groeien. Informatiebeveiliging is inmiddels een terugkerend onderwerp op de managementagenda’s. Dit is een randvoorwaarde voor risicomanagement en controle op informatiebeveiliging. Daarnaast zijn het werken ‘in regie’ en werken via ‘cloud’ belangrijke ontwikkelingen waarbij het belang van controle, audit en rapportage toeneemt. Drie speerpunten geven richting aan een effectief en doeltreffend informatiebeveiligingsbeleid voor de komende jaren.

2.3 Speerpunten voor de komende beleidsperiode

De komende periode blijft het ‘Team Informatieveiligheid’ – op dit moment als onderdeel van de Stafafdeling van Duo+, zich samen met direct betrokken afdelingen zoals Team I&A (ICT-gerelateerd) en Team ID (Fysieke beveiliging), zich inzetten op drie speerpunten voor informatiebeveiliging. Deze speerpunten vormen de kaders en deze worden nader uitgewerkt in de jaarlijkse informatiebeveiligingsplannen of plannen met een afzonderlijke team/afdeling. Naast de speerpunten hanteert de organisatie een aantal leidende principes die richting geven aan de invulling van informatiebeveiliging. Deze leidende principes worden in hoofdstuk 3 toegelicht.

2.3.1 Speerpunt 1: Het belang voor informatiebeveiliging is duidelijk voor iedereen

Het beschermen van informatie is een verantwoordelijkheid van iedereen. Men kan pas verantwoordelijkheid nemen als men weet wat er verwacht wordt en welke mogelijke gevaren er zijn. Het is daarom essentieel dat medewerkers getraind zijn en blijven op het gebied van informatiebeveiliging. De structurele bewustwording resulteert in een verhoogde weerbaarheid tegen de steeds veranderende social engineering-aanvallen. [6] Het beveiligingsbewustzijn wordt een onderdeel van de manier van werken en daarmee creëren we een sterke menselijke schakel in informatiebeveiliging. Gezien het blijvende belang van het beveiligingsbewustzijn, is dit speerpunt gehandhaafd uit het voorgaande informatiebeveiligingsbeleid.

[5] IBD_dreigingsbeeld_2023-2024_DEF-versie.pdf (informatiebeveiligingsdienst.nl)

[6] Social engineering is de aanvalsmethode die gericht is op het uitbuiten van zwakheden in de menselijke factor.

2.3.2 Speerpunt 2: Technische maatregelen groeien mee met het cyberdreigingsbeeld

Naast een goed beveiligingsbewustzijn, beschermen ook technische beveiligingsmaatregelen de informatie. Dit begint met een goede inrichting van de basismaatregelen uit de verplichte normenkaders zoals BIO,[7] DigiD en Suwinet. De digitale dreigingen ontwikkelen zich continue, waardoor aanvallers bestaande barrières weten te doorbreken of te omzeilen. Een beveiligingsmaatregel die een aantal jaar geleden nog voldoende bescherming bood, schiet nu mogelijk te kort. Om mee te blijven groeien en in de pas te blijven met het cyberdreigingsbeeld, is het zaak om de technische beveiligingsmaatregelen te blijven controleren op effectiviteit en doeltreffendheid. Deze controle vindt plaats door het uitvoeren van zelfevaluaties en/of audits.
Bij het adopteren van nieuwe technologieën wordt er al in een vroeg stadium gekeken naar informatiebeveiligings- en privacy risico's. Geïdentificeerde risico's worden inzichtelijk gemaakt zodat risicobehandeling plaats kan vinden.

2.3.3 Speerpunt 3: P&C-cyclus voor informatiebeveiliging is ingericht voor alle afdelingen

Uitwerking van het Informatiebeveiligingsbeleid moet vertaald worden naar specifieke plannen voor elke afdeling / team. De komende periode wordt de P&C cyclus nog verder doorontwikkeld en aangepast op basis van nieuwe wetgeving, zodat de P&C cyclus voor informatiebeveiliging tot op afdelingsniveau actueel blijft.

Afdelingsmanagers zijn verantwoordelijk voor informatiebeveiliging binnen hun afdeling. Dit stelt de afdelingsmanager in staat om zelf maatregelen te treffen en risico's binnen de afdeling af te wegen. Over de verantwoordelijkheid voor informatiebeveiliging en status van het juist implementeren van de AVG voor zijn/haar team/afdeling dient de manager verantwoording af te leggen aan het 'Team Informatieveiligheid' (CISO, Privacy Officers en FG) en de directie van de desbetreffende organisatie. De afdelingsmanager stelt hiervoor in overleg met het 'Team Informatieveiligheid' een managementverantwoordingsdocument op.

De CISO stelt op basis van de verantwoordingsdocumenten de gemeente brede verantwoording vast. Op basis van de gemeente brede verantwoording worden het college en de gemeenteraden geïnformeerd.

Gemeente breed wordt het informatiebeveiligingsbeleid jaarlijks uitgewerkt in een informatiebeveiligingsplan. Het beveiligingsplan bevat de activiteiten die noodzakelijk zijn om te komen tot de doelstellingen.

2.3.4 Informatie uit incidenten, en bevindingen uit audits / testen

De DUO-organisaties kennen naast het hierboven genoemde dreigingsbeeld ook een proces waarin beveiligincidenten en mogelijk hieruit voortvloeiende datalekken worden vastgelegd, gemonitord en besproken met het management. Dit proces geeft ook waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid. Ook laten de DUO-organisaties om kwetsbaarheden op te sporen en de digitale weerbaarheid te vergroten, jaarlijks audits en regelmatig (vulnerability)testen uitvoeren. Dit heeft als doel om inzicht te krijgen in de status en effectiviteit van de beveiligingsmaatregelen.

2.3.5 Wetgeving

Wetgeving is aan verandering onderhevig en dat kan inhouden dat er wetswijzigingen zijn die tot gevolg hebben dat het gemeentelijk informatiebeveiligingsbeleid moet veranderen. Voorbeelden (niet uitputtend, zie ook Bijlage VI) hiervan zijn o.a.:

- Algemene Verordening Gegevensbescherming (AVG)
- Wetpolitiegegevens (Wpg)

[7] Baseline Informatiebeveiliging Overheid, een overzicht van de aandachtsgebieden is opgenomen in Bijlage III.

- De Network and Information Security directive (NIS2-richtlijn); De vertaling van deze Europese richtlijn naar Nederlandse wetgeving middels de NIB2-richtlijn, de Netwerk- en informatiebeveiliging richtlijn) zal naar verwachting effectief worden via de Cyberbeveiligingswet (Cbw)
- Basis Registratie Personen (BRP)
- Basisregistratie Adressen en Gebouwen (BAG)
- Basisregistratie Grootschalige Topografie (BGT)
- Basisregistratie Ondergrond (BRO)
- Paspoortuitvoeringsregeling Nederland 2001 (PUN)
- Archiefwet 1995

2.4 Standaarden van informatiebeveiliging

De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002 genomen.

Voor de ondersteuning van gemeenten bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek [8] in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen.

Om te kunnen bepalen welke beveiligingsmaatregelen nodig zijn worden beveiligingsclassificaties toegepast. Hierbij is de aard van de informatie in deze processen leidend. Er wordt geclassificeerd op de drie betrouwbaarheidsaspecten van informatie: beschikbaarheid, integriteit en vertrouwelijkheid.

De BIO (1.0) bestaat uit een baseline met verschillende Basis BeveiligingsNiveaus (BBN).

BBN 1
- Minimale beveiligingsniveau voor overheidssystemen.
- Basisniveau en verplichte controls en maatregelen o.b.v. wet-& regelgeving (AVG) en beveiligingsprincipes (uit de BIO).
- Beschikbaarheid Laag, Integriteit Laag, Vertrouwelijkheid Laag.

BBN 2
- Uitgangspunt voor gemeenten.
- Vertrouwelijke informatie, incidenten kunnen leiden tot bestuurlijke commotie, veiligheid van andere systemen wordt beïnvloed.
- Beschikbaarheid Midden, Integriteit Midden, Vertrouwelijkheid Midden.

BBN 3
- Weerstand tegen statelijke actoren, niveau AIVD, aanvullende maatregelen o.b.v. risicoanalyse.
- Alleen bij zeer grote impact, kritieke infrastructuur, staatsgeheimen.
- Beschikbaarheid Midden, Integriteit Midden, Vertrouwelijkheid Hoog.

In Bijlage IV staan de BIO overheidsmaatregelen nog eens nader gespecificeerd. Of deze BBN-niveaus in dezelfde vorm terugkomen in uiteindelijk de BIO2 is op dit moment nog onduidelijk.

[8] De Interbestuurlijke werkgroep Normatiek bestaat uit vertegenwoordigers van bijvoorbeeld VNG en de IBD, maar ook waterschappen, provincies en het rijk.

Ook documenten hebben een classificatie op basis waarvan wordt bepaald hoe het document behandeld dient te worden. De documentclassificatie kent vier classificatieniveaus, [9] te weten Geheim, Vertrouwelijk, Bedrijfsvertrouwelijk en Openbaar. De classificatieniveaus zijn vastgelegd in het classificatieschema, inclusief de voorwaarden om de informatie te verwerken.

2.5 Informatieveiligheidsbeleid

Doelstelling: Het bieden van ondersteuning aan het bestuur, management en organisatie bij de sturing op en het beheer van Informatieveiligheid. Resultaat: Beleid waarin de taken, bevoegdheden en verantwoordelijkheden voor Informatieveiligheid alsmede het vereiste beveiligingsniveau zijn vastgelegd.

2.6 Beleidsdocument voor Informatieveiligheid

Het Bestuur van Duo+ en de colleges van burgemeester en wethouders van de DUO-gemeenten behoren respectievelijk een organisatie breed beleidsdocument voor Informatieveiligheid goed te keuren, uit te geven en kenbaar te maken aan alle medewerkers, alsmede hiernaar te handelen. Dit beleid dient in overeenstemming te zijn met het beleid van alle DUO-organisaties, vandaar ook dat deze een eigen kader vaststelt middels dit document.

De volgende aspecten zijn in dit beleidsdocument aanwezig:

- De doelstellingen van Informatieveiligheid voor de DUO-organisaties.
- De beveiligingseisen en –prioriteiten.
- De organisatie van de informatieveiligheidsfunctie.
- Een omschrijving van de algemene en specifieke verantwoordelijkheden en bevoegdheden met betrekking tot Informatieveiligheid voor leidinggevenden, medewerkers en ondersteunende informatiebeveiligingsrollen.
- De verwijzing naar relevante wet- en regelgeving en gemeentelijke regels en voorschriften op het gebied van privacybescherming, integriteit, archivering en fysieke beveiliging en de wijze waarop naleving van deze wettelijke, reglementaire of contractuele verplichtingen wordt gewaarborgd (zie hoofdstuk 0).
- De beschrijving van een periodiek evaluatieproces waarmee de inhoud en de effectiviteit van het vastgestelde beleid kunnen worden getoetst.

2.7 Plaats van het langere termijn beleid

Het langere termijn beleid wordt gebruikt om de basis te leggen voor de tactische beleidsplannen en daarmee richting te geven voor de verdere invulling van informatiebeveiliging op algemeen en meer operationeel niveau. Deze nota beschrijft op ‘hoog niveau’ het informatiebeveiligingsbeleid. Dit beleid zal worden vertaald in tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks te schrijven “Jaarplanning over Gegevensbescherming en Informatieveiligheid.”

2.8 Scope informatiebeveiliging

De scope van dit beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, informatie en gegevens van de gemeente en externe partijen, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

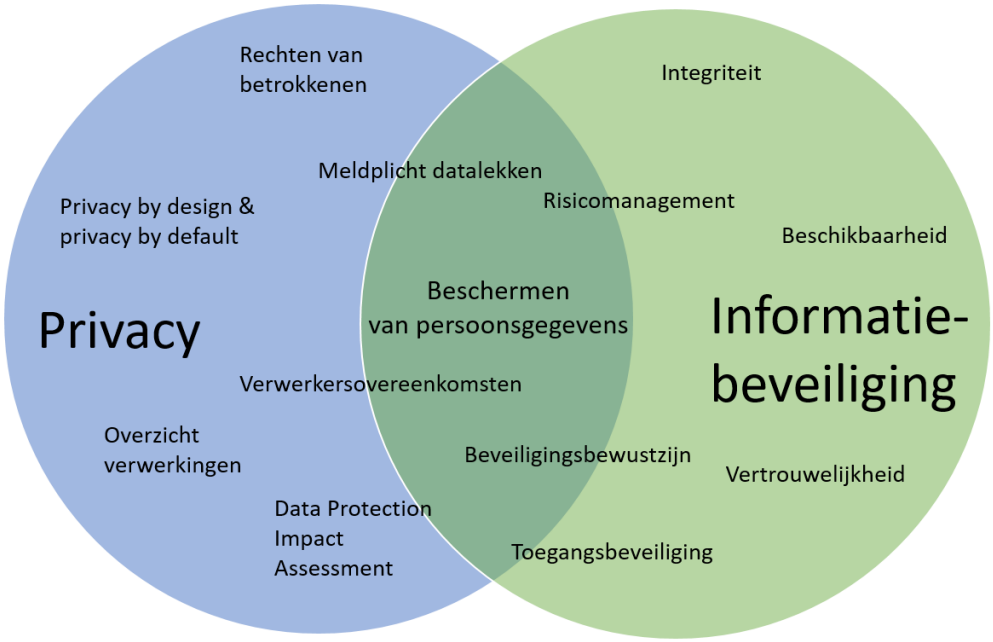
[9] Deze classificaties komen voort uit de richtlijnen van de IBD.

Dit Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals voor de BRP, PNIK, BAG, BGT, BRO en SUWI. [10] Voor bepaalde kerntaken gelden op grond van deze en wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld SUWI en gemeentelijke basisregistraties). Deze worden in aanvullende documenten geformuleerd.

Bewust wordt in het beleid zelf geen limitatief overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar meer specifieke onderdelen gelegd.

2.9 Informatiebeveiliging in relatie tot privacy

Er is nauwe samenhang tussen privacy en informatiebeveiliging. De burger en medewerkers hebben recht op eerbiediging en bescherming van de persoonlijke levenssfeer en een zorgvuldige omgang met persoonsgegevens. Dit vraagt een adequate beveiliging van deze persoonsgegevens en het respecteren van de geldende privacywetgeving. Het beschermen van persoonsgegevens is het gemeenschappelijke domein waar privacy en informatiebeveiliging samenkomen.



Figuur 2 Informatiebeveiliging in relatie tot privacy

Met de komst van de Algemene Verordening Gegevensbescherming (AVG) zijn de regels op Europees niveau vastgesteld. De DUO-organisaties moeten op basis van de eisen van de AVG passende technische en organisatorische maatregelen treffen om persoonsgegevens te beschermen.

