gemeente
Haarlemmermeer

Nota van B&W

Onderwerp	Beleid voor informatiebeveiliging
Portefeuillehouder	S. Bak, J.J. Nobel
Collegevergadering	29 oktober 2013
Inlichtingen	Michael Pols (06 53541531)
Registratienummer	2013.0073785

Samenvatting
Het document "Beleid voor informatiebeveiliging" en het document "Normenkader informatiebeveiliging Haarlemmermeer", vormen gezamenlijk het nieuwe gemeentelijk beleid voor informatiebeveiliging.

In het "Beleid voor informatiebeveiliging" worden de visie en missie van de gemeente op het gebied van informatiebeveiliging en gegevensbescherming benoemd. Tevens worden de strategische uitgangspunten weergegeven welke als basis dienen voor het inhoudelijk normenkader.

In het document "Normenkader informatiebeveiliging", wordt volgens NEN/ISO 27002:2007 en NEN/ISO 27001:2005 het normenkader neergezet. Deze standaarden zijn voor de Nederlandse overheid gekozen en algemeen aanvaard als de norm voor informatiebeveiliging.

In het document "Beveiligingsplan Sociale Dienstverlening", worden de resultaten van de risicoanalyse weergegeven die in het voorjaar van 2013 is uitgevoerd en zijn adviezen opgenomen t.a.v. informatiebeveiliging. Dit cluster heeft een eigen beveiligingsplan, omdat hier meer dan bij andere clusters met privacygevoelige informatie wordt gewerkt en bijzondere aandacht voor beveiliging nodig is.

Inleiding
Een betrouwbare informatievoorziening is essentieel voor het goed functioneren van de processen van de gemeente. Informatiebeveiliging borgt deze betrouwbare informatievoorziening. Het is vanzelfsprekend dat informatiebeveiliging een normaal kwaliteitscriterium voor een gezonde bedrijfsvoering is. Geen keuze, maar een noodzaak.

Aanleiding
Het oude beleid dateert uit 2009. Hierin is vastgelegd dat beveiligingsbeleid elke 4 jaar wordt herzien. Hieraan komen wij thans tegemoet. Het oude beleid ging onvoldoende in op nieuwe vormen zoals tablets, smartphones, flexwerken en cybercrime. Een andere aanleiding is de ontwikkeling van de "Baseline Informatiebeveiliging Gemeenten. Deze is ontwikkeld door VNG/King en de Taskforce Bestuur en Informatieveiligheid Dienstverlening en gaat voor gemeenten een dwingend normenkader vormen.

Het voorgestelde beleid sluit hier volledig op aan. Dit beleid is overkoepelend en incorporeert ook meer specifieke gemeentelijke kaders zoals wet GBA (Gemeentelijke Basis Administratie), auditnormen BAG (Basisregistraties Adressen en Gebouwen) , de eisen Gezamenlijke Elektronische Voorzieningen SUWI (Structuur Uitvoering Werk en Inkomen), Gemma (Gemeentelijk Model Architectuur), en NORA (Nederlands Overheids ReferentieArchitectuur) kaders. Ook de nieuwe richtlijnen van het College Bescherming Persoonsgegevens van voorjaar 2013 zijn meegenomen.
Tenslotte vraagt de toenemende flexibilisering, het nieuwe werken, grotere mobiliteit, om een medewerker die altijd en overal toegang heeft tot de informatie die op dat moment noodzakelijk is. De nauwere samenwerking tussen de gemeenten en andere overheidsorganisaties op het gebied van bedrijfsvoering en gemeentelijke processen vraagt om een stringentere beveiligingshouding en het toepassen van een nieuwe beveiligingsstrategie om risico's af te dekken.

Risico's
Het niet voldoen aan de afspraak om het elke vier jaar het beleid actualiseren en kan problemen opleveren bij audits. Daarnaast geeft het oude beleid geen regels voor nieuwe technologie en processen, die in de afgelopen jaren wel toegepast zijn. Tenslotte anticipeert de gemeente met dit beleid op de Baseline Informatiebeveiliging Gemeenten, waarvan bekend is dat deze vanaf 2014 dwingend van karakter zal worden.

Doelstelling
Met het nieuwe gemeentelijk beleid voor informatiebeveiliging geeft het college vorm aan informatiebeveiliging als kwaliteitsaspect voor een betrouwbare dienstverlening en voldoet het beleid aan alle normenkaders en richtlijnen op het gebied van informatiebeveiliging.

Middelen
Bij informatiebeveiliging is de 'mens' de belangrijkste en tevens zwakste schakel. Investeren op bewustwording en bewustzijn van beveiligingsrisico's is een belangrijk onderdeel in het verbeteren van informatiebeveiliging. Het nieuwe beleid zal ondersteund worden met een communicatie- en trainingsbudget, waarmee het beleid in de organisatie onder de aandacht kan worden gebracht en waarbij medewerkers en management kunnen worden getraind om een veilige omgang met informatie en informatievoorzieningen te verbeteren. De kosten worden gedekt binnen de huidige begroting.

Evaluatie
In het nieuwe beleid is expliciet opgenomen dat rapportage op het beleid periodiek zal plaatsvinden. Daarin zijn op verschillende niveaus de rapportage momenten benoemd. Dit moet zorgen voor een nauwere betrokkenheid van directie en bestuur bij het onderwerp en proces van informatiebeveiliging en verbetert de mogelijkheden om hierop te sturen. Het beleid zal tenminste iedere 4 jaar worden geëvalueerd en bijgesteld, of wanneer dit eerder noodzakelijk wordt geacht.