Ook met betrekking tot de uitvoering van de AVG zijn de afdelingsmanagers zelf verantwoordelijk. De Functionaris Gegevensbescherming (FG) kan samen met de Privacy Officer(s) adviseren en toetst onder andere op de naleving. In Bijlage V zijn de belangrijkste aandachtsgebieden van de AVG beschreven.

In het eerder beschreven managementverantwoordingsdocument (zie par. 2.3.3) kunnen afspraken,

[10] BRP is de Basis Registratie Personen, PNIK is Paspoort en Nederlandse Identiteitskaarten, BAG is wet basisregistratie adressen en gebouwen, BGT is Wet basisregistratie grootschalige topografie, BRO is wet basisregistratie ondergrond, SUWI is Structuur Uitvoeringsorganisatie Werk en Inkomen.

maatregelen en risico's afwegingen op AVG-gebied door de afdelingsmanager in samenspraak met de FG en CISO worden opgenomen. Elke afdelingsmanager legt AVG-verantwoording af te leggen aan het bestuur van elke individuele DUO-organisatie. Dit heeft te maken dat juridisch elke organisatie afzonderlijk verantwoordelijk is voor een juiste invulling van de AVG.

2.10 Logging

Het gebruik van informatiesystemen, alsmede uitzonderingen en informatiebeveiligingsincidenten, worden vastgelegd in logbestanden op een manier die in overeenstemming is met het risico, en zodanig dat tenminste wordt voldaan aan alle relevante wettelijke eisen.

2.11 Informatieveiligheidsanalyse

Op basis van dit document, welke door de colleges van B en W van de DUO gemeenten worden vastgesteld, werkt de directeur Duo+ in samenwerking met de CISO het meer "operationele Informatieveiligheidsbeleid" en de AVG-planning verder uit. Directieberaad Duo+ en Bestuur Duo+ zien toe op haalbaarheid van de voorgestelde instrumenten, voor alle onderdelen van de DUO organisatie en coherentie met overige afspraken, welke intern en extern gericht kunnen zijn.

De kernelementen in het operationele informatieveiligheidsbeleid zijn de uitwerkingen van de volgende onderwerpen:

- Beveiligingsaspecten ten aanzien van personeel
- Fysieke beveiliging
- Beheer van communicatie- en bedieningsprocessen
- Logische toegangsbeveiliging
- Verwerving, ontwikkeling en onderhoud van systemen
- Beveiligingsincidenten
- Continuïteitsbeheer
- Naleving

De kernelementen in de informatieveiligheidsanalyse zijn:

- Beschrijving van het huidige niveau van Informatieveiligheid en de mate waarin aan de beveiligingseisen en -prioriteiten uit de betrokken Informatiebeveiligingsdocumenten en aan alle onderdelen van de informatieveiligheidsanalyse wordt voldaan. Recente ontwikkelingen worden ook beschreven, zoals het in productie nemen van een nieuw informatiesysteem of technische infrastructuur die gevolgen kunnen hebben voor het beveiligingsniveau.
- Voor het bepalen van afhankelijkheden en risico's is een analyse verricht ten aanzien van de bedrijfsprocessen ten opzichte van de ICT-omgeving. Naar aanleiding van deze analyse zijn minimaal de volgende aandachtspunten voor het plan onderkend:
    - Risico's die onvoldoende af te dekken zijn door maatregelen.
    - Risico's die zijn gerelateerd aan de kritische bedrijfsprocessen en/of (informatie)systemen.
    - Een overzicht van verbeterpunten, aangevuld met een kostenaanduiding voor uitvoering en de wijze en termijn waarop zij uitgevoerd zullen worden.

2.12 Aanvullende maatregelen

2.12.1 Afwijkend beveiligingsniveau

Als uit de risicoanalyse en de daarbij horende dataclassificatie blijkt dat voor bepaalde gegevensverwerkingen een specifiek beveiligingsniveau is vereist of de Baseline Informatiebeveiliging

Overheid (BIO) /NIS2 deze adviseert, kunnen daarvoor aanvullende maatregelen worden getroffen. In bepaalde gevallen zal hiervoor toestemming gevraagd worden aan het college van B en W.

2.12.2 Persoonsgegevens

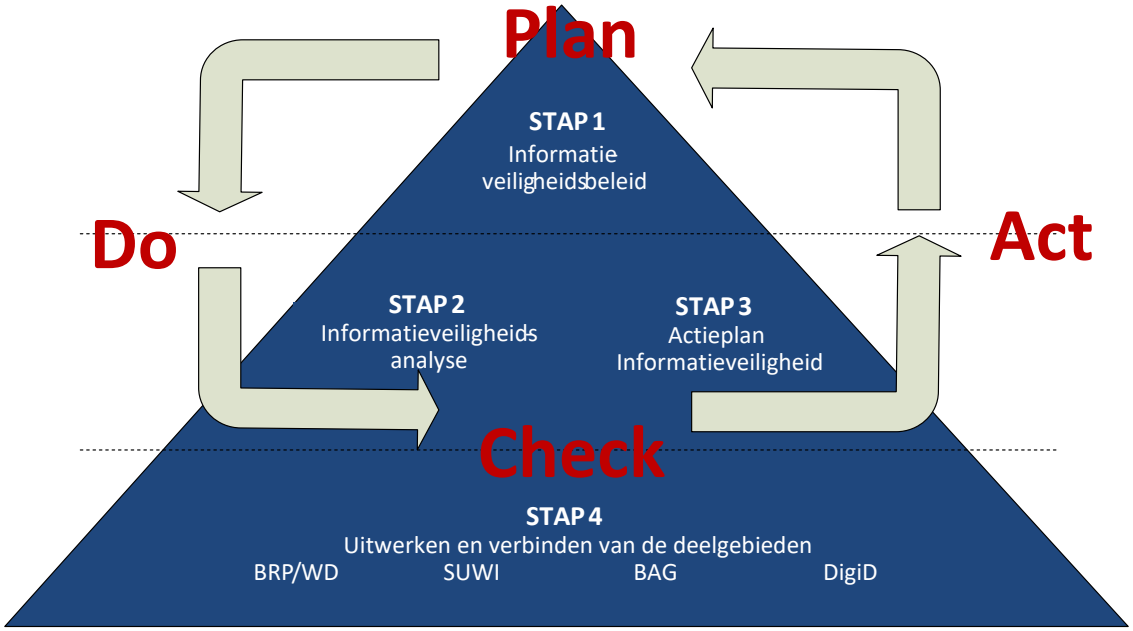
Bij de verwerking van persoonsgegevens zijn ook aanvullende maatregelen vereist, dit is afhankelijk van welke categorie persoonsgegevens het betreft en op basis van de Algemene verordening gegevens-bescherming (AVG) er technische of organisatorische maatregelen genomen moeten worden.

2.13 Borging van het informatieveiligheidsbeleid

Om borging van het informatieveiligheidsbeleid en de daarvan afgeleide plannen te realiseren, wordt naast een toebedeling van rollen (zie hoofdstuk Organisatie, taken & verantwoordelijkheden), onderstaande Plan, Do, Check, Act (PDCA)-cyclus doorlopen. Alhoewel altijd tussentijds documenten kunnen worden bijgesteld, worden onderstaande uitgangspunten gehanteerd voor het doorlopen van de PDCA-cyclus (zie Figuur 3):

1. **Informatieveiligheidsbeleid (zowel korte als lange termijn):** bevat het informatieveiligheidsbeleid en de visie op Informatieveiligheid. Bijstelling van het informatieveiligheidsbeleid vindt plaats rond een cyclus van 3 of 4 jaar. Indien zich grote wijzigingen voordoen vindt actualisatie eerder plaats.
2. **Informatieveiligheidsanalyse:** bevat de risicoanalyse (de toets aan de praktijk) op basis van informatieveiligheidsbeleid en de normen die hierin zijn vermeld of de normen waar in het beleid naar wordt gerefereerd. Bijstelling van de informatieveiligheidsanalyse vindt plaats na 1 tot 2 jaar.
3. **Actieplan Informatieveiligheid**: bevat de concrete geprioriteerde acties volgend uit de informatieveiligheidsanalyse (GAP). De CISO /team Informatieveiligheid en privacy (FG en PO's) in samenwerking met Team I&A, middels de Senior Informatie adviseur, komt bij elkaar om de implementatie van het "Jaarplan" te monitoren.

In de jaarrekening van de Duo+ organisatie wordt gerapporteerd over het doorlopen van de beschreven cyclus met betrekking tot Informatieveiligheid. Ook aan de DUO-gemeenten wordt een rapportage opgeleverd die kan worden overgenomen in de jaarstukken.



Figuur 3 De informatieveiligheidspiramide met PDCA-cirkel

2.14 Eenduidige Normatiek Single Information Audit (ENSIA)

Elke DUO-gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek. Deze zelfevaluatie wordt gedaan aan de hand van de Eenduidige Normatiek Single Information Audit (ENSIA). De ENSIA-coördinator zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de afdeling waar de vraag betrekking op heeft. Op die manier wordt men op de afdelingen bewust dat zij hierin ook een verantwoordelijkheid hebben.

De verantwoording over de informatiebeveiliging komt in het jaarverslag tot uitdrukking in de collegeverklaring Informatiebeveiliging. Met deze verklaring geeft het college van B en W aan in hoeverre de gemeente voldoet aan de afspraken die gemaakt zijn voor de ENSIA-verantwoording Informatiebeveiliging. Ook worden de eventuele verbetermaatregelen vermeld die de gemeente gaat treffen. De ingevulde zelfevaluatievragenlijst vormt de basis voor het opstellen van de collegeverklaring aan de raad.

Middels deze verantwoording wordt het bestuur van elke DUO-gemeente en de afzonderlijke gemeenteraden geïnformeerd. De betrokkenheid van het bestuur is essentieel, en laat zien dat de gemeente informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.

2.15 Uitgangspunten lange termijn informatiebeveiligingsbeleid

Het bestuur, de directie en de teammanagers van de DUO-organisaties spelen een cruciale rol bij het uitvoeren van dit meer langere termijn Informatiebeveiligingsbeleid. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente heeft, de risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis hiervan zet het management dit beleid voor informatiebeveiliging op, draagt dit uit naar de organisatie(s) en ondersteunt en bewaakt de uitvoering ervan.

De directie van de DUO-organisaties geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van

een informatiebeveiligingsbeleid van en voor de gehele DUO-organisaties. Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van de DUO-organisaties, gemeente en de relevante landelijke en Europese wet- en regelgeving.

2.15.1 Risk Management

De DUO-organisaties volgen een aanpak van Informatieveiligheid op basis van risicobeheersing. Het streven naar 100% veiligheid is niet het uitgangspunt, het uitgangspunt is optimale beveiliging van informatie. Het richt zich op de bescherming van informatie tegen bedreigingen en gaat in principe uit van de beantwoording van drie vragen:

1. Wat zijn voor ons de meest waardevolle processen, informatiesystemen en informatie?
2. Welke gebeurtenissen kunnen schade toebrengen aan deze waardevolle informatiesystemen en informatie?
3. Wat doen we wel en vooral ook niet om deze informatiesystemen en informatie te beschermen tegen deze gebeurtenissen?

Het informatiebeveiligingsrisico is de som van de kans op een beveiligingsincidenten en de impact daarvan: **risico = kans x impact**. Risicomanagement is een gestructureerde manier om risico's en gevolgen in kaart te brengen, te evalueren en proactief te beheersen door het treffen van maatregelen. Met een aanpak gebaseerd op risicobeheersing is de gemeente beter in staat om een evenwichtige set van veiligheidsmaatregelen te implementeren en om daarbij een betere afweging tussen kosten en noodzaak te maken. Dit zorgt ervoor dat informatiebeveiliging zo optimaal mogelijk ingericht kan worden. Minder maatregelen en meer focus leggen op grote risico's.

2.15.2 Lange termijn doelen

De langere termijn doelen van het informatiebeveiligingsbeleid zijn:

- Het managen van de informatiebeveiliging
- Adequate bescherming van bedrijfsmiddelen
- Het minimaliseren van risico's van menselijk gedrag
- Het voorkomen van ongeautoriseerde toegang
- Het garanderen van correcte en veilige informatievoorzieningen
- Het beheersen van de toegang tot informatiesystemen
- Het waarborgen van veilige informatiesystemen
- Het adequaat reageren op incidenten
- Het beschermen van kritieke bedrijfsprocessen
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers
- Het waarborgen van de naleving van dit beleid

2.15.3 Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van het beleid zijn:

- Alle informatie en informatiesystemen zijn van belang voor de DUO organisaties, bepaalde informatie is van vitaal en kritiek belang. Het college van B en W van elk afzonderlijke DUO-gemeente is eindverantwoordelijk voor de informatiebeveiliging.
- De uitvoering van de informatiebeveiliging en het om de juiste manier omgaan met persoonsgegevens is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de DUO organisaties hebben een interne eigenaar die de vertrouwelijkheid en/of waarde

bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.

- Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening en privacy verankerd binnen de DUO organisaties. Het informatiebeveiligingsbeleid vormt samen met de “Jaarplanning over Gegevensbescherming en Informatieveiligheid” het fundament onder een betrouwbare informatievoorziening. In de “Jaarplanning Gegevensbescherming en Informatieveiligheid” wordt de betrouwbaarheid van de informatievoorziening organisatie breed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
- Informatiebeveiliging en privacy is een continu verbeterproces. ‘Plan, do, check en act’ vormen samen het managementsysteem van informatiebeveiliging.
- De DUO-organisaties stelen de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid.
- Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld.
- Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.
- Continuïteit, bij continuïteitsbeheer gaat het om maatregelen die gericht zijn om langdurige onderbreking van bedrijfsactiviteiten bij de gemeente tegen te gaan en om kritische bedrijfsprocessen te beschermen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.
- Security by design, security maakt onderdeel uit van de processen en dient vanaf de beginfase betrokken te zijn.

2.15.4 Invulling van de uitgangspunten

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- Het DMT Duo+, gevolgd door het OGON Staf stelt als eerste dit geactualiseerde meerjarige ‘Informatiebeveiligingsbeleid DUO-organisaties 2025-2027’ vast.
- Vervolgens stelt elke afzonderlijke DUO-gemeente, het college van B en W als eindverantwoordelijke dit meerjarige ‘Informatiebeveiligingsbeleid DUO-organisaties 2025-2027’ vast.
- Dit Informatieveiligheidsbeleid betreft een actualisatie van het huidige beleid en hoeft daarom niet opnieuw aan de raad van de DUO-gemeenten te worden aangeboden.
- Uiteindelijk stelt het Dagelijks bestuur Duo+ ook nog het geactualiseerde ‘Informatieveiligheidsbeleid DUO-organisaties 2025-2027’ vast voor de Duo+ organisatie.
- Jaarlijks stelt de directie Duo+ in samenspraak met de betrokken afdelingen, de CISO en de FG een jaarplanning vast. Dit wordt apart vastgelegd.
- De directie Duo+ is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit Informatieveiligheidsbeleid.
- De directie Duo+ is verantwoordelijk voor het vragen om informatie bij de teammanagers en ziet erop toe dat de teammanagers adequate maatregelen genomen hebben voor de bescherming van de informatie die onder hun verantwoordelijkheid valt.
- De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan de directie Duo+, voorafgaand aan de P&C-gesprekken.
- Tijdens P&C-gesprekken dient er aandacht te zijn voor de informatiebeveiliging n.a.v. de rapportage van de CISO en FG. De onderwerpen, die als risicovol worden gezien, kunnen worden opgenomen in de auditplannen.

- De teammanagers zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- Hoewel de basiskernregistraties (zoals BRP, PUN, SUWI, BAG, BGT en BRO) en toekomstige basisregistraties belangrijk zijn in het kader van informatiebeveiliging, krijgen zij niet meer of minder voorrang dan andere (primaire) processen binnen de gemeente. Het samenspel van alle processen binnen de bedrijfsvoering is belangrijk voor de missie en de visie van de gemeente en het behalen van de doelen die zijn gesteld.
- Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures die voor hen van toepassing zijn.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere (bedrijf vertrouwelijke) informatie.
- Teammanagers dienen erop toe te zien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende ambtenaren de juiste persoonsgegevens ingezien en verwerkt hebben.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Teammanagers/leiders kunnen in samenwerking met het ‘Informatieveiligheidsteam’ (quick)scans doorlopen op het gebied van informatiebeveiliging om risico-afwegingen te kunnen maken.

2.15.5 Randvoorwaarden

Belangrijke randvoorwaarden zijn:

- De informatiebeveiliging maakt deel uit van afspraken met ketenpartners.
- Kennis en bewustzijn van informatiebeveiliging en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden (bewustwording).
- Jaarlijks wordt de “Jaarplanning voor Gegevensbescherming en Informatieveiligheid” opgesteld door de CISO /team Informatieveiligheid en privacy in samenwerking met Team I&A, middels Senior Informatie adviseur, gebaseerd op:
    - De uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA).
    - Het dreigingsbeeld gemeenten van de IBD.
    - Informatie uit incidenten, inbreuken op de beveiliging en bevindingen uit audits en (vulnerability) testen
    - De door de teammanagers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn.

3 Organisatie, taken & verantwoordelijkheden

Doelstelling: Het benoemen van het eigenaarschap van de bedrijfsprocessen met bijbehorende informatieprocessen en/of (informatie)systemen en het verankeren van de hieraan verbonden verantwoordelijkheden. Resultaat: Verankering in de organisatie van verantwoordelijkheden, taakomschrijvingen en coördinatie- en rapportagemechanismen met betrekking tot Informatieveiligheid.

3.1 Doel

Informatiebeveiliging vereist een governance structuur waarin rollen en verantwoordelijkheden op het gebied van Informatiebeveiliging zijn gedefinieerd. In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij de in de bedrijfsvoering bekende Three Lines of Defence (3LoD). In dit model is het lijnmanagement verantwoordelijk voor de eigen processen. De tweede lijn (CISO en FG) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering. Informatiebeveiliging is de verantwoordelijkheid van iedereen die voor de DUO-organisaties werkt. Onderstaand zijn een aantal rollen en verantwoordelijkheden verder uitgewerkt. Het is voornamelijk van belang de relatie tussen de verschillende rollen te verhelderen.

3.2 Verantwoordelijkheidsniveaus binnen Duo+

Binnen de Duo+ organisatie worden de volgende verantwoordelijkheids- en takenniveaus met betrekking tot Informatieveiligheid onderscheiden:

3.3 Beleidsbepalende, regisserende en coördinerende verantwoordelijkheden

Het bestuur van Duo+, bestaande uit de burgemeesters van de gemeenten Diemen, Uithoorn en Ouder-Amstel, alsook de directeur van Duo+, ziet toe op het houden van toezicht op alles wat Duo+ aangaat. Hieronder valt ook het Informatiebeveiligingsbeleid en de uitvoering daarvan.

De vaststelling en implementatie van de informatiebeveiligingsstructuur en de organisatie brede beleidsnormen vormen de verantwoordelijkheid van de drie afzonderlijke colleges van B&W van de DUO-gemeenten. Het is heel wel mogelijk, dat de Colleges medewerker(s) van Duo+ benoemen in functies die van belang zijn voor de eigen informatiebeveiligingsstructuur. Dit is een voordeel van de samenwerking op het gebied van bedrijfsvoering. Het werkt kwetsbaarheid verlagend, kwaliteit verhogend en kostenbesparend. De beveiligingsorganisatie werkt in één veiligheidsstructuur voor vier organisaties.

De directeur Duo+ is verantwoordelijk voor het inrichten van de beveiligingsorganisatie, met aan het hoofd de CISO. De CISO houdt onafhankelijk toezicht, rapporteert of de gewenste informatiebeveiligingsniveaus voor Duo+ en de DUO-gemeenten worden behaald. Dat leidt tot gevraagd en ongevraagd advies aan diverse gremia, waaronder de directeur Duo+ en indien het specifiek een van de drie gemeenten betreft ook de gemeentesecretaris van die desbetreffende gemeente.

Beveiligingseisen worden per proces vastgesteld. Elders zijn er afspraken gemaakt tussen Duo+ en de DUO-gemeenten over de verdeling van de processen en taakgebieden tussen hen. Deze verdeling is leidend voor de volgende stap: op voorhand, volgend op beleidskeuzes, wordt er voor ieder (bedrijfs-)proces een verantwoordelijke aangewezen, waarmee men ook de verantwoordelijke voor elke gegevens set en

informatiesysteem impliciet aanwijst. Deze lijn- of procesverantwoordelijken krijgen via de beveiligingsorganisatie best practices en hulpmiddelen aangeboden om de beveiligingseisen samen te stellen die bij het proces horen waarvoor zij verantwoordelijk zijn.

De directeur Duo+ heeft in ieder geval de volgende verantwoordelijkheden. Dit in overleg met het Directieberaad:

- Het stellen van operationele kaders en het geven van sturing ten aanzien van de veiligheid van informatie.
- Het sturen op risico's omtrent Informatieveiligheid.
- Periodiek evalueren van beleidskaders en deze bijstellen waar nodig.
- Het (laten) controleren of de getroffen veiligheidsmaatregelen overeenstemmen met de betrouwbaarheidseisen en of deze veiligheidsmaatregelen voldoende bescherming bieden.
- Het vastleggen van de verantwoordelijkheid voor informatieveiligheidscomponenten en -systemen.
- Het vastleggen van functiescheiding tussen uitvoerende, controlerende en beleidsbepalende taken met betrekking tot Informatieveiligheid.

3.4 Verantwoordelijkheden en taken van leidinggevenden

De leidinggevenden zijn verantwoordelijk voor de (informatie)veiligheid van de gegevenssets, informatieprocessen en -systemen binnen hun organisatie onderdeel/afdeling/team.

De leidinggevenden hebben in ieder geval de volgende verantwoordelijkheden*:*

- Het (laten) uitvoeren van maatregelen uit de informatieveiligheidsanalyse die op het organisatie onderdeel/afdeling/team van toepassing zijn.
- Op basis van een expliciete risicoafweging opstellen van betrouwbaarheidseisen voor de informatiesystemen.
- De keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen.
- Het sturen op beveiligingsbewustzijn, op bedrijfscontinuïteit en op naleving van regels en richtlijnen (gedrag en risicobewustzijn).
- Het aanwijzen van specialisten informatiebeveiliging en andere medewerkers binnen de beveiligingsorganisatie, wanneer classificatie van de gegevens set of het informatiesysteem daartoe aanleiding geeft.

3.5 Betrokken partijen

3.5.1 Het College van B&W en de gemeenteraad

Het College van B&W stelt formeel het informatiebeveiligingsbeleid vast en is bestuurlijk verantwoordelijk voor informatiebeveiliging binnen de gemeente. De burgemeester is de portefeuillehouder en is daarmee ook eindverantwoordelijk voor het goed beveiligen van de gemeentelijke informatie. Door middel van het hoofdstuk Informatieveiligheid in het jaarverslag en de uitkomsten van ENSIA in de collegeverklaring legt het College verantwoording af aan de gemeenteraad over Informatieveiligheid.

3.5.2 Directieteam en gemeentesecretaris

De gemeentesecretaris is binnen de gemeente ambtelijk eindverantwoordelijk voor de informatiebeveiliging. De directie belegt alle processen en systemen en de daarbij behorende middelen onder de verantwoordelijkheid van de teammanagers. De directie zorgt dat de teammanagers zich verantwoorden over de beveiliging van de informatie binnen hun scope. De directie zorgt dat de eindverantwoordelijke portefeuillehouders binnen het college gevraagd en ongevraagd geïnformeerd worden over de mate waarin

informatiebeveiliging een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het college zich ook verantwoorden naar de raad.

De directie stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. BBN 2 is het uitgangspunt voor gemeenten. De directie draagt zorg voor het uitwerken van tactische informatiebeveiligings-beleidsonderwerpen en laat zich hierin bijstaan door de CISO van de gemeente. De directie autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging wordt binnen de DUO-organisaties gezien als een integraal onderdeel van risicomanagement.

3.5.3 Teammanagers / -leiders

Informatiebeveiliging valt onder de verantwoordelijkheid van de teammanager voor wat betreft hun team, en hun processen en gegevensverzamelingen. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. De bedoeling is dat alle processen, systemen, data, applicaties altijd minimaal 1 eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. Teammanagers rapporteren aan de directie over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten. Afstemming met de teams over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp Informatiebeveiliging te bespreken in het directieberaad.

Taken van de teammanagers in het kader van informatiebeveiliging zijn:

- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het binnen de eigen afdeling uitdragen van het beveiligingsbeleid, en de daaraan gerelateerde procedures.
- Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Duiding van beveiligingsclassificaties van de processen en gegevensverzamelingen waar zij de proces- c.q. gegevenseigenaar zijn.
- Bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen. Voorbereiding en coördinatie van het overleg ligt bij de CISO.

3.5.4 Chief Information Security Officer (CISO)

De Chief Information Security Officer (CISO) is verantwoordelijk voor de organisatie van informatiebeveiliging. De CISO heeft als taak Informatieveiligheid op een hoger niveau te brengen en om het vervolgens structureel te laten borgen in de organisatie. De lijnorganisatie blijft zelf verantwoordelijk voor informatiebeveiliging. De belangrijkste bevoegdheid van de CISO is om op elke plek binnen de organisatie gevraagd en ongevraagd onderzoek te kunnen (laten) doen en zo nodig zaken voor te schrijven. Daarbij rapporteert de CISO periodiek over de gang van zaken. Onderstaand een aantal taken van de CISO ten aanzien van informatiebeveiliging:

- Rapporteert rechtstreeks voor reguliere zaken aan het afdelingshoofd Staf van de Duo+ organisatie en indien nodig rechtstreeks aan de Directeur Duo+ , daarnaast rechtstreeks aan de besturen van de DUO-gemeenten.
- Coördineert het formuleren van informatieveiligheidsbeleid.
- Stelt de informatieveiligheidsanalyse op en zorgt voor de actualisatie hiervan.
- Coördineert de prioritering van informatieveiligheidsmaatregelen uit de informatieveiligheidsanalyse en de uitvoering van het actieplan Informatieveiligheid.
- De periodieke toetsing op de juiste naleving, de werking, de effectiviteit en de kwaliteit van de maatregelen ten aanzien van Informatieveiligheid. De CISO is hiervoor verantwoordelijk, maar organiseert dit proces waar mogelijk met de inzet van (proces)eigenaar en specialisten informatiebeveiliging, verdeeld

over de vier organisaties. Het principe hierbij is dat de toetsing binnen een bepaald domein plaatsvindt door een (proces)eigenaar of specialist informatiebeveiliging van een ánder domein en visa versa.
- Stelt een plan op voor overleg en rapportage met betrekking tot Informatieveiligheid.
- Ondersteunt de directeur Duo+, de managementteams en besturen van de DUO-gemeenten, met kennis over Informatieveiligheid, zodat zij hun verantwoordelijkheid voor de betrouwbaarheid van de informatievoorziening juist kunnen invullen.
- Ondersteunt het management bij het opstellen van informatiebeveiligingsrapportages en beoordeelt deze rapportages.
- Periodiek rapporteren over de voortgang van de planning, status van informatiebeveiliging, incidenten en andere ontwikkelingen aan de portefeuillehouder(s) van de desbetreffende DUO-organisatie(s).
- Is aanspreekpunt voor medewerkers/teamleiders van de DUO-organisaties over het onderwerp Informatieveiligheid;
- Het inrichten van de informatiebeveiligingsorganisatie.
- Het uitvoeren van informatiebeveiligingsassessments.
- Het toezien op naleving van de eisen voor informatiebeveiliging.
- Het bevorderen van het informatiebeveiligingsbewustzijn over de hele organisatie.
- De voorbereiding op toekomstige informatiebeveiligingsrisico’s en ICT-beveiligingsrisico’s o.b.v. het dreigingsbeeld Nederlandse Gemeenten.
- Het coördineren en adviseren bij afhandelen van beveiligingsincidenten.
- Rapporteert over de Informatieveiligheid van de DUO-gemeenten in de documentatie van de P&C-cyclus.
- De controle op de voortgang van het uitvoeren van de maatregelen uit de informatieveiligheidsanalyse en actieplan Informatieveiligheid.
- De controle op de periodieke actualisatie van het informatieveiligheidsbeleid en de informatieveiligheidsanalyse.
- Toetsen/bewaken van het niveau van Informatieveiligheid.
- Toetsing van evaluatieproces van beveiligingsincidenten.
- Samen met de ENSIA-coördinator bewaakt en stuurt hij waar nodig bij in het ENSIA-verantwoordingsproces dat aan de DUO-gemeenten is opgelegd.
- Organiseert communicatie en voorlichting.
- Actief deelnemen in regionale overleggen van collega-CISO’s in de regio en of veiligheidsregio Amsterdam Amstelland.
- Neemt actief deel in overleggen met de (Cyber)burgermeester en de Veiligheidsregio Amsterdam Amstelland en Politie
- Neemt actief deel in het ambtelijk Subdriehoek Cyber-overleg van de gemeente Amsterdam, het Openbaar Ministerie, politie en DUO-gemeenten
- Onderhoudt actieve relaties bij de Informatieveiligheidsdienst (IBD) van de VNG