In- en externe communicatie
Medewerkers zullen op verschillende manieren in 2014 op de hoogte gebracht worden van het nieuwe beleid voor informatiebeveiliging en instructie ontvangen om in hun werkzaamheden goed vorm te kunnen geven aan de normen die het beleid stelt.

Relatie Beveiligingsplan GBA- en Waardedocumenten
Zoals ook genoemd in de documenten, heeft de gemeente vanuit de GBA een beveiligingsplan. Deze is in juni 2012 vastgesteld door college van B&W en de gemeenteraad. Om die reden wordt de gemeenteraad nu ook in kennis gesteld van het organisatie brede beleid voor informatiebeveiliging.

Beveiligingsplan Sociale Dienstverlening
Het beveiligingsplan Sociale Dienstverlening was net als het organisatie brede beleid toe aan vernieuwing. Het oorspronkelijke stuk dateert uit 2010. In verband met de vele veranderingen op het gebied van Sociale Dienstverlening was er behoefte aan een geactualiseerd plan, welke aansluiting bij de huidige situatie en risico's van het cluster. Dit is ook een van de aandachtspunten die uit het BKWI (Bureau Ketenautomatisering Werk en Inkomen) onderzoek in 2012 zijn gekomen, met het nieuwe beveiligingsplan Sociale Dienstverlening is invulling gegeven aan de adviezen die in 2012 zijn gegeven vanuit de toetsing door het BKWI.

Besluit
Op grond van het voorgaande hebben wij besloten om:
1. het Beleid voor informatiebeveiliging vast te stellen;
2. het Normenkader informatiebeveiliging vast te stellen;
3. het Beveiligingsplan Sociale Dienstverlening vast te stellen;
4. deze nota ter informatie aan de raad te zenden.

Burgemeester en wethouders van de gemeente Haarlemmermeer,
namens dezen,
de portefeuillehouders,

S. Bak

J.J. Nobel

Bijlage(n)
'Beleid voor informatiebeveiliging'
'Normenkader informatiebeveiliging'
'Beveiligingsplan Sociale Dienstverlening

gemeente
Haarlemmermeer

Beleid voor Informatiebeveiliging

Strategisch kader voor een veilige en beveiligde informatievoorziening en gegevensverwerking

1

INLEIDING

INFORMATIE

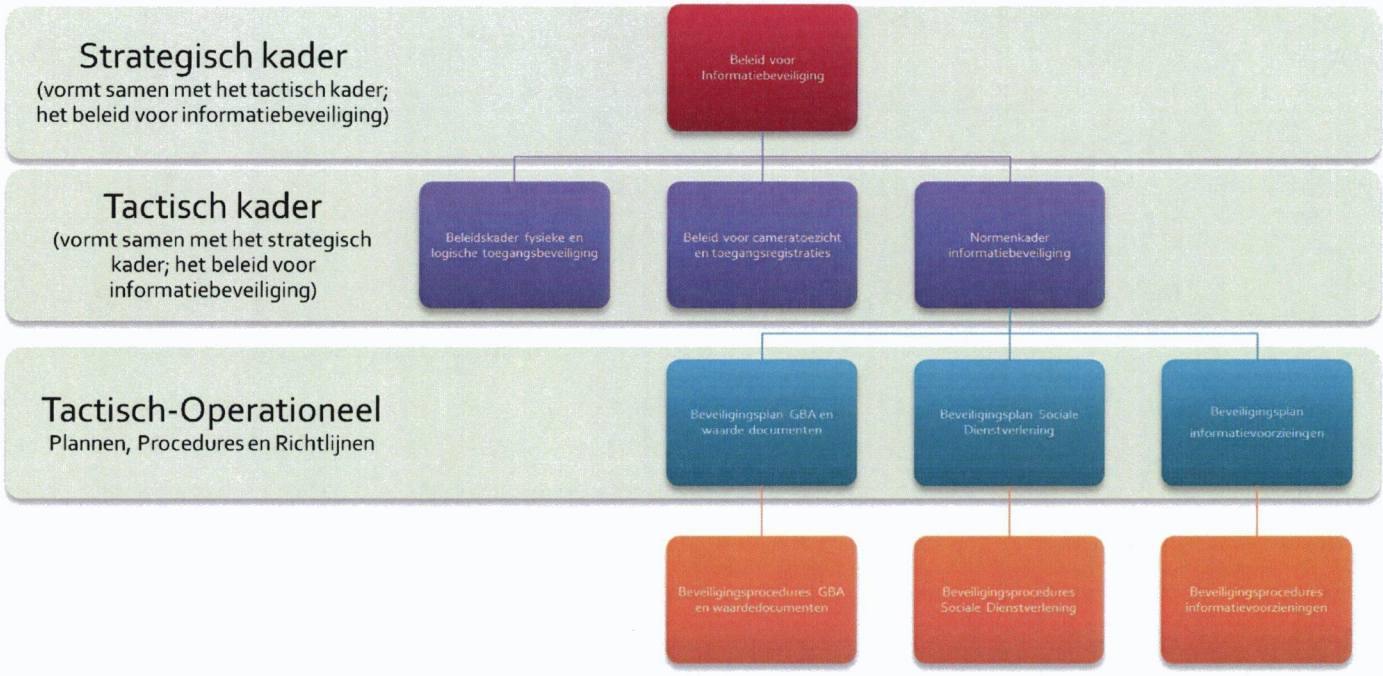
is één van de voornaamste bedrijfsmiddelen van een overheidsorganisatie. Toegankelijke en betrouwbare informatie is essentieel voor 'behoorlijk bestuur': voor een gemeente die zich verantwoordelijk gedraagt, aanspreekbaar en servicegericht is, die transparant en proactief verantwoording aflegt aan burgers en volksvertegenwoordiging en die met minimale middelen maximale resultaten behaalt. Incidenten tonen aan dat de beveiliging van informatie vaak onderbelicht is, maar dat het belang erg groot is. Het niet op orde hebben van informatiebeveiliging is hinderlijk voor de bedrijfsvoering en staat een deugdelijke verantwoording over beveiliging in de weg, gedegen informatiebeveiliging is noodzakelijk.