3.5.5 Functionaris Gegevensbescherming (FG)

De Functionaris Gegevensbescherming (FG) is ingesteld op grond van de Algemene Verordening Gegevensbescherming (AVG). De FG is een onafhankelijke toezichthouder met als hoofdtaak: erop toezien dat de DUO-organisaties de aan haar toevertrouwde persoonsgegevens in voldoende mate beschermt en beveiligt volgens de normen van de AVG. De taken van de FG zijn terug te vinden in de relevante artikelen uit de AVG en zijn onder andere:

- Informeren en adviseren over privacywet- en regelgeving;
- Toezien op de naleving van privacywet- en -regelgeving, inclusief het interne privacybeleid;
- Adviseren over en toezien op de uitvoering van Data Privacy Impact Assessments (DPIA’s);

- Fungeren als aanspreekpunt voor betrokkenen. Dit kunnen zowel inwoners van de DUO-gemeenten zijn, alsmede personeelsleden van de DUO-organisaties;
- Toezien op naleving van zowel de AVG, de WPG en andere wetten met betrekking tot gegevensbescherming als het beleid met betrekking tot de bescherming van persoonsgegevens van de verwerkingsverantwoordelijke of de (sub)verwerker. Hierbij hoort tevens toewijzing van verantwoordelijkheden, bewustmaking en opleiding van de bij de verwerking betrokken personeel en de betreffende audits. Desgevraagd adviseren omtrent gegevensbeschermingseffectbeoordeling en toezien op de uitvoering daarvan:
    - Verzorgen van meldingen en intrekkingen van meldingen bij de Autoriteit Persoonsgegevens (AP) tot de inwerkingtreding van de AVG;
    - Coördineren van verzoeken om inzage, correctie en verzet ten aanzien van persoonsgegevens en adviseren over de afhandeling;
    - Rapporteren aan de directeur Duo+ en indien het specifiek een van de drie gemeenten betreft ook de gemeentesecretaris van die desbetreffende gemeente;
    - Inrichten procedures voor het afhandelen van datalekken waarbij persoonsgegevens betrokken zijn;
    - Beheer en onderhoud van de standaarddocumenten voor verwerkersovereenkomsten, convenanten en reglementen;
    - Advisering en ondersteuning bij het besluitvormingsproces en het afsluiten van verwerkersovereenkomsten en convenanten en de vaststelling van reglementen.
- Optreden als aanspreekpunt voor en samenwerken met de Autoriteit Persoonsgegevens.

3.5.6 De teamleider Informatisering en Automatisering

Medewerkers van het team Informatisering & Automatisering (I&A), beheren voor de DUO-organisaties de werkplekken, serverplatformen, lokale netwerken, WiFi-verbindingen, externe netwerkverbindingen (zoals Gemnet en Suwinet) en verzorgt het technische (wijzigings-)beheer van databases, bedrijfsapplicaties en kantoorautomatiseringshulpmiddelen. Verder is zij medeverantwoordelijk voor alle technische aansluitingen op andere ketenpartners en landelijke voorzieningen en (implementatie van) cryptografie en bijbehorend sleutelbeheer (op ICT-gebied). Daarnaast zijn zij verantwoordelijk voor de implementatie van ICT-technische beveiligingsmaatregelen. Verantwoording over het gevoerde beheer van de getroffen beveiligingsmaatregelen wordt aan de verantwoordelijken voor (informatie)systemen afgelegd.

3.5.7 De teamleider Interne Dienstverlening Duo+

De teamleider Interne Dienstverlening (ID) is verantwoordelijk voor de fysieke veiligheid in en rond de gebouwen van de gemeenten Ouder-Amstel en Uithoorn. Zij draagt zorg voor fysieke toegangsbeveiliging, de kantoorinrichting (archiefkasten, kluizen, enzovoort) en contacten en contracten met externe partijen die voorzien in fysieke veiligheid, zoals alarmopvolging, bewaking en beveiliging. Daarnaast zorgt de teamleider ID ook het inplannen van capaciteit onder de medewerkers om te voldoen aan het Informatieveiligheidsbeleid, en het realiseren van voldoende formatie in de rol van beveiligingsbeheerder al naar gelang af te leiden is uit door de onderling afgesproken ambitie van betrokken organisaties.
Tenslotte is de Teamleider ID Duo+ ook verantwoordelijk voor alle binnenkomende poststromen (= informatie en informatieprocessen) en beheert alle (vertrouwelijke) archieven = informatie.

3.5.8 De Teamleider Gebouwen en Facilitaire Zaken van Diemen

De teamleider Gebouwen en Facilitaire Zaken is verantwoordelijk voor de fysieke veiligheid in en rond de gebouwen van de gemeente Diemen. Hij/zij draagt zorg voor fysieke toegangsbeveiliging, de kantoorinrichting (archiefkasten, kluizen, enzovoort) en contacten en contracten met externe partijen die voorzien in fysieke veiligheid, zoals alarmopvolging, bewaking en beveiliging. Tot zijn leidinggevende taken behoort ook het inplannen van capaciteit onder de medewerkers om te voldoen aan het Informatieveiligheidsbeleid, en het realiseren van voldoende formatie in de rol van specialist informatiebeveiliging al naar gelang af te leiden is uit door de organisatie vastgestelde ambitie.

3.5.9 De teamleider Personeel en Organisatie

De teamleider Personeel & Organisatie (P&O) is verantwoordelijk voor de personele en de organieke aspecten voor de DUO-organisaties en speelt hiermee een belangrijke adviesrol op het gebied van organisatie en informatieprocessen.

3.5.10 Team Informatieveiligheid en Privacy

Het team van Informatieveiligheid en Privacy binnen de Stafafdeling van Duo+ is verantwoordelijk voor signaleren, onderzoeken en in overleg opvoeren op de (jaar)planning, taken en verbeteractiviteiten. Dit kan bijvoorbeeld ook na het constateren van een datalek en/of beveiligingsincident. De samenstelling van het team kan variëren naar aanleiding van de benodigde expertise maar bestaat in principe uit de CISO, de ENSIA-coördinator en de Functionaris Gegevensbescherming. Deze kan indien van toepassing aangevuld worden met de specialisten informatiebeveiliging en of de Privacy Officer en mogelijk het afdelingshoofd Staf Duo+.

Onderwerpen:

- Voortgang uitvoering maatregelen uit de informatieveiligheidsanalyse c.q. uit het actieplan Informatieveiligheid
- Beveiligingsincidenten en of datalekken
- Planning en voorbereiding van controle, zelfevaluaties en audits
- Evaluatie en actualisatie informatieveiligheidsbeleid en de informatieveiligheidsanalyse
- Inspelen op veranderende beveiligingseisen of jurisprudentie

Daarnaast vindt indien nodig afstemming plaats tussen de CISO en de functioneel applicatie- en gegevensbeheerder(s) en de procesverantwoordelijke van (informatie)systemen.

De teams binnen de DUO-organisaties hebben sleutelpersonen als contactpersoon tussen hun team en team Informatieveiligheid en Privacy. In een zogenaamd ‘sleutelpersonenoverleg’ wordt informatie gedeeld tussen de teams en worden afspraken gemaakt met de sleutelpersonen binnen de DUO-organisaties en de teamleider/ afdelingshoofd van de desbetreffende afdeling in verband met de uitvoering van het informatieveiligheidsbeleid.

3.5.11 Privacy Officer (PO)

De Privacy Officer houdt zich dagelijks bezig met de uitvoering van het privacybeleid. De Privacy Officer brengt de verwerkingen van persoonsgegevens en de privacy risico’s hiervan in kaart, beoordeelt verwerkersovereenkomsten en convenanten over gegevensuitwisseling af en heeft een adviserende rol richting de organisatie. Ook neemt de Privacy Officer, samen met de FG en de CISO, deel aan het Privacy Informatiebeveiliging Team. Dit team komt bijeen bij een datalek en neemt maatregelen om deze te dichten en schade te voorkomen en te beperken. De CISO, PO en FG werken nauw met elkaar samen. Binnen de DUO-organisaties zijn op dit moment twee functies beschikbaar voor de Privacy Officer functie.

3.5.12 Specialist informatiebeveiliging per team

Een aantal teams heeft een specialist informatiebeveiliging als 'liaison' tussen hun team en Team Informatieveiligheid en Privacy. Deze verzorgt coördinatie en advies ten aanzien van de Informatieveiligheid van specifieke gegevensverzamelingen en de informatiesystemen die toegang tot en beheer van deze gegevens regelen. Er worden bijvoorbeeld specialisten aangewezen op verschillende aspecten van de bedrijfsvoering: Facilitaire Zaken, ICT (Automatisering), DIV (Archivering) en P&O.

De *specialist* is voor het toegewezen deelgebied verantwoordelijk voor het geheel van activiteiten gericht op de toepassing en naleving van de maatregelen en procedures die voortkomen uit het informatieveiligheids-beleid, inclusief de maatregelen die op de audit en zelfevaluatie onderdelen gelden.
Hieronder vallen:

- De voorbereiding en coördinatie (binnen hun team) van audits en (zelf)evaluaties.
- De preventie en detectie van beveiligingsincidenten en het geven van een adequate respons.
- Coördineren en toepassen van specifieke wet- en regelgeving.
- Rapporteren aan de CISO en de coördinator ENSIA.

3.5.13 De Gegevensbeheerders

De gegevensbeheerder is verantwoordelijk voor het geheel van activiteiten gericht op het ondersteunen van de informatiesystemen en de waarborging van continuïteit aan de gebruikerszijde van de informatie-voorziening en voor het geheel van activiteiten gericht op de inhoudelijke kwaliteitszorg betreffende het gegevens verzamelen, de gegevensverwerking en de informatievoorziening. Binnen de DUO-organisaties is deze verantwoordelijkheid ook belegd bij de teamleider I&A.

3.5.14 De Medewerkers

Alle medewerkers van de DUO-organisaties dragen verantwoordelijkheid voor de veiligheid van de activiteiten die behoren tot hun eigen functie en taken. Zij betrachten zorgvuldigheid en discipline bij het omgaan met informatie en (informatie)systemen. Zij zijn zich bewust van de eisen ten aanzien van de betrouwbaarheid, de integriteit, de beschikbaarheid en de controleerbaarheid van de informatieprocessen waarbij zij zijn betrokken.

3.6 Rapporteren beveiligingsincidenten en datalekken

De CISO wordt door de medewerkers van de DUO-organisaties geïnformeerd over beveiligingsincidenten en legt deze vast ten behoeve van rapportages. Hieronder vallen o.a. inbreuken op en (ver)storingen in de informatietechnologie, datacommunicatie of andere infrastructurele voorzieningen die gevolgen kunnen hebben voor de continuïteit en integriteit van de bedrijfsprocessen evenals signaleringen dat het informatieveiligheidsbeleid niet wordt nageleefd.

Indien een melding van een beveiligingsincident een (mogelijk) datalek melding blijkt te zijn, wordt de Functionaris Gegevensbescherming ingeschakeld en worden hierover ook de volgende data ten behoeve van rapportage geregistreerd.

- Datum melding datalek
- Naam organisatie / afdeling
- Melding bij de AP
- Doorlooptijd
- Reden van de melding
- Impact op betrokkenen

Per melding wordt er een informatie memo gemaakt welke aan verantwoordelijke organisatie en betrokken management wordt verstuurd. De Functionaris Gegevensbescherming levert de informatie aan bij de CISO.

I.v.m. NIS2, zal dit proces waarschijnlijk worden uitgebreid cf. wettelijke verplichtingen vanuit de Cyber-beveiligingswet wanneer deze van kracht wordt.

Gezamenlijk vindt er een terugkoppeling middels rapportage plaats over de beveiligingsincidenten en datalekken per kwartaal via de manager Staf van Duo+ aan het MT van Duo+ en ook aan de portefeuille Informatieveiligheid van elke DUO-gemeenten.

3.7 Controle en verantwoording

Dit meerjarige Informatieveiligheids beleid is een verantwoordelijkheid van het bestuur uitvoeringsorganisatie Duo+ en de DUO-gemeenten. De bestuurders en directie zullen volgens de 10 principes voor informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging en privacy door het geven van voorbeeldgedrag en het vragen om informatie. De directie is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan respectievelijke portefeuillehouders. De directie rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit meerjarige beleid.

3.8 Overlegvormen

Het regelmatig voeren van overleg over de lopende zaken voor privacy en informatiebeveiliging is noodzakelijk om de onderwerpen onder de aandacht te houden en de juiste richting te behouden. DUO-breed zijn overlegvormen ingericht, de afdelingen kunnen zelf hun eigen werkgroepen organiseren.

3.9 Afstemming met portefeuillehouder

DUO-breed vindt er een ambtelijke afstemming van beleid en uitvoering plaats van de CISO met de verantwoordelijke portefeuillehouder per DUO-gemeente. De voorstellen hierin worden afgestemd met de verantwoordelijke manager voor Informatieveiligheid en privacy, welk is belegd bij de afdeling Staf van de Duo+-organisatie.

3.10 ICT-crisisbeheersing (Business Continuity)

Voor interne crisisbeheersing dient een crisisteam Informatieveiligheid en privacy geïnstalleerd te zijn. Dit team komt uitsluitend bij elkaar in geval van grote incidenten of calamiteiten.

Dit team bestaat in ieder geval uit:

- De directeur Duo+ (voorzitter) en indien het specifiek een van de drie deelnemende gemeenten betreft ook de desbetreffende gemeentesecretaris
- De CISO
- De specialisten informatiebeveiliging ICT
- De verantwoordelijke specialisten informatiebeveiliging (afhankelijk van het incident of de calamiteit)
- Relevante experts (indien nodig), bijvoorbeeld de FG ingeval van betrokkenheid van persoonsgegevens
- Een lid van de afdeling communicatie (afhankelijk van het incident of de calamiteit)

De bovenstaande personen zullen eerst zelf bepalen wat de impact is van het incident of de calamiteit. Op basis van de mogelijke politieke gevolgen van het incident licht de directeur Duo+ de verantwoordelijke portefeuillehouder in.

In het kader van de NIS2 zal hiervoor een apart procedure op basis van Business Continuity Management (BCM) worden opgesteld ter aanvulling het op het huidige Draaiboek Gemeentelijk Actiecentrum crisisbeheersing van de DUO-organisaties.

3.11 Coordinated vulnerability disclosure / responsible disclosure

Het is denkbaar dat derden kwetsbaarheden vinden in applicaties die in gebruik zijn door de DUO-organisaties, zoals in iBurgerzaken of RX.Enterprise. De VNG Informatiebeveiligingsdienst heeft een handreiking Coordinated Vulnerability Disclosure gepubliceerd waar uitleg wordt gegeven over onder welke voorwaarden een melder kwetsbaarheden kan melden zonder bang te hoeven zijn dat er strafrechtelijke aangifte wordt gedaan bij (schijnbare) computervredebreuk. En waarbij toezeggingen worden gedaan over de snelheid waarbij wordt gereageerd op de melding.

De DUO-organisaties hebben hiertoe een beschrijving op hun websites. Waar het SaaS-systemen betreft, wordt tenzij anders besloten in overleg met de CISO verwezen naar de VNG Informatiebeveiligingsdienst.

Dit heeft verschillende redenen:

- Bij SaaS-applicaties zoals iBurgerzaken en RX.Enterprise gebeuren hosting, technisch beheer, en de softwareontwikkeling bij derde partijen. Kwetsbaarheden in deze aspecten kunnen we dan ook niet zelf oplossen. We hebben afspraken met de betreffende leveranciers, maar kunnen niet op voorhand zeker zijn van de oplostijden en hier dan naar derden ook geen beloften over doen.
- Dezelfde kwetsbaarheid zal ook gelden voor andere gemeenten, waarbij wij geen zicht hebben op wanneer de kwetsbaarheid bij hen is opgelost. Dit is aan de betreffende leverancier om te verifiëren. Het is van belang dat ook de IBD z.s.m. kennis heeft van mogelijke kwetsbaarheden.
- De DUO-organisaties maken gebruik van vele verschillende webapplicaties. Het is voor een (wellicht niet-Nederlandstalige) melder niet per se duidelijk of een kwetsbaarheid bijv. RX.Enterprise of onze MS Teams-omgeving betreft, allen gehost door derde partijen. Een vrijwaring door Duo+ om een bepaalde server ‘uit te proberen’ zal niet gelden voor een andere server, wat melders in een kwetsbare positie kan brengen.
- Het is vanzelfsprekend wel zaak dat een kwetsbaarhedenmelding zorgvuldig wordt opgepakt en afgehandeld. Ons bekendgemaakte kwetsbaarheden worden, zorgvuldig, gedeeld met de betreffende leverancier.

Daarbij worden de volgende uitgangspunten gehanteerd:

- Waar mogelijk wordt een externe melder (ook) doorverwezen naar de betreffende softwareleverancier zodat die direct kan schakelen met de melder.
- Z.s.m. de gemelde kwetsbaarheid intern registreren, melden bij de betreffende leverancier en het oplossen ervan bewaken;
- Afhankelijk van de kwetsbaarheid en daaruit volgende risico’s worden vervolgstappen besproken met de CISO (is het bijv. nodig om tijdelijk dienstverlening te staken?);
- Wij delen indien nodig de ontvangen melding met de Informatiebeveiligingsdienst voor gemeenten. Zo borgen wij dat gemeenten hun ervaringen op dit vlak met elkaar delen;
- De mogelijk gewenste privacy van de melder wordt gewaarborgd: indien de melder anoniem wil blijven zal Duo+ waar mogelijk waarborgen dat dit zo blijft.
- Uitgangspunt van de Duo+ Uitvoeringsorganisatie is dat, zolang de melder zich conformeert aan eigenschappen van een Coordinated vulnerability disclosure zoals gehanteerd in de handreiking CVD van de Informatiebeveiligingsdienst, de Duo+ Uitvoeringsorganisatie geen strafrechtelijke aangifte tegen melders zal doen en ook geen civielrechtelijke zaak tegen hen zal starten.

Bovengenoemde uitgangspunten zijn van toepassing op alle webapplicaties en websites / domeinen in gebruik bij de DUO-organisaties.

3.12 Verantwoordelijkheden afdelingsoverstijgende (informatie)systemen

De afdelingsoverstijgende (informatie)systemen binnen de DUO organisaties worden onder de verantwoordelijkheid van Duo+ gefaciliteerd en onderhouden. Deze systemen, die door meer dan één organisatieonderdeel worden gebruikt, bevatten gegevens die door meerdere organisatieonderdelen worden vastgelegd. De procesverantwoordelijke van een afdelingsoverstijgend (informatie)systeem draagt er zorg voor dat bij het gebruik ervan de wettelijke eisen en de gemeentelijke voorschriften worden nageleefd en dat de verantwoordelijkheden voor beveiliging voor alle betrokken partijen duidelijk omschreven zijn. De procesverantwoordelijke maakt schriftelijk afspraken met het onderdeel van de bedrijfsvoeringsorganisatie Duo+, het organisatieonderdeel of de externe organisatie dat van het afdelingsoverstijgend (informatie)systeem gebruik maakt (de gebruikende partij).

Minimaal worden in deze afspraken vastgelegd:

- Voorwaarden voor het toegestane gebruik van het afdelingsoverstijgend (informatie)systeem.
- De verantwoordelijkheden van de gebruikende partij binnen zijn organisatieonderdeel voor de gegevens uit het afdelingsoverstijgend (informatie)systeem.
- Voorwaarden met betrekking tot de bescherming van het verwerken van persoonsgegevens.
- Voorwaarden die de gebruikende partij verplichten voorzieningen te treffen voor een passend niveau van Informatieveiligheid.
- Procedure(s) betreffende autorisatie van medewerkers.
- Procedure(s) betreffende toezicht op de naleving van de afspraken en oplossing van eventuele geschillen.
- Het recht op inzage in de resultaten van de externe audits en zelfevaluaties bij de gebruikende partij waaruit blijkt in welke mate deze aan het informatieveiligheidsbeleid voldoet.

3.13 Contracten met derden

3.13.1 Servicelevel agreement (niveau van dienstverlening)

Bij structurele / langdurige ondersteuning en of uitbesteding van beheer van (een deel van) de (informatie)systemen, netwerken, en/of werkstations of hosting van de website(s) wordt tussen Duo+ en de externe partij een Service Level Agreement (SLA) afgesloten. Hierin staan afspraken over het niveau van Informatieveiligheid en een duidelijke definitie van de verantwoordelijkheden op het gebied van Informatieveiligheid. In het uitbestedingscontract wordt verwezen naar de SLA.

3.13.2 (ICT-)overeenkomsten met een derde partij

Bij het aangaan van overeenkomsten met derde partijen gelden de volgende beveiligingseisen:

- De maatregelen behorend bij par. 3.13 zijn voorafgaand aan het ingaan van het contract gedefinieerd en geïmplementeerd.
- Uitbesteding (ontwikkelen en aanpassen) van software is geregeld volgens formele contracten waarin
- o.a. intellectueel eigendom, kwaliteitsaspecten, beveiligingsaspecten, aansprakelijkheid, escrow en reviews geregeld worden.
- In contracten met externe partijen is vastgelegd hoe men om dient te gaan met wijzigingen en hoe ervoor gezorgd wordt dat de beveiliging niet wordt aangetast door de wijzigingen.
- In contracten met externe partijen is vastgelegd hoe wordt omgegaan met geheimhouding en de geheimhoudingsverklaring.

- Er is een plan voor beëindiging van de ingehuurde diensten waarin aandacht wordt besteed aan beschikbaarheid, vertrouwelijkheid, integriteit en controleerbaarheid.
- In contracten met externe partijen is vastgelegd hoe escalaties en aansprakelijkheid geregeld zijn.
- Als er gebruikt gemaakt wordt van onderaannemers dan gelden daar dezelfde beveiligingseisen voor als voor de contractant. De hoofdaannemer is verantwoordelijk voor de borging bij de onderaannemer van de gemaakte afspraken.
- De producten, diensten en daarbij geldende randvoorwaarden, rapporten en registraties die door een derde partij worden geleverd, worden beoordeeld op het nakomen van de afspraken in de overeenkomst. Verbeteracties worden geïnitieerd wanneer onder het afgesproken niveau wordt gepresteerd.

3.13.3 Verwerkers van persoonsgegevens

De algemene verordening gegevensbescherming (AVG) stelt regels voor het opslaan, verzamelen, vernietigen, verstrekken en combineren (kort gezegd: het verwerken) van persoonsgegevens. Wanneer een partij het verwerken van persoonsgegevens bij een andere partij uitbesteedt noemt men deze andere partij ‘een verwerker’. De DUO-organisaties zijn verplicht in een register vast te leggen welke derden persoonsgegevens worden verwerkt. Ook wordt vastgelegd of een verwerkersovereenkomst nodig is in de relatie tot die andere partij. In een verwerkersovereenkomst leggen de partijen onder andere vast voor welke doeleinden de gegevens verwerkt mogen worden, welke vormen van toezicht de eigenaar van de gegevens mag uitoefenen en hoe het zit met de onderlinge aansprakelijkheid.

3.13.4 Toegang derden tot systemen

Bij toegang van derden tot de ICT-voorzieningen gelden in principe de onderstaande uitgangspunten:

- Informatieveiligheid is (op basis van een risicoafweging) meegewogen bij het besluit een externe partij wel of niet in te schakelen.
- Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald welke toegang (fysiek, netwerk of tot gegevens) de externe partij(en) moet(en) hebben om de in het contract overeen te komen opdracht uit te voeren en welke noodzakelijke beveiligingsmaatregelen hiervoor nodig zijn.
- Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald welke waarde en gevoeligheid de informatie heeft waarmee de derde partij in aanraking kan komen en of hierbij eventueel aanvullende beveiligingsmaatregelen nodig zijn.
- Voorafgaand aan het afsluiten van een contract voor uitbesteding en externe inhuur is bepaald hoe geauthentiseerde en geautoriseerde toegang vastgesteld wordt.
- Voorafgaand aan het afsluiten van een contract voor uitbesteding en externe inhuur is bepaald wat de duur is van het contract.
- Indien externe partijen systemen beheren waarin persoonsgegevens verwerkt worden, wordt een aanvullende verwerkersovereenkomst (conform de AVG) in relatie tot het contract afgesloten.
- Er is in contracten met externe partijen vastgelegd welke beveiligingsmaatregelen vereist zijn, dat deze door de externe partij zijn getroffen en worden nageleefd en dat beveiligingsincidenten onmiddellijk worden gerapporteerd.
- Ook wordt beschreven hoe die beveiligingsmaatregelen door de uitbestedende partij te controleren zijn (bijv. audits, penetratietests en geheimhoudingverklaringen / VOG) en hoe het toezicht is geregeld.
- Over het naleven van de afspraken van de externe partij wordt jaarlijks gerapporteerd.
- In beginsel wordt de reguliere indienstprocedure gevolgd v.w.b. de informatiebeveiligingsaspecten.

3.13.5 Specialistische Inhuur derden

Soms is het nodig om voor een beheer-account aan te maken voor medewerkers van een van onze softwareleveranciers of consultants. Dit om dan toegang te krijgen tot een van onze applicaties waar we

ondersteuning vragen voor bijv. ICT-verstoringen en -calamiteiten, inrichting, beheer, ondersteuning, troubleshooting. Soms kan dit door direct in de betreffende applicatie een account te maken maar steeds vaker zal een EntraID-account nodig zijn waar inloggen tot de te benaderen applicatie gebeurt via single sign on. En wegens die single sign on heeft dan de leverancier een Duo+-account nodig om te kunnen inloggen, ook waar het de SaaS-leverancier zelf betreft voor door hen gehoste en technisch beheerde software.
Waar een normale 'indienstprocedure' gevolgd kan worden, dient dit te gebeuren: aanvraag door gemachtigde voor 1 account op naam, VOG-verklaring, etc.

Echter zullen er gevallen zijn waar dit niet werkbaar is. Doordat er steeds andere mensen bij de leverancier werk voor ons uitvoeren, of bijv. doordat de betreffende leverancier uit privacy-oogpunt niet bereid is VOG-verklaringen voor al hun medewerkers te overleggen die potentieel een keer werk voor ons uitvoeren.
Voor die categorie geldt in overleg met de CISO (en indien aan de orde advies van de betreffende specialist informatiebeveiliging) een afwijkende procedure: het verschaffen van 'maatwerk'-toegang tot een Duo+-applicatie t.b.v. beheer / ondersteuning op afstand. Dit kan voor projectmatige wijzigingen en/of voor reguliere ondersteuning op afstand.

De externe werkt onder verantwoordelijkheid van de verantwoordelijk leidinggevende welk dient te waarborgen dat activiteiten binnen het kader van het informatieveiligheidsbeleid worden uitgevoerd.

4 Inventarisatie en beheer van informatie en bedrijfsmiddelen

4.1 Inleiding

Doelstelling: Het bepalen, handhaven en waarborgen van het juiste beveiligingsniveau voor informatie, (informatie) systemen en bedrijfsmiddelen. Resultaat: Een goed overzicht van alle ICT-componenten en andere relevante bedrijfsmiddelen en een toegewezen eigenaarschap. Een informatieclassificatiesysteem waarmee de behoefte, de prioriteit en de mate van beveiliging kan worden bepaald.

4.2 Inventarisatie van informatie en (informatie) bedrijfsmiddelen

Om een passend beveiligingsniveau te kunnen bieden, moeten de informatie en de bedrijfsmiddelen worden geïnventariseerd en de waarde en het belang ervan worden vastgelegd.

Duo+ houdt een registratie bij van alle bedrijfsmiddelen die verband houden met (informatie) systemen (configuratiemanagement):

- Informatie (bijvoorbeeld databases, gegevensbestanden, documentatie en procedurebeschrijvingen).
- Programmatuur (bijvoorbeeld systeemprogrammatuur en standaardsoftware inclusief versiebeheer), incl. SaaS-programmatuur.
- Fysieke bedrijfsmiddelen (bijvoorbeeld apparatuur, schijven, accommodatie en netwerkinfrastructuur en actieve componenten).
- Diensten (bijvoorbeeld communicatiediensten, PKI-diensten, energievoorziening ten behoeve van de informatievoorziening).

In de registratie is opgenomen waar de gegevens(bestanden) zijn opgeslagen, op welke computers de programmatuur draait, van welke componenten daarbij gebruik wordt gemaakt en wie de proces-verantwoordelijken en beheerders zijn.

Duo+ houdt een registratie bij van alle fysieke voorzieningen die verband houden met (informatie-)veiligheid van ruimten, gebouw(en) en de directe omgeving van de gemeentekantoren.

4.3 Eigendom van informatie en bedrijfsmiddelen

Alle informatie en bedrijfsmiddelen die verband houden met ICT-voorzieningen behoren een eigenaar te hebben in de vorm van een aangewezen deel van de organisatie. Voor elk bedrijfsproces, applicatie, gegevensverzameling en ICT-faciliteit is een verantwoordelijk leidinggevende benoemd. Dit kan een ook een medewerker buiten Duo+ zijn, wanneer deze als lijnverantwoordelijke is aangewezen door het bevoegd bestuur.