De wereld om ons heen vergt een betere beveiliging van gemeentelijke informatie. De overheid en ook de gemeente gaat producten en diensten in toenemende mate online aanbieden en dient dit snel en betrouwbaar te doen en waarbij de waarborging van privacy goed geregeld is. De interactie tussen de gemeente en de samenleving intensiveert. In al die ontwikkelingen is beschikbaarheid, juistheid en vertrouwelijkheid van informatie de sleutel tot goede bedrijfsvoering. De gemeente komt daarom met dit gemeentelijke 'Beleid voor Informatiebeveiliging' welke is opgesteld op basis van de Nationale Cyber Security Strategie (NCSC), de Baseline Informatiebeveiliging Gemeenten (KING/VNG), de internationale standaard ISO27002 en gemeentelijke doelstellingen. Met deze strategie komt de gemeente tegemoet aan de verzoeken van verschillende toezichthouders (Logius BZK, Bureau Ketenautomatisering Werk & Inkomen (BKWI), Agentschap BPRBZK en de gemeenteraad) en geeft het college van B&W vorm aan de integrale aanpak voor informatiebeveiliging.

Leeswijzer

Dit document " Beleid voor informatiebeveiliging" en het document "Normenkader informatiebeveiliging Haarlemmermeer", vormen gezamenlijk het gemeentelijk beleid voor informatiebeveiliging. In het "Beleid voor informatiebeveiliging" worden de visie en missie van de gemeente op het gebied van informatiebeveiliging en gegevensbescherming benoemd. Tevens worden de strategische uitgangspunten weergegeven welke als kapstok dienen voor het inhoudelijk normenkader. In het document " Normenkader informatiebeveiliging", wordt volgens NEN/ISO 27002:2007 en NEN/ISO 27001:2005 het normenkader neergezet. Deze standaarden zijn voor de Nederlandse overheid gekozen en algemeen aanvaard als de norm voor informatiebeveiliging. Binnen de gemeente bevinden zich een aantal specifieke werkterreinen die een ' eigen' beveiligingsplan kennen. Het gaat daarbij om het cluster KCC, waar op grond van wetgeving GBA een eigen "beveiligingsplan GBA en waarde documenten" wordt gehanteerd. Het cluster Sociale Dienstverlening beschikt over het "Beveiligingsplan Sociale Dienstverlening" en "Beveiligingsprocedures Sociale Dienstverlening" , die zij in het kader van de Verantwoordingsrichtlijn SUWI hanteren. Het cluster Info+ heeft voor informatievoorzieningen, IT-procedures en het beheer van het gemeentelijk datacenter een eigen "Beveiligingsplan Informatievoorzieningen" en "Beveiligingsprocedures Informatievoorzieningen". Allen hanteren de normen zoals beschreven in het "Normenkader informatiebeveiliging" en volgen daarmee het gemeente brede beveiligingsbeleid. Ze beschrijven echter ook specifiekere procedures en richtlijnen op tactisch-operationeel niveau voor eindgebruikers, daar waar het gaat om beveiliging en gegevensbescherming.

De opzet zoals hierboven beschreven is op de volgende pagina schematisch weergegeven.



Verwant beleid

Het beveiligingsbeleid heeft haar relaties met aanverwante beleidskaders binnen de gemeente. Hierbij valt te denken aan het integriteitsbeleid en het ARBO-beleid. Daaraan gerelateerd is het 'beleid Omgang met Agressie en Geweld. Verder heeft de gemeente al bestaande beleidskaders voor cameratoezicht en toegangsregistraties. De verschillende beleidskaders hebben samenhang en de verschillende betrokken disciplines zijn binnen de organisatie vertegenwoordigd in de 'Beveiligingsadvies Commissie' die eens per kwartaal bijeenkomt om integrale afstemming te houden.

Voor wie

Het beleid geldt voor de hele gemeentelijke organisatie. Daarbinnen is het College van Burgemeester en Wethouders integraal verantwoordelijk voor de beveiliging van informatie binnen de werkprocessen van de gemeente. In dat kader is ook de kwaliteit van de binnen de werkprocessen gegenereerde en verzamelde informatie haar belang en haar zorg.

Het beleid voor informatiebeveiliging is voor B&W een hulpmiddel om 'in control' te zijn waar het gaat om de informatiebeveiliging. Het beleid is daarnaast bestemd voor alle managers en medewerkers die binnen de gemeente te maken hebben met eigenaarschap, beheer of gebruik van informatie(voorzieningen).

De gemeente heeft belang bij juiste bedrijfsvoering en het maatschappelijk functioneren van zijn organisatie. B&W legt een solide basis voor strategisch, innovatief en ethisch handelen, voor een effectieve bedrijfsvoering, voor een soepele en efficiënte uitvoering, voor compliance, compatibiliteit, prestatie-, kwaliteits- en risicomanagement en voor een betrouwbaar geheugen van organisatiekennis.