4.4 Aanvaardbaar gebruik van bedrijfsmiddelen

Er zijn regels (o.a. op Intercomm alsook vastgelegd in CAR/UWO) vastgesteld, gedocumenteerd en geïmplementeerd voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met ICT-voorzieningen en informatieprocessen. Hieronder volgen de geldende uitgangspunten:

- Apparatuur en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen.

- De verantwoordelijkheid voor specifieke beheersmaatregelen mag door de eigenaar worden gemandateerd, maar de eigenaar blijft verantwoordelijk voor een goede bescherming van de bedrijfsmiddelen.
- Medewerkers dienen bij het gebruik van ICT-middelen, social media en geclassificeerde informatie de nodige zorgvuldigheid te betrachten en de integriteit en goede naam van de DUO-organisaties te waarborgen.
- Medewerkers gebruiken geclassificeerde informatie uitsluitend voor het uitvoeren van de aan hen opgedragen taken en het doel waarvoor de informatie is verstrekt.
- Privégebruik van geclassificeerde informatie en bestanden is niet toegestaan.
- Voor het werken op afstand en het gebruik van privémiddelen worden nadere regels opgesteld. De medewerker is gehouden aan regels zoals:
    - Illegale software, of niet goedgekeurde software mag niet worden gebruikt voor de uitvoering van het werk;
    - Er bestaat geen plicht het eigen device te beveiligen, maar de geclassificeerde informatie daarop wel;
    - Het verbod op ongewenst gebruik in de (fysieke) kantooromgeving geldt ook als dat via de eigen computer plaatsvindt.
- De medewerker neemt passende technische en organisatorische maatregelen om geclassificeerde informatie te beveiligen tegen verlies of tegen enige vorm van onrechtmatig gebruik. De medewerker houdt hierbij in ieder geval rekening met:
    - De beveiligingsclassificatie van de informatie;
    - De door Duo+ gestelde beveiligingsvoorschriften (o.a. dit informatieveiligheidsbeleid)
    - Aan de werkplek verbonden risico’s;
    - Het risico door het benaderen van geclassificeerde informatie met andere dan door de Duo+ verstrekte of goedgekeurde ICT-apparatuur

5 Assessment bij gebruik van DigiD-aansluitingen

5.1 Inleiding

Digitale persoonsidentificatie (DigiD) is een authenticatiemiddel dat wordt ingezet voor onze digitale dienstverlening. Dit is een veilig en betrouwbaar middel waarmee met zekerheid de identiteit van burgers bij gebruiker van digitale dienstverlening vastgesteld kan worden.

Het aanschaffen en onderhouden van een DigiD-aansluiting vergt veel inspanning. Daarnaast kost het geld en mensuren. Om zo efficiënt mogelijk te kunnen werken is het belangrijk dat de taken en verantwoordelijkheden bekend en belegd zijn. Ook behoeven de DigiD-aansluitingen veel aandacht voor de informatiebeveiliging hieromtrent.

Het doel van dit hoofdstuk is het kenbaar maken van de randvoorwaarden voor het aanvragen en behouden van een DigiD-aansluiting, en van de taken en verantwoordelijkheden voor desbetreffende DigiD-proceseigenaar.

5.2 DigiD-audit en Third Party Mededeling SaaS-diensten

Iedere onlinedienst die aangeboden wordt via DigiD, moet worden getoetst of het voldoet aan informatie-beveiligingsnormen. Via deze DigiD-audit houdt Logius (als toezichthouder DigiD) toezicht op veilig gebruik van de DigiD-aansluitingen. Het betreft een audit van de dienst die wordt aangeboden ‘achter’ DigiD-inlog, zoals het burgerloket.

Voor nieuwe aansluitingen dient binnen 2 maanden na aansluiting op de productieomgeving van DigiD het ICT-beveiligingsassessment-rapport worden aangeleverd bij Logius. Daarna dient de aansluiting jaarlijks geaudit te worden. Dit gebeurt binnen de DUO-organisaties door middel van de ENSIA-verantwoordingssystematiek.

Het DigiD Normenkader omschrijft de normen waaraan de DigiD-aansluiting moet voldoen. Op de website van Logius of NOREA zijn deze normen te vinden.

De Duo+ Uitvoeringsorganisatie gebruikt voor haar opdrachtgevers, de DUO-gemeenten (gemeenten Diemen, Ouder-Amstel en Uithoorn), veelal ‘cloud’- of SaaS-applicatie. Bij SaaS-applicaties valt een deel van de DigiD-omgeving en het beheer daarvan onder de betreffende leverancier (serviceorganisatie). De serviceorganisatie valt hierdoor binnen de scope van het DigiD-assessment. Daarom wordt een deel van de normen niet bij de aansluithouder maar bij de serviceorganisatie getoetst, of bij beide. Een serviceorganisatie dient voor zijn gedeelte van de DigiD-normen een DigiD-Assessment uit laten voeren en het resultaat daarvan ter beschikking stellen aan de DigiD-aansluithouder in de vorm van een ‘Third Party Mededeling’ (TPM, een verklaring van een onafhankelijke derde auditpartij). Het leveren van de TPM dient te worden meegenomen in de opdracht voor de leverancier.

5.3 Randvoorwaarden DigiD-aansluiting

1. Elke DigiD-aansluiting dient een proceseigenaar te hebben.
2. De proceseigenaar draagt zorg dat:
    a. De taken uit de volgende paragraaf, 5.4, goed geborgd zijn en worden nageleefd;
    b. Er wordt voldaan aan alle (actuele) Logius DigiD-normen;
    c. De beheertaken worden uitgevoerd door een functioneel- of applicatiebeheerder;
    d. De kosten (audits en uren) belegd zijn.

5.4 Taken en verantwoordelijkheden proceseigenaar

De DigiD-proceseigenaar is eindverantwoordelijk voor de DigiD-aansluiting. Dit betekent dat hij/zij zorg moet dragen en er (o.a. bij delegatie aan bijv. functioneel-/applicatiebeheer) op toe ziet dat er uitvoering wordt gegeven aan de volgende taken:

- Zorg dragen dat er wordt voldaan aan alle (actuele) Logius DigiD-normen (huidige versie norm ICT-beveiligingsassessments DigiD versie 3.0).
- Opstellen en onderhouden van contracten / afspraken met de leverancier(s)
    - Hoofdovereenkomst:
        - o.a. afspraken over informatiebeveiliging: ISO27001/ dataclassificatie;
        - Gemeente wordt geïnformeerd wanneer niet (meer) aan ISO27001/ dataclassificatie kan worden voldaan;
        - Tijdig aanleveren van een TPM (zonder extra kosten voor opdrachtgever);
        - Dat er geen kosten in rekening worden gebracht voor benodigde certificeringen
        - Van leverancier.
    - Service Level Agreement;
    - Verwerkersovereenkomst.
- Dataclassificatie (bijv. BBN2) moet bepaald worden d.m.v. een BIO-toets, zoals een Business Impact Assessment.
- Erop toezien dat gedurende de samenwerking de leverancier zich houdt aan de gemaakte afspraken.
- Dat er gedurende het hele jaar een functioneel-/applicatiebeheerder aanwezig is die zorgdraagt voor de borging van de normen. Waaronder tweemaal per jaar (geagendeerd) beoordeling of alle autorisaties compleet en actueel zijn; hierover wordt verslag (autorisatiematrix) gedaan richting verantwoordelijk leidinggevende.
- Dat er een functioneel-/applicatiebeheerder aanwezig is die verantwoording aflegt tijdens de DigiD-audit en de ENSIA-audit.
- Het auditdossier wordt jaarlijks aan de externe auditor beschikbaar gesteld en bevat tenminste de contracten en servicerapportages van onze SaaS-leverancier(s) (norm B.05), de incidentprocedure en een overzicht van de incidenten (U/WA.02), de dataclassificatie (U/WA.05), bewijs dat de webapplicatie gehardend is (U/NW.06, t.a.v. DNSSEC) en de beoordeelde releases (C.08). Waar aan de orde middels TPM.
- Dat er tijdig (uiterlijk medio okt) een TPM wordt opgeleverd door de leverancier(s) aan de proceseigenaar. De proceseigenaar c.q. een functioneel-/applicatiebeheerder levert de TPM intern aan bij de ENSIA-coördinator.
- Wanneer er niet voldaan wordt aan de DigiD-normen (TPM) dan dient de proceseigenaar contact op te nemen met de leverancier en dan zijn de volgende vragen relevant:
    - Wat is de reden voor het niet voldoen aan de norm(en)?
    - Kunnen we onze diensten achter DigiD nog veilig aanbieden?
    - Wat is het verbeterplan?
    - Wanneer kunnen wij een nieuwe (‘schone’) TPM verwachten?
- Wanneer er niet voldaan wordt aan de DigiD-normen (zoals aangetoond in de TPM) dan:
    - Moet door de proceseigenaar bestuurlijk verantwoording afgelegd worden aan de portefeuillehouder en bestuurlijk ENSIA-coördinator;
    - Moet door de proceseigenaar aan de bestuurlijk ENSIA-coördinator een verbeterplan aangeleverd worden;
    - Moet door de proceseigenaar erop toegezien worden dat de verbeteringen tijdig (binnen de afgesproken termijn) worden doorgevoerd.
- In geval dat de proceseigenaar de organisatie verlaat of van functie wisselt dan moet er bij de overdracht(document) duidelijk verwezen te worden naar de bovenstaande verantwoordelijkheden.

- Over de DigiD- en ENSIA-audits vindt horizontaal (van college aan de raad) en verticaal (naar Logius) verantwoording plaats.

6 Uitzonderingen op dit informatiebeveiligingsbeleid

Het zal voorkomen dat er niet volledig kan worden voldaan aan dit informatiebeveiligingsbeleid of het onderliggende beleid. Deze uitzonderingen kunnen mogelijk leiden tot een risico en dienen te worden beheerst. Uitzonderingen worden gemeld bij Team Informatieveiligheid en Privacy, dat zorgt voor een vastlegging en een inschatting van het risico. De CISO wordt geïnformeerd over de uitzonderingen.

7 Slot

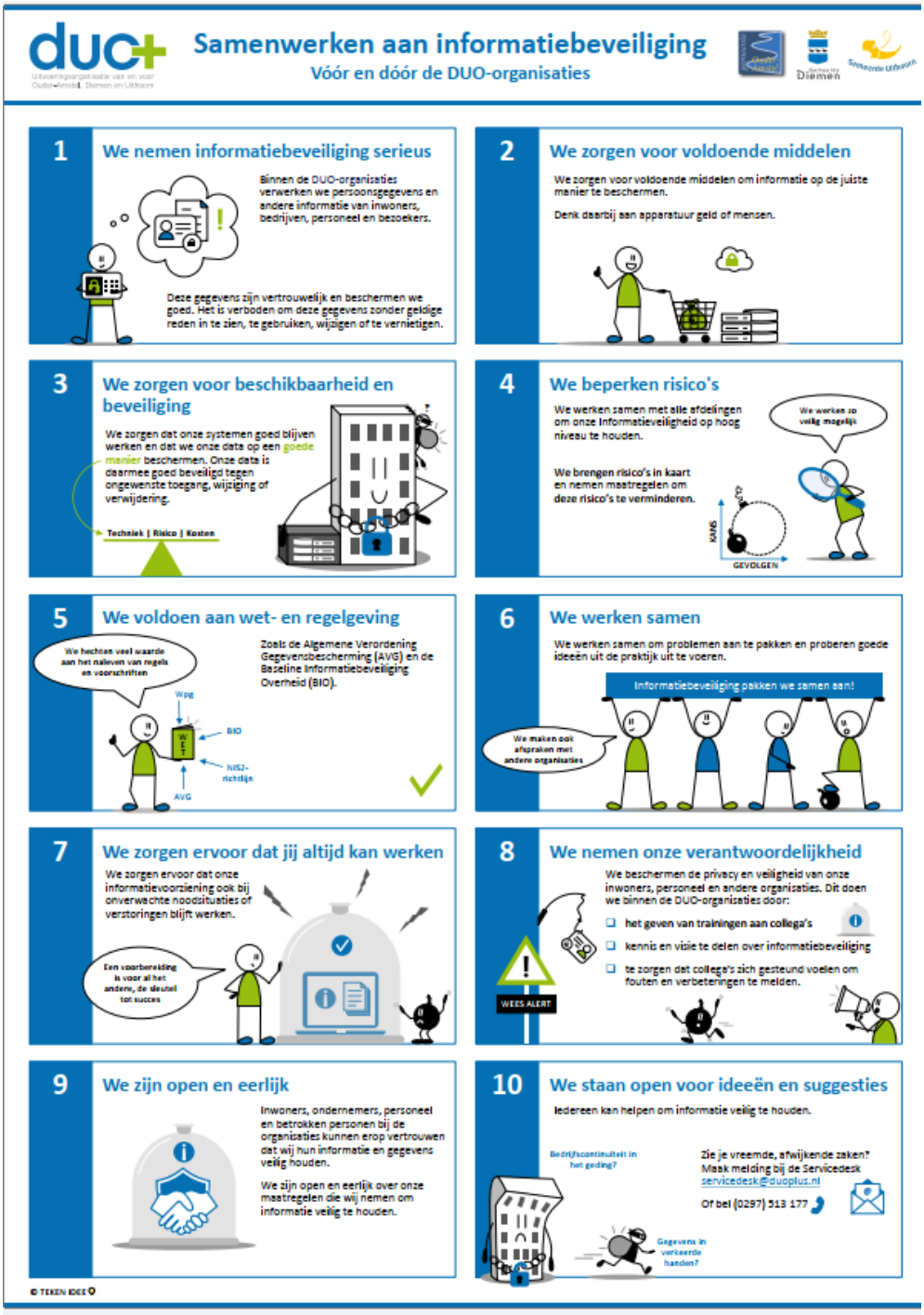
Dit informatiebeveiligingsbeleid zorgt ervoor dat de DUO-organisaties de komende jaren kunnen bouwen op het bestaande fundament dat in de afgelopen periode is neergezet. Dit beleid stelt de DUO-organisaties in staat om snel te acteren bij het opkomen van nieuwe bedreigingen. Burgers, bedrijven en personeel kunnen erop blijven vertrouwen dat hun gegevens veilig zijn.

Bijlage I. Huidige DigiD-aansluitingen

DigiD aansluiting	Eigenaar
1005371 voor Gemeente Diemen, digitaal loket (RX.Enterprise)	Directeur Duo+
1002510 voor Gemeente Diemen, burgerzaken	Teamleider Burgerzaken en Klant Contact Centrum Diemen
1005373 voor Gemeente Ouder-Amstel, digitaal loket	Directeur Duo+
1002514 voor Gemeente Ouder-Amstel, burgerzaken	Teamleider burgerzaken Duo+
1005379 voor Gemeente Uithoorn, digitaal loket	Directeur Duo+
1002516 voor Gemeente Uithoorn, burgerzaken	Teamleider burgerzaken Duo+

Indien er wijzigingen zijn van dit overzicht binnen de DUO-organisaties, zal een nieuwe lijst in een addendum op dit document worden vastgesteld en ondertekend. Zie ook hoofdstuk 5 voor de vereisten van een nieuwe DigiD-aansluiting.

Bijlage II. Visie op Informatieveiligheid in beeld



Figuur 4 Visie op Informatieveiligheid in beeld

Bijlage III. Overzicht BIO normenkader

Het BIO normenkader is onderverdeeld in een aantal aandachtsgebieden, deze zijn hieronder weergegeven. (nummering op basis van de BIO-indeling)

1. Informatiebeveiligingsbeleid
    a. Aansturing door de directie van de informatiebeveiliging
2. Organiseren van informatiebeveiliging
    a. Interne organisatie
    b. Mobiele apparatuur en telewerken
3. Veilig personeel
    a. Voorafgaand aan het dienstverband
    b. Tijdens het dienstverband
    c. Beëindiging en wijziging van het dienstverband
4. Beheer van bedrijfsmiddelen
    a. Verantwoordelijkheid voor bedrijfsmiddelen
    b. Informatieclassificatie
    c. Behandelen van media
5. Toegangsbeveiliging
    a. Bedrijfseisen voor toegangsbeveiliging
    b. Beheer van toegangsrechten van gebruikers
    c. Verantwoordelijkheden van gebruikers
    d. Toegangsbeveiliging van systeem en toepassing
6. Cryptografie
    a. Cryptografische maatregelen
7. Fysieke beveiliging en beveiliging van de omgeving
    a. Beveiligde gebieden
    b. Apparatuur
8. Beveiliging bedrijfsvoering
    a. Bedieningsprocedure en verantwoordelijkheden
    b. Bescherming tegen malware
    c. Back-up
    d. Verslaglegging en monitoring
    e. Beheersing van operationele software
    f. Beheer van technische kwetsbaarheden
    g. Overwegingen betreffende audits van informatiesystemen
9. Communicatiebeveiliging
    a. Beheer van netwerkbeveiliging
    b. Informatietransport
10. Acquisitie, ontwikkeling en onderhoud van informatiesystemen
    a. Beveiligingseisen voor informatiesystemen
    b. Beveiliging in ontwikkelings- en ondersteunende processen
    c. Testgegevens
11. Leveranciersrelaties
    a. Informatiebeveiliging in leveranciersrelaties
    b. Beheer van dienstverlening van leveranciers
12. Beheer van informatiebeveiligingsincidenten
    a. Beheer van informatiebeveiligingsincidenten en - verbeteringen
13. Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer
    a. Informatiebeveiliging continuïteit
    b. Redundante componenten
14. Naleving
    a. Naleving van wettelijke en contractuele eisen
    b. Informatiebeveiligingsbeoordelingen

Bijlage IV. Overzicht BIO-overheidsmaatregelen

Onderstaande betreft een indicatie / 'inhoudsopgave' van de BIO-normen. BIO versie 2.0 zal op afzienbare termijn van kracht worden. De meest courante versie van de BIO is te vinden op https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid/

BIO – Overheidsmaatregelen en relevante nummering	
BIO-nummer	Overheidsmaatregel
6.1.1.5	De CISO draagt zorg voor advies en uitleg over de BBN2+ eisen.
6.1.1.6	De CISO draagt zorg voor het beoordelen en vaststellen van beveiliging gerelateerde documenten zoals risicomanagement documentatie, beveiligingsplannen, beveiligingsarchitecturen, documenten met betrekking tot het testen/beoordelen van de beveiliging en gebruikersinstructies.
6.1.1.7	De Gemeente Secretaris draagt zorg voor het afgeven van toestemming tot ingebruikname voor de veilige verwerking van BBN2+-informatie, waarbij de voorwaarden waaronder de toestemming geldig is en de duur van de toestemming wordt opgenomen.
6.1.1.8	De CISO draagt zorg voor toezicht dat de beveiliging van het systeem in overeenstemming is met de eisen en afspraken, door audits, inspecties en beoordelingen.
6.1.1.9	De CISO draagt zorg voor het geven van aanwijzingen aan lijnmanagement, systeemontwikkelaars en dienstenleveranciers en/of de ICT-afdeling bij het onderzoeken van incidenten of vermoedens van incidenten.
6.1.1.10	De dienstenleverancier en/of de ICT-afdeling draagt zorg voor het opstellen en onderhouden van beveiligingsdocumentatie die door de CISO verlangd en gecontroleerd wordt ten behoeve van de toestemmingsverlening.
6.1.1.11	De Gemeentesecretaris zal de restrisico's die op basis van het risicomanagement geaccepteerd worden ook formeel accepteren. De restrisico's mogen niet afwijken van wat met de CISO overeen is gekomen.
6.1.1.12	De lijnmanager draagt zorg voor controles dat externe ontvangers van gegevensdragers beschikken over de juiste middelen om deze gegevensdragers in overeenstemming met de eisen kunnen opslaan en behandelen.
6.1.1.13	De lijnmanager draagt zorg voor controle op de logging.
6.1.1.14	De lijnmanager draagt zorg voor het periodiek testen of de maatregelen voor de bedrijfscontinuïteit adequaat werken.
6.1.1.15	De lijnmanager, dienstverlener en de CISO draagt zorg voor rapporteren over gevonden zwakten aan de Gemeentesecretaris.
6.1.1.16	Er is functiescheiding tussen systeembeheerderstaken en de beveiligingsrollen.
6.1.1.17	De lijnmanager zal, in samenspraak met de CISO systeemontwikkelaar en de dienstenleverancier en/of de ICT-afdeling, de eisen aan de beoordeling van de beveiliging vaststellen.
6.1.1.18	De lijnmanager, de dienstenleverancier en/of de ICT-afdeling en/of de systeemontwikkelaar houden de CISO tijdig op de hoogte van ontwikkelingen, zoals voorgenomen wijzigingen van het systeem, van de wijze waarop het systeem wordt ingezet en van wijzigingen in de belangen waarop het systeem betrekking heeft.
6.1.1.19	De lijnmanager zorgt ervoor dat alle beveiligingseisen van het informatiesysteem, ook die uit eventuele aanvullende risicoanalyses zijn vastgelegd.

7.1.1.2	Medewerkers met bijzondere bevoegdheden (bijvoorbeeld auditors en systeembeheerders) in een infrastructuur die bedoeld is voor de verwerking van BBN2+ informatie, beschikken over een VOG.
7.1.2.2	Medewerkers worden geïnformeerd over hun verantwoordelijkheden met betrekking tot de beschikbaarheid, de vertrouwelijkheid en de integriteit van informatie.
7.2.2.4	Medewerkers worden initieel en periodiek bewust gemaakt van de noodzaak om te voldoen aan beveiligingsvoorschriften en om te handelen in het belang van de veiligheid.
7.2.2.5	Medewerkers worden initieel en periodiek bewust gemaakt (door geschikte training en regelmatige bijscholing) van de onderkende dreigingen waaronder indien relevant: statelijke actoren/ondermijning/georganiseerde misdaad. Bijzondere aandacht wordt hierbij gegeven aan kwetsbaarheden en dreigingen met betrekking tot de gebruikte ICT-middelen.
7.2.2.6	Beveiligingsbewustzijn en instructie: In functionerings- en beoordelingsgesprekken wordt het individuele bewustzijn en gedrag besproken en de behoefte aan ondersteunende training.
7.3.1.4	Bij beëindiging van dienstverband, contract of overeenkomst of verandering van functie binnen de organisatie waarin kennis is genomen van BBN2+ informatie worden medewerkers aantoonbaar op de hoogte gesteld van hun verantwoordelijkheden ten aanzien van de geheimhouding van deze informatie. Dit wordt opgenomen in het personeelsdossier van de medewerker.
8.3.3.3	Fysieke verzending van BBN2+ informatie dient te geschieden met goedgekeurde middelen, waardoor de inhoud niet zichtbaar, niet kenbaar en inbreuk detecteerbaar is.
9.2.1.3	Er zijn alleen accounts toegestaan die te herleiden zijn naar natuurlijke personen. Systeemprocessen draaien onder een eigen gebruikersnaam (een functioneel account), voor zover deze processen handelingen verrichten voor andere systemen of gebruikers.
9.2.3.2	Het raadplegen van logbestanden is voorbehouden aan geautoriseerde gebruikers. Hierbij is de toegang beperkt tot leesrechten.
9.2.3.3	Logbestanden worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden.
9.2.3.4	De instellingen van logmechanismen worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden. Indien de instellingenaangepast moeten worden zal daarbij altijd het vier ogen principe toegepast worden.
9.2.3.5	Standaard gebruikers hebben een gebruikersaccounts (Tier 2), zonder beheerdersrechten.
9.3.1.3	Uitsluitend door de CISO geadviseerde wachtwoordkluizen zijn toegestaan.
9.3.1.4	Voorafgaand aan het aanmelden wordt aan de gebruiker een melding getoond dat alleen geautoriseerd gebruik is toegestaan voor expliciet door de organisatie vastgestelde doeleinden en de verantwoordelijkheid die de gebruiker als gevolg daarvan heeft.
9.4.1.3	Er wordt tijdens het inloggen geen extra informatie vrijgegeven die misbruikt kan worden door derden (bijv. geen aantal telbare sterretjes, leidend tot de lengte van het wachtwoord). Indien een fout tijdens het inloggen optreedt, zal het systeem niet aangeven welke gegevens juist of onjuist zijn (bijv. geen bevestiging gebruikersnaam, geen wachtwoordhints).
9.4.1.4	Het aantal sessies dat één gebruiker gelijktijdig kan hebben, is beperkt en wordt gemonitord op misbruik. Maak bij het aanmelden een nieuwe sessie aan en verbreek een eventueel al bestaande sessie van die gebruiker. Maak de oude sessie-identifier ongeldig.

9.4.1.5	Stel vast welke functies nodig zijn en schakel alle andere functies uit (minste functionaliteit). Deactiveer of verwijder (deïnstallatie) alle functies, protocollen, services en accounts op het ICT-component als die niet noodzakelijk zijn. Toets periodiek (eventueel automatisch) of de in productie zijnde ICT-componenten niet meer dan de vastgestelde noodzakelijke functies bieden (statusopname) en de geconstateerde afwijkingen worden hersteld.
9.4.3.6	De dienstenleverancier en/of de ICT-afdeling staat uitsluitend het gebruik van tijdelijke wachtwoorden toe voor de eerste keer inloggen en het resetten van een wachtwoord. Het ICT-systeem vereist dat het tijdelijke wachtwoord bij het eerste gebruik worden gewijzigd in een permanent wachtwoord wordt gewijzigd. Een tijdelijk wachtwoord heeft een zeer korte geldigheidsduur. Een tijdelijk wachtwoord is voor eenmalig gebruik. Initiële wachtwoorden worden alleen verstrekt als de identiteit van de gebruiker is vastgesteld.
9.4.3.7	De dienstenleverancier en/of de ICT-afdeling past hardening toe ter beveiliging van credential stores en -mechanismen.
9.4.3.8	Replay aanval op authenticatie en binnen een sessie wordt voorkomen.
9.4.3.9	Inactieve accounts worden na 90 dagen geblokkeerd.
9.4.4.3	Basic Input Output System (BIOS)/Unified Extensible Firmware Interface (UEFI) instellingen zijn niet toegankelijk voor eindgebruikers. Uitsluitend de noodzakelijke BIOS/UEFI features zijn geactiveerd. Het BIOS/UEFI systeem wordt gepatcht in overeenstemming met het patchbeleid. UEFI Secure Boot is geactiveerd, waar mogelijk.
10.1.1.3	Voor PKI-gebaseerde authenticatie zorgt de dienstenleverancier en/of de ICT-afdeling ervoor dat het ICT-systeem certificaten valideert door een certificaatpad naar een trust anchor op te zetten en te verifiëren, en dat het daarbij ook informatie over de certificaatstatus controleert.
10.1.1.4	Een token (bijvoorbeeld smartcard) wordt geblokkeerd indien de pincode of het wachtwoord vijf keer verkeerd wordt ingevoerd.
10.1.1.5	De dienstenleverancier en/of de ICT-afdeling voert voor natuurlijke personen het eerste PKI aanvraag- en uitgifteproces persoonlijk (d.w.z.: face to face) uit.
11.1.2.2	Fysieke beveiligingsmaatregelen moeten zo zijn ingericht dat ze: (a) heimelijke of geforceerde toegang van een indringer buitenhouden; (b) acties van wraakzuchtige en onbetrouwbare medewerkers ontmoedigen, belemmeren en detecteren; (c) het mogelijk maken dat ruimtes zodanig beschermd worden dat uitsluitend tot die gegevens geautoriseerde medewerkers toegang kunnen krijgen. (d) beveiligingsinbreuken zo snel mogelijk detecteren en erop reageren.
11.1.2.3	Fysieke toegang tot serverruimtes of datacenters waar BBN2+ informatie wordt opgeslagen of verwerkt, wordt gecontroleerd.
11.1.2.4	Toegang tot ruimtes/locaties/zones waarbinnen transport van onversleutelde BBN2+ informatie plaatsvindt, is beperkt en gecontroleerd.
11.1.2.5	Toegang tot ruimtes/locaties/zones waarbinnen zich voor het systeem noodzakelijke faciliteiten bevinden, is beperkt, geregistreerd en gecontroleerd.
11.1.2.6	Toegang tot ruimtes/locaties/zones waarbinnen zich centrale BBN2+ apparatuur bevindt, is uitsluitend toegankelijk voor medewerkers die beschikken over minimaal een VOG en op een autorisatielijst staan.
11.1.2.7	Het moet voorkomen worden dat bezoekers kennis kunnen nemen van BBN2+ informatie.
11.1.4.3	Uitsluitend door de CISO geadviseerde wijze waarop voor BBN2+ relevante facilitaire systemen (op afstand) worden gemonitord zijn toegestaan.
11.1.4.4	Bij brand, wateroverlast, koelingsproblemen en stroomstoring blijft de beveiliging van de BBN2+ informatie intact.