De baten van goede informatiebeveiliging komen echter niet alleen ten goede aan de overheid zelf, maar ook aan de burgers, die sneller en beter bediend worden met toegankelijke, juiste en betrouwbare overheidsinformatie. De gemeente streeft naar meer transparantie en naar een betere dienstverlening waarbij informatiebeveiliging een belangrijk kwaliteitscriterium is.

In deze documenten is gestreefd naar een stelsel van regels die een hoge mate van toekomstvastheid bezit.

2

CONTEXT

Informatievoorziening en het belang voor samenleving en economie.
Uitval van computers of telecommunicatiesystemen, het in ongerede raken van gegevensbestanden of het door onbevoegden kennisnemen dan wel manipuleren van bepaalde gegevens kan ernstige gevolgen hebben voor de beleids- en bedrijfsvoering. Dit heeft mogelijk negatieve gevolgen voor burger, bedrijf en / of overheid. Ketens en de koppeling van voorheen losstaande informatiesystemen, leiden tot complexe situaties met diffuse verantwoordelijkheden.

Enerzijds komen gegevens steeds gemakkelijker beschikbaar, anderzijds zijn gegevensstromen steeds moeilijker beheersbaar. Het gebruik van informatievoorzieningen neemt daarbij een veelheid aan verschijningsvormen aan: kantoorautomatisering, e-mail, netwerken, plaats en tijdonafhankelijk werken, de integratie van spraak, beeld en conventionele data en soortgelijke trends. De wijze waarop deze geautomatiseerde hulpmiddelen ter beschikking gesteld en geëxploiteerd worden, is aan verandering onderhevig. Dit alles verandert de mogelijkheden op controle en toezicht.

Nut en noodzaak
Een betrouwbare informatievoorziening is essentieel voor het goed functioneren van de processen van de gemeente. Informatiebeveiliging is het proces dat deze betrouwbare informatievoorziening borgt. Het opnemen van informatiebeveiliging als normaal kwaliteitscriterium voor een gezonde bedrijfsvoering is tegenwoordig niet langer een keuze, maar een noodzaak.

Deze noodzaak komt onder meer voort uit de toenemende digitalisering van de gemeentelijke dienstverlening, waardoor de afhankelijkheid van de geautomatiseerde informatieverwerking steeds verder groeit. Maar het is niet alleen de automatisering. De samenwerking met andere overheden (in ketens) en contacten met burgers en bedrijven neemt steeds verder toe. Dit legt (deels nieuwe) eisen op aan de kwaliteit van de informatievoorziening van de gemeente. Daarnaast spelen wet- en regelgeving een belangrijke rol. De Wbp (Wet Bescherming Persoonsgegevens) en de Archiefwet zijn voorbeelden van wetten die eisen stellen aan de verwerking en opslag van informatie.

Tot slot is er de maatschappelijke verantwoordelijkheid die een overheidsinstantie zoals de gemeente tegenover de inwoners en bedrijven heeft. Van de gemeente mag verwacht worden dat zij zorgvuldig omgaat met de gegevens die zij beheert, en dat de gegevens die zij levert juist, accuraat en tijdig zijn. Kortom, structurele aandacht voor de betrouwbaarheid van de informatievoorziening, het domein van informatiebeveiliging, helpt de gemeente bij een goede invulling van haar maatschappelijke taken. Een goede borging van informatiebeveiliging zorgt voor een betere betrouwbaarheid van de informatievoorziening en een grotere continuïteit van de gemeentelijke bedrijfs-voering.

Samenwerking, altijd en overal
Toenemende flexibilisering, het nieuwe werken, grotere mobiliteit vraagt om een medewerker die altijd en overal toegang heeft tot de informatie die voor hem op dat moment noodzakelijk is. De nauwere samenwerking tussen de gemeenten en andere overheidsorganisaties op het gebied van bedrijfsvoering en gemeentelijke processen vraagt om een veranderende beveiligingshouding en het toepassen van nieuwe middelen om risico's af te dekken. Gemeenten hebben in toenemende mate te maken met normenkaders zoals aansluitvoorwaarden op basisregistraties, deze normenkaders verschillen in opbouw, overlappen elkaar deels en zijn daardoor moeilijk te beheren en te implementeren. Zoveel verschillende normenkaders is verwarrend en belemmert een beheerste beveiliging en het implementeren en beheren van de normenkaders. Met dit beleid voor informatiebeveiliging is geprobeerd al deze kaders te vatten in één, om daarmee voor een beleidskader te zorgen waarmee aan alle voor de gemeente relevante normen wordt voldoen m.b.t. beveiliging en bescherming van gegevens.

3

HET STRATEGISCH KADER

Begripsbepalingen
Informatiebeveiliging: het proces van vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen;
Informatiesysteem: een samenhangend geheel van gegevensverzamelingen, en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie.

Plaatsbepaling en Reikwijdte
Dit strategisch kader geldt voor de hele gemeentelijke organisatie waartoe gerekend worden de gemeente met de daaronder vallende diensten, bedrijven en instellingen.
Dit beleid geldt voor het gehele proces van informatievoorziening en de gehele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie.