11.1.4.5	Het maken van audio- of video-opnames van BBN2+-informatie moet worden voorkomen.
11.2.1.4	ICT-middelen (ook kopieerapparaten, faxapparatuur) die toegang kunnen geven tot BBN2+ informatie worden op ten minste BBN2+ niveau beschermd.
11.2.1.5	De uitgifte en inname van fysieke sleutels van beveiligingsmiddelen verloopt overeenkomstig een vastgestelde en gedocumenteerde procedure en mogen het kantoorgebouw niet verlaten.
11.2.1.6	Uitsluitend door de CISO goedgekeurde KVM switches en andere randapparatuur die gedeeld worden onder verschillende omgevingen zijn toegestaan.
11.2.1.7	Apparatuur die ooit is gebruikt voor de opslag of verwerking van BBN2+ informatie (eigen apparatuur, apparatuur van dienstenleveranciers maar ook laptops van consultant of gehuurde ICT-middelen (waaronder kopieerapparaten en faxapparatuur) blijven binnen de organisatie. Uitsluitend als BBN2+ informatie is verwijderd met een door de CISO goedgekeurde methode is hergebruik van apparatuur buiten de organisatie toegestaan.
11.2.1.8	Externe medewerkers en ingehuurd personeel werken met BBN2+ informatie uitsluitend op door de gemeente verstrekte apparatuur. Indien dit niet mogelijk is dan kan er na overleg met de CISO van worden afgeweken.
11.2.9.6	Na een bepaalde periode van inactiviteit (zoals met de CISO overeengekomen) wordt een sessie vergrendeld waarbij alle informatie op het beeldscherm onleesbaar en ontoegankelijk wordt.
12.1.2.2	De dienstenleverancier en/of ICT-afdeling past softwarebescherming toe overeenkomstig vastgestelde en gedocumenteerde procedures van de organisatie.
12.1.2.3	De dienstenleverancier en/of ICT-afdeling past (veilig) onderhoud toe overeenkomstig vastgestelde en gedocumenteerde procedures van de organisatie.
12.2.1.6	De authenticiteit en integriteit van software, firmware, patches en security-updates is bij installatietechnisch geborgd.
12.3.1.7	Back-upstrategieën zijn vastgesteld op basis van de soort gegevens ((log)bestanden, databases, software, standaardconfiguraties, VM-templates, et cetera), de maximaal toegestane periode waarover gegevens verloren mogen raken, en de maximaal toelaatbare back-up- en hersteltijd.
12.3.1.8	Het back-up- en herstelproces wordt op basis van vastgestelde en gedocumenteerde procedures regelmatig getest op doelmatigheid. De frequentie wordt door de lijnmanager in overleg met de CISO, op basis van het risicoprofiel, bepaald en is in lijn met de back-upstrategie.
12.3.1.9	Back-ups worden zodanig opgeslagen dat bij een incident niet zowel het ICT-systeem als de back-ups worden getroffen.
12.4.1.7	Er zijn maatregelen getroffen die zeker stellen dat voldoende, complete en juiste (log)informatie beschikbaar is om gebeurtenissen zorgvuldig te analyseren (onderzoeken).

12.4.1.8	Onderstaande voorwaarden om onderzoek uit te kunnen voeren naar gebruikershandelingen en systeemactiviteiten zijn ingevuld: 1) Er is bepaald welke gebruikershandelingen, systeemactiviteiten, gebeurtenissen en/of beheeractiviteiten vastgelegd moeten worden. 2) Er is vastgelegd waar en hoe centralisering van logging is ingericht (inclusief configuratie-instellingen). 3) Er is een plan met daarin activiteiten die worden uitgevoerd (wie, wat en wanneer) indien logrecords op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet aan de gestelde eisen en/of verwachtingen hebben voldaan of tekortkomingen hebben opgeleverd. 4) De systemen zijn zodanig geconfigureerd dat interne systeemklokken automatisch gesynchroniseerd worden. 5) Er is bepaald wat te doen bij het uitvallen van loggingmechanismen (alternatieve paden). 6) Er zijn bewaartermijnen vastgesteld voor de loginformatie. 7) De loggegevens zijn beveiligd tegen achteraf wijzigen/verwijderen door onbevoegden.
12.4.1.9	ICT-systemen leggen ten minste het volgende vast: • authenticatiegebeurtenissen; • bestands- en objectgebeurtenissen; • export- (bijv. uploads) en importgebeurtenissen (bijv. downloads); • gebeurtenissen betreffende gebruikersaccounts; • gebeurtenissen betreffende accounts met speciale bevoegdheden.
12.4.1.10	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT-systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en over de bevindingen gerapporteerd. Om dit uit te kunnen voeren zijn onderstaande voorwaarde ingevuld: 1) De verschillende gelogde informatie wordt samengebracht voor analysedoeleinden. 2) De signaleringssystemen (detectie) maken tijdig melding van ongewenste gebeurtenissen (alarmeringen). 3) Er zijn procedures vastgelegd met daarin beschreven hoe en wanneer controles op logging moeten plaatsvinden en hoe taken op dit gebied belegd zijn. 4) Er is vastgelegd waar en hoe correlaties worden aangebracht (analyseren / auditing). 5) De geregistreerde menselijke en systeemacties worden periodiek geanalyseerd. 6) De ongebruikelijke situaties (incidenten) worden periodiek geanalyseerd. 7) De geanalyseerde en beoordeelde gelogde gegevens worden geconsolideerd en gerapporteerd naar het hoogste management.

Bijlage V. Aandachtsgebieden AVG

Hieronder zijn de aandachtsgebieden weergegeven welke de Algemene Verordening Gegevensbescherming (AVG) beschrijft.

1 **Governance – Het onderhouden van de bedrijfsstructuur (art 24, 27, 38, 39 AVG)**

1.1 Wijs verantwoordelijkheid(en) voor bescherming persoonsgegevens toe aan interne persoon

1.2 Betrek Senior Management bij bescherming persoonsgegevens

1.3 Benoem Functionaris voor de gegevensbescherming (FG)

1.4 Wijs verantwoordelijkheid privacy activiteiten toe aan medewerkers binnen de organisatie

1.5 Onderhoud rollen en verantwoordelijkheden van medewerkers, privacy officer en FG

1.6 Uitbrengen rapportage status bescherming persoonsgegevens

1.7 Uitvoeren bedrijfsrisicobeoordeling bescherming persoonsgegevens

2 Register gegevensverwerking (art 30, 35, 36, 45, 46, 47, 49 AVG)

2.1 Onderhouden register van gegevensverwerking

2.2 Zorg indien nodig voor goedkeuring van de Autoriteit Persoonsgegevens

2.3 Onderhoud registratie overdrachtsmechanismen internationale gegevensstromen

2.4 Gebruik indien nodig Binding Corporate Rules als overdrachtsmechanisme voor internationale gegevensoverdracht

2.5 Gebruik indien nodig modelcontractbepalingen voor internationale gegevensoverdracht

2.6 Gebruik indien nodig voorafgaande toestemming Autoriteit Persoonsgegevens als legitimerend overdrachtsmechanisme

2.7 Gebruik indien nodig een van de afwijkingen als legitimerend instrument voor gegevensoverdracht naar niet-EER landen

2.8 Gebruik indien nodig een juridisch bindend en afdwingbaar instrument tussen overheden als overdrachtsmechanisme voor internationale gegevensoverdracht

3 Awareness/Training en bewustwording (art 39 AVG)

3.1 Organiseer trainingen over het naleven van beleid en procedures over het beschermen van persoonsgegevens.

4 Privacybeleid (art 5, 6, 8, 9, 10,12,24, 91 AVG)

4.1 Onderhoud privacybeleid voor de bescherming persoonsgegevens

4.2 Documenteer de juridische grondslag voor de verwerking van persoonsgegeven

4.3 Onderhoud procedures voor de verwerking van bijzondere persoonsgegevens

4.4 Onderhoud procedures voor de verwerking van persoonsgegevens van minderjarigen

5 Privacybeleid in de bedrijfsvoering (art 4, 5, 6, 7, 8, 12 , 22, 25, 89 AVG)

5.1 Onderhoud beleid en procedures voor behoud kwaliteit persoonsgegevens

5.2 Onderhoud beleid en procedures voor beoordelen geheel of gedeeltelijk geautomatiseerde uitgevoerde verwerkingen

5.3 Onderhoud beleid en procedures voor secundair gebruik van persoonsgegevens

5.4 Onderhoud beleid en procedures voor bewaren van persoonsgegevens

5.5 Onderhoud beleid en procedures voor het gebruik van persoonsgegevens in de onderzoekspraktijk

5.6 Onderhoud beleid en procedures voor de de-identificatie van persoonsgegevens

5.7 Onderhoud beleid en procedures voor het verkrijgen van geldige toestemming

6 Beveiligingsrisico's (art 5, 32 AVG)

6.1. Integreer de bescherming van persoonsgegevens in de risicobeoordeling veiligheidsplan

6.2 Integreer de bescherming van persoonsgegevens in het informatiebeveiligingsbeleid

6.3 Onderhoud technische en organisatorische beveiligingsmaatregelen

6.4 Ondersteun het pseudonimiseren en versleutelen van persoonsgegevens

6.5 Integreer de bescherming van persoonsgegevens in het bedrijfscontinuïteitsplan

6.6 Test regelmatig de status van de beveiliging van persoonsgegevens

7 Verwerkersrisico's (art 28, 29 AVG)

7.1 Onderhoud de aan derde te stellen vereisten voor de bescherming van (gedeelde) persoonsgegevens

7.2 Onderhoud beleid en procedures voor het aangaan/uitvoeren van contracten of overeenkomsten met derde verwerker

7.3 Voer due diligence uit omtrent de bescherming van persoonsgegevens bij (potentiële) leveranciers/verwerkers

8 Privacyverklaring (art 12, 13, 14 AVG)

8.1 Onderhoud kennisgevingen omtrent de bescherming en omgangspraktijken van en met persoonsgegevens

8.2 Verstrek mededelingen over de bescherming van en omgangspraktijken met persoonsgegevens op alle punten waar deze worden verzameld

9 Verzoeken / klachten (art 15, 15, 17, 18, 19, 20, 21 AVG)

9.1 Onderhoud beleid en procedures omtrent reacties op verzoeken voor toegang tot persoonsgegevens

9.2 Onderhoud beleid en procedures om te reageren op verzoeken om informatie

9.3 Onderhoud beleid en procedures met betrekking tot reacties op verzoeken van betrokkenen tot rectificatie

9.4 Onderhoud beleid en procedures om te reageren op het afmelden van, beperken van, of bezwaar maken tegen het verwerken van persoonsgegevens

9.5 Onderhoud beleid en procedures om te reageren op verzoeken om gegevensportabiliteit

9.6 Onderhoud beleid en procedures om te reageren op verzoeken omtrent "right to be forgotten" of voor het wissen van gegevens

10 Nieuwe gegevensverwerking praktijk (art 25, 35, 36, 39 AVG)

10.1 Integreren bescherming van persoonsgegevens in systeem en productontwikkeling

10.2 Onderhoud Data Protection Impact Assessment (DPIA) richtlijnen en sjablonen

10.3 Uitvoeren DPIA's voor (nieuwe) programma's, systemen en processen

10.4 Uitvoer DPIA's voor wijzigingen in (bestaande) programma's, systemen of processen

10.5 Betrekken externe belanghebbenden bij het uitvoeren van DPIA's

10.6 Raadpleeg in geval van restrisico's vanuit DPIA de toezichthoudende autoriteit

11 Datalek managementprogramma (art 33, 34 AVG)

11.1 Onderhouden van een datalekprocedure voor gegevensinbreuk incidenten m.b.t. de bescherming van persoonsgegevens

11.2 Onderhoud een register voor het bijhouden van inbreuken in verband met persoonsgegevens

12 Monitoring gegevensverwerkingpraktijk (art 5, 24 AVG)

12.1 Uitvoeren zelfbeoordeling omtrent bescherming persoonsgegevens

12.2 Onderhoud bewijsvoering omtrent naleving AVG en/of afleggen verantwoording

12.3 Onderhouden van certificaten en accreditaties voor het aan de Autoriteit Persoonsgegevens kunnen aantonen van naleving AVG

13 Privacy-ontwikkelingen/Overzicht wet- & regelgeving (art 39 AVG)

13.1 Onderhouden van kennis en vaardigheden omtrent AVG-compliance vereisten, verwachtingen en best practices

Bijlage VI. Afkortingen, wet- en regelgeving, richtlijnen en normenkaders

- Ambtenarenwet
- Algemene Rijksvoorwaarden bij IT-Overeenkomsten (ARBIT2018)
- Algemene Verordening Gegevensbescherming (AVG)
- Algemene wet bestuursrecht
- Archiefwet
- Baseline Informatiebeveiliging Overheid (BIO)
- Beveiligingsvoorschrift Rijksdienst 2013 (BVR 2013)
- Code voor Informatiebeveiliging (ISO 27001:2013 en ISO 27002:2013)
- Comptabiliteitswet
- Cookiewet
- Eenduidige Normatiek Single Information Audit (ENSIA)
- Europese Netwerk- en informatiebeveiligingsrichtlijn (NIB2), *zie ook NIS2-richtlijn*
- eIDAS-verordening en eHerkenning
- Forum Standaardisatie open standaarden
- Gemeentelijke arbeidsvoorwaarden (CAR-UWO)
- Kader Rijkstoegangsbeleid
- Netwerk- en informatieveiligheid richtlijn (NIB-richtlijn)
- Network and Information Security directive (NIS2-richtlijn), *zie ook NIB2*
- Norm ICT-beveiligingsassessments DigID
- OGON-overleg (OpdrachtGever <de DUO-gemeenten>, OpdrachtNemer <de Duo+ Uitvoeringsorganisatie> overleg)
- Paspoortuitvoeringsregeling Nederland (PUN)
- Programma van Eisen PKI-Overheid
- Registratiewet
- Richtlijnen van het Nationaal Cyber Security Centrum (NCSC)
- Telecommunication Infrastructure Standard for Data Centers (TIA-942)
- Uitgangspunten online communicatie rijksambtenaren
- Uitvoeringswet AVG (UAVG)
- Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007)
- Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie (VIRBI:2013)
- Wet Basisregistratie Adressen en Gebouwen (BAG)
- Wet Basisregistratie personen (BRP)
- Wet Computercriminaliteit III
- Wet Elektronisch Bestuurlijk Verkeer (WEBV)
- Wet hergebruik van overheidsinformatie
- Wet Openbaarheid van Bestuur (WOB)
- Wet op de identificatieplicht
- Wet Particuliere Beveiligingsorganisaties en Recherchebureaus (WBPR)
- Wet Politiegegevens (WPG)
- Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI)
- Wet Veiligheidsonderzoeken (WVO)
- Wet Werk en Bijstand