Informatiebeveiliging is een onderdeel van de kwaliteitszorg voor bedrijfs- en bestuursprocessen en de ondersteunende informatiesystemen. Informatiebeveiliging is een 'gewone' lijnverantwoordelijkheid. Daaraan inhoud geven, gebeurt zowel op basis van interne ovenwegingen betreffende de betrouwbaarheid van de werkprocessen van een organisatie als op basis van externe randvoorwaarden zoals bestaande wet- en regelgeving. Uitgangspunt daarbij vormt de noodzaak om tot een integrale benadering van informatiebeveiliging te komen.

Dreigingen
De traditionele benadering van informatiebeveiliging, waarbij aan de buitenkant van de organisatie muren werden opgetrokken om het kwaad buiten te houden, is niet meer houdbaar. Medewerkers maken immers gebruik van internet, sociale media, mobiele apparaten, werken ook thuis of brengen eigen apparatuur mee naar kantoor. Digitale buitengrenzen van de organisatie vervagen en de kwetsbaarheid voor dreigingen verhoogt. Het bewust of onbewust verspreiden van virussen en andere kwaadaardige software , onvoldoende beveiligde websites en webapplicaties, toegangsbeveiliging die eenvoudig is te omzeilen, niet bijgewerkte software, het gebruik van mobiele apparaten, flexwerken en de effecten daarvan, zijn zaken waar iedere organisatie zich tegen moet wapenen.

De organisatie zal er vanuit moeten gaan dat hun digitale muren doordringbaar zijn, zelfs als de kritische netwerken niet direct met het internet verbonden zijn. Dat een organisatie slachtoffer kan worden van een aanval, betekent dat het accent van de veiligheidsmaatregelen verschuift van het steeds hoger maken de van muren (weerbaarheid) naar de capaciteit veerkrachtig op te kunnen treden. Detectie van en response op incidenten moet goed worden georganiseerd.

Als hogere muren niet voldoende zijn, wordt het beveiligen van kleinere delen binnen de muren relevanter. Onderdeel hiervan is een gelaagde beveiligingsstrategie. Deze strategie wil de gemeente in de komende jaren verder opbouwen, omdat zij gelooft dat de context waarin informatiebeveiliging zich bevind en komende jaren in toenemende mate zal bevinden, alleen maar effectief kan worden toegepast wanneer een dergelijke strategie wordt gehanteerd.

Vernieuwing van informatiebeveiliging, overgang naar veilig faciliteren
Beveiligingsprocessen- en procedures hebben de naam veelal belemmerende effecten te hebben. Dit past niet goed meer bij de organisatiedoelstellingen en manier van bedrijfsvoering die gewenst is. Dit beleid wil dan ook veilig faciliteren en biedt kaders voor een veilige en beveiligde informatievoorziening en gegevensverwerking. De traditionele manier van inperken wordt waar mogelijk vervangen door een aanpak van veilig faciliteren.

Informatiebeveiliging is en blijft een verantwoordelijkheid van het lijnmanagement
Het lijnmanagement is verantwoordelijk voor de kwaliteit van bedrijfsvoering. Die verantwoordelijkheid wordt verticaal in de lijn verdeeld, van organisatietop tot teammanager. Informatiebeveiliging geldt als een integraal onderdeel van de bedrijfsvoering. Zo is het lijnmanagement ook eindverantwoordelijk voor informatiebeveiliging.

Het lijnmanagement kan besluiten om (delen van) de ontwikkeling, exploitatie of het onderhoud van systemen uit te besteden. Ook in deze gevallen blijft het lijnmanagement eindverantwoordelijk voor de beveiliging van het individuele systeem. Het lijnmanagement communiceert de betrouwbaarheidseisen van het systeem aan de derde partij. Via een schriftelijke overeenkomst (bijvoorbeeld een bewerkersovereenkomst of een Service Level Agreement) wordt vastgelegd hoe de derde partij aan deze eisen gaat voldoen en tevens worden er consequenties verbonden aan het niet naleven van deze afspraken. Vanuit zijn hoedanigheid als verantwoordelijke partij, controleert het lijnmanagement of de werkzaamheden van de derde partij het vereiste betrouwbaarheidsniveau realiseren.

Eigen verantwoordelijkheid
Alle gebruikers nemen passende maatregelen om in hun eigen werkzaamheden en werkprocessen rekening te houden met beveiliging en veiligheidsrisico's voor anderen. Zij zijn zorgvuldig met het opslaan en delen van gevoelige informatie en respecteren de informatie en de systemen van de organisatie en anderen.

Conformeren aan standaarden
Het beleid vormt een samenhangend stelsel van maatregelen welke gebaseerd zijn op standaarden, (overheids) normen, bestaande beveiligingsdocumentatie voor gemeenten en aansluitvoorwaarden van basisregistraties.

Verbinden en versterken van initiatieven
Wederzijds vertrouwen is essentieel om samen te werken en informatie met elkaar te delen. Overheid en bedrijfsleven werken dan ook samen als gelijkwaardige partners.
Het grensoverschrijdende karakter van dreigingen maakt het noodzakelijk sterk in te zetten op samenwerking. Uitgangspunt is gelijkwaardigheid en betrokkenheid. Veel maatregelen zullen pas effect sorteren als ze breder worden afgestemd dan wel getroffen. De gemeente Haarlemmermeer steunt en draagt actief bij aan de inspanningen van bijvoorbeeld de Informatiebeveiligingsdienst (IBD) en beveiligingsinitiatieven van het CIO Platform Nederland en andere samenwerkingsverbanden.

Te nemen maatregelen zijn proportioneel
Honderd procent veiligheid bestaat niet. De gemeente maakt keuzes in het oppakken van informatiebeveiligingsactiviteiten op basis van een risicoafweging. Belangrijk onderdeel daarbij vormt een aantal kernwaarden van onze samenleving. Privacy, respect voor anderen en fundamentele rechten als de vrijheid van meningsuiting en informatievergaring dienen overeind te blijven. Er moet een goede balans blijven bestaan. Maatregelen moeten proportioneel zijn. Hiervoor worden waarborgen en toetsingsmechanismen, waaronder de bestaande toezichtfuncties, benut en waar nodig versterkt.

Zelfregulering als het kan, wet- en regelgeving als het moet
Overheid en bedrijven bereiken de gewenste digitale veiligheid allereerst door zelfregulering. Wanneer zelfregulering niet werkt wordt gekeken naar mogelijkheden van wet- en regelgeving. Ontwikkelingen gaan snel. Wetgeving kan daardoor snel verouderen. De gemeente gaat na of de wetgeving adequaat ingaat op de ontwikkelingen in het digitale domein, en stelt haar beveiliging hierop weloverwogen af.

Het primaire uitgangspunt voor informatiebeveiliging is risicomanagement
Informatiebeveiliging is altijd een op risicomanagement gebaseerde toepassing van processen, maatregelen en sturing. Echter het is van groot belang dat de organisatie ook op de hoogte blijft van ontwikkelingen buiten de organisatie, zoals; in hoeverre heeft de digitale buitenwereld impact op de organisatie? Is er bijvoorbeeld sprake van dreigingen die cruciale elementen tot doelwit heeft? Is de organisatie op de hoogte van hoe er over haar wordt gesproken? Zijn er bij vergelijkbare organisaties aanvallen geweest waar we van kunnen leren? Deze informatievergaring wordt steeds belangrijker. Het verstrekt het omgevingsbewustzijn en kan ervoor zorgen dat de organisatie beter in staat is een incident op te vangen.

Aanvullend is versterking van het omgevingsbewustzijn over de digitale wereld ook nodig om bestuurs- en directieniveau. Digitale onveiligheid raakt namelijk belangrijke bedrijfsmiddelen van de organisatie, zoals geld, organisatiegegevens, continuïteit van processen, gegevens van burgers en imago. Voor de bestuurders en directie moet duidelijk zijn welke risico's de organisatie loopt en welke maatregelen nodig en gerechtvaardigd zijn op basis van de kritieke bedrijfsmiddelen.

Een vertaling van digitale trends naar actuele en voor de organisatie kritische parameters is dan ook belangrijk. Het voorkomt een focus op incidenten en geeft de directie de mogelijkheid om een goed beeld te krijgen en te houden en daarmee met de juiste informatie sturing te geven als onderdeel van het strategisch risicomanagement. In de invulling van dit beleid is rapportage naar directie en bestuur een belangrijk uitgangspunt waarop de gemeente sterker wil inzetten, omdat dit als cruciaal onderdeel wordt gezien om informatiebeveiliging op een hoger plan te krijgen en verdere verbetering te bewerkstelligen.

Verantwoord en bewust gedrag van mensen is essentieel voor een goede informatiebeveiliging
Hoe technisch 'informatiebeveiliging' ook lijkt, informatiebeveiliging omvat veel meer dan technologie. Juist de mens en de organisatie zijn belangrijke dimensies voor een veilige informatievoorziening en gegevens bescherming. In de dimensie 'mens' zijn met name bewustwording, gedrag en informatie uitwisseling van belang. Versterking van omgevingsbewustzijn, over zowel de dreigingen als de ontwikkelingen in de digitale wereld, is noodzakelijk op alle niveaus in de organisatie.

Beveiliging is zo sterk als de zwakste schakel en deze is bijna altijd menselijk handelen. Verantwoord en bewust gedrag van medewerkers is dus essentieel voor een geslaagde beveiligingsweerbaarheid. Een belangrijk speerpunt vanuit dit 'Beleid voor Informatiebeveiliging' is dan ook om bewustwording bij medewerkers van de organisatie op het gebied van informatiebeveiliging en veilige omgang met gegevens te vergroten, zodat zij worden voorzien van de nodige kennis om juist te handelen en bewuster om te gaan met informatie en informatievoorzieningen die zij voor hun werkzaamheden gebruiken.

Beveiliging vereist een integrale aanpak
Informatiebeveiliging is vanwege het belang voor de organisatie bij uitstek een onderwerp voor de directie. Beveiligingsrisico's moeten onderdeel zijn van het cyclische proces van strategisch risicomanagement, waarbij periodiek belangen, risico's en maatregelen (controls) worden geëvalueerd. Digitale beveiliging is daarbij slechts één dimensie waar de

organisatie rekening mee moet houden. Een integrale aanpak kijkt ook naar dreigingen en kwetsbaarheden vanuit andere dimensies. Alleen al daarom is een integrale aanpak nodig, waarbij gestreefd wordt naar synergie en samenwerking met disciplines zoals, HRM, FM, Financiën, Communicatie, Juridische zaken en Corporate Control. Alleen door deze integrale aanpak kunnen de bestuurders 'in control' zijn over de veiligheid in de organisatie.

Gehanteerde principes

- Het beleid is opgesteld op basis van de Baseline Informatiebeveiliging Gemeenten.
- Bij de opbouw van het beleid wordt het principe van gelaagde opbouw gehanteerd. Er is een basisbeveiligingsniveau (overeenkomend met "Vertrouwelijk"). Daar waar bepaalde toepassingen, werkomgevingen of specifieke dreigingen een hogere beveiligingsgraad of specialistische maatregelen vereisen, kunnen extra maatregelen getroffen worden bovenop het basisbeveiligingsniveau. Dit kan vorm worden gegeven door een gerichte risicoanalyse uit te voeren en op basis daarvan een specifiek beveiligingsplan op te stellen.
- Specialistische maatregelen voor afwijkende situaties of hogere beveiligingsniveaus dan het basisniveau, zijn niet in dit beleid opgenomen. Hiervoor zijn aanvullende beveiligingsplannen en beveiligingsprocedures, waar nodig.
- Het gekozen beveiligingsniveau is zodanig, dat er in een overgrote meerderheid van de gevallen geen aanleiding bestaat om tot extra maatregelen over te gaan.
- Het gemeentelijke beleid voor informatiebeveiliging wordt iedere vier jaar herzien en opnieuw vastgesteld door directie, college van B&W en de gemeenteraad.

Vertrouwen in toetsing

Als de gemeente de informatievoorziening en IT inricht volgens de hier geformuleerde uitgangspunten en de normen uit het Normenkader (in opzet, bestaan en werking) dan moet dat voldoende garantie bieden dat de gemeente haar eigen informatie en die van andere overheidsinstellingen (centraal en decentraal) veilig (beschikbaar, integer en vertrouwelijk) kan behandelen. Gemeenten moeten elkaar hierop kunnen aanspreken. Bij de implementatie geldt voor de tactische normen en eisen een " voldoe of leg uit regime". Het toetsen vindt plaats aan de hand van de 'in control' verklaring. De 'in control' verklaring moet dus inzicht geven aan welke normen wordt voldaan en voor welke normen een "leg uit" is gedefinieerd. In feite wordt aan het management een managementverantwoording (in control statement) wat betreft de informatiebeveiliging gevraagd.

Door het beveiligingsbeleid op te nemen in de planning en control cyclus en hierover door de organisatieonderdelen verantwoording af te laten leggen door reguliere voortgangsrapportages, heeft beveiliging een duidelijke rol in de verticale sturingskolom van een gemeente. Een planning en control cyclus is vastgelegd in de gemeentelijke begrotingssystematiek. Aansluiting hierbij voorkomt dat informatiebeveiliging als een eigenstandig onderwerp wordt behandeld en daardoor laag geprioriteerd wordt. Over de begroting en de uitvoering wordt verantwoording afgelegd. Over het functioneren van de informatiebeveiliging (dus de kwaliteitscirkel) wordt conform de planning en control cyclus binnen de gemeente en richting de raad verantwoording afgelegd door B&W. Voor het effectueren van informatiebeveiliging wordt gewerkt via de Plan Do Check Act cyclus. Na het vaststellen wat nodig is, worden maatregelen getroffen en gecontroleerd of die maatregelen het gewenste effect sorteren (controle). Deze controle kan direct aanleiding geven tot bijsturing in de maatregelen. Ook kan het totaal van eisen, maatregelen en controle aan revisie toe zijn (evaluatie). Het goed doorlopen van deze kwaliteitscirkel zorgt op elk moment voor controle en verbetering van het beveiligingsniveau.

Controleerbaarheid

Het 'in control statement' op het gebied van informatiebeveiliging vervult een essentiële rol. Het in control statement wordt door de gemeente zelf opgesteld en vermeld in de bedrijfsvoeringparagraaf van het jaarrapport. Om te komen tot het 'in control statement' zullen de bedrijfsonderdelen van een gemeente aan de hand van de normen van het beleid zelf na moeten gaan in welke mate ("voldoe of leg uit") zij daaraan voldoen (interne audit). Die interne toetsing vindt plaats op basis van een toets aan ISO 27001:2005/ ISO27002:2007, plus de beleid specifieke aanvullingen, indien van toepassing.

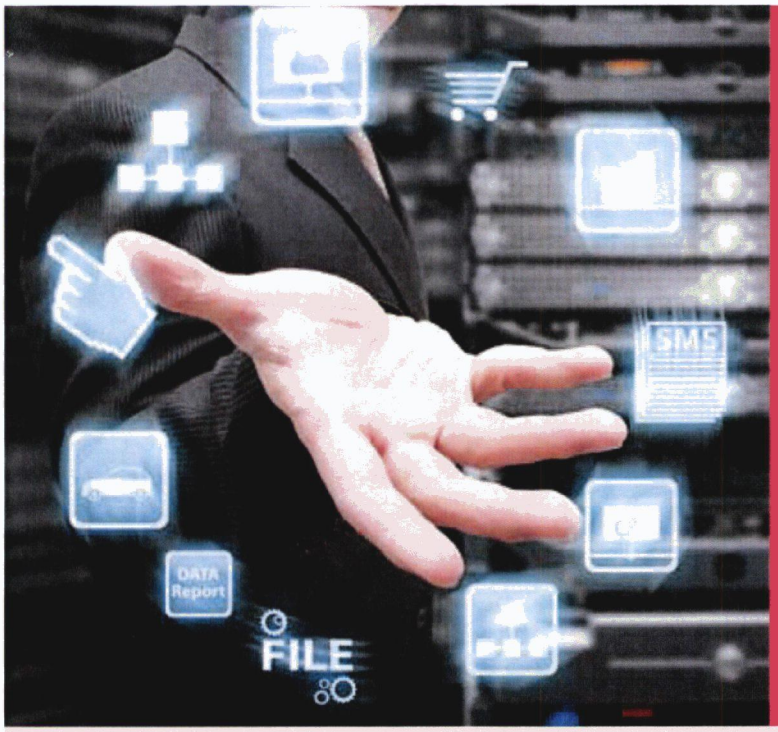
Vervolg 'Beleid voor informatiebeveiliging' in het 'Normenkader informatiebeveiliging'.

gemeente
Haarlemmermeer

Normenkader
informatiebeveiliging

VEILIGHEID

INHOUDSOPGAVE



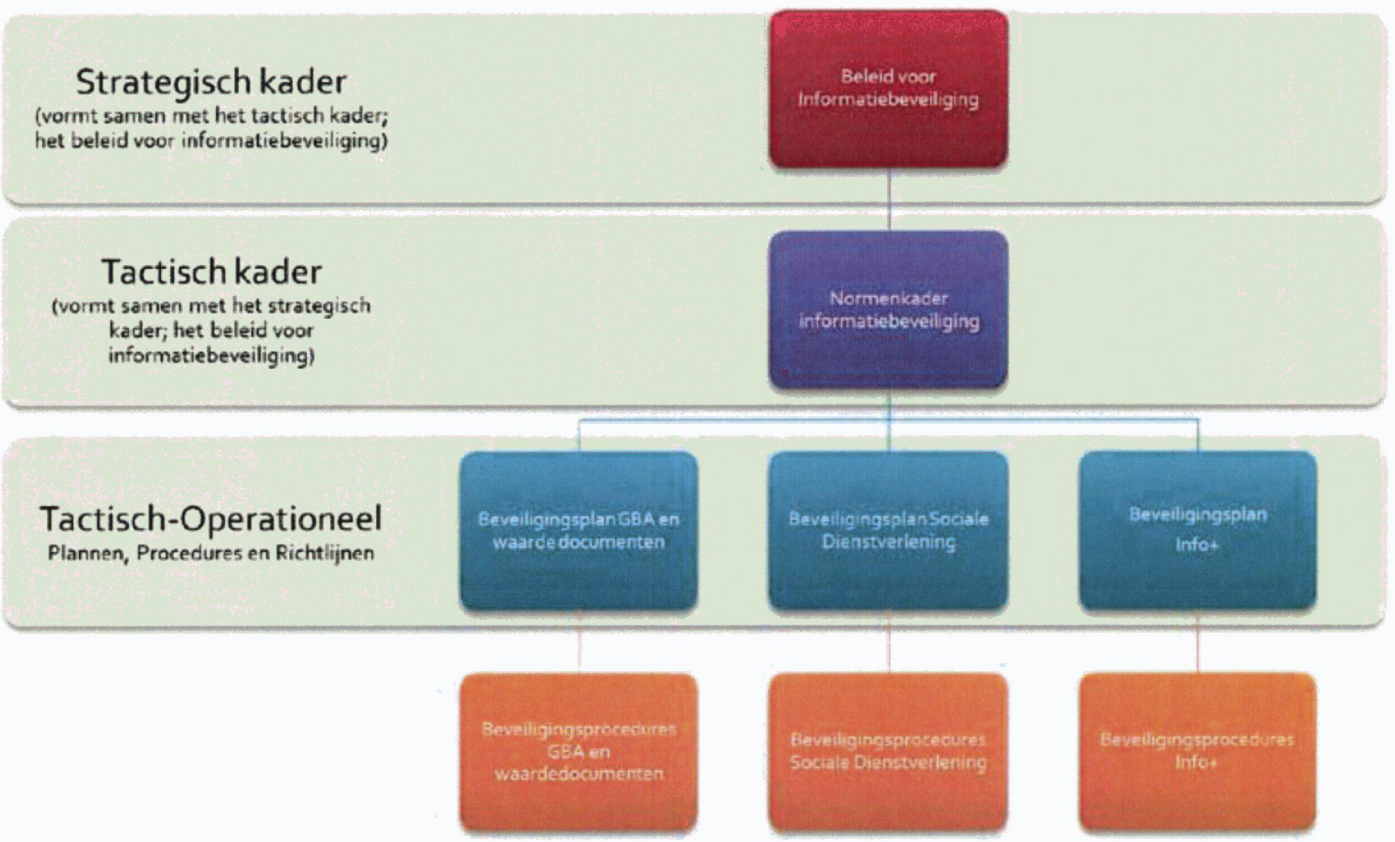
VEILIGHEID

INLEIDING

BELEID VOOR INFORMATIEBEVEILIGING

Leeswijzer

In dit document treft u het normenkader dat de beschikbaarheid, integriteit en exclusiviteit van gemeentelijke informatie (systemen) bevordert. Het bevat een totaalpakket aan informatiebeveiligingsmaatregelen. Dit beleid is opgezet rondom bestaande normen de NEN/ISO 27002:2007 en NEN/ISO 27001:2005. Deze standaard is voor de Nederlandse Overheid gekozen en algemeen aanvaard als de norm voor informatiebeveiliging. In het document "Beleid voor informatiebeveiliging" is aangegeven waarom informatiebeveiliging en welke uitgangspunten de gemeente als belangrijkste aandachtsgebieden definieert. In de verbijzonderde beveiligingsplannen, uitvoeringsrichtlijnen en procedures worden meer detaillistische en praktische uitwerkingen gegeven van de in dit document genoemde normen.



VEILIGHEID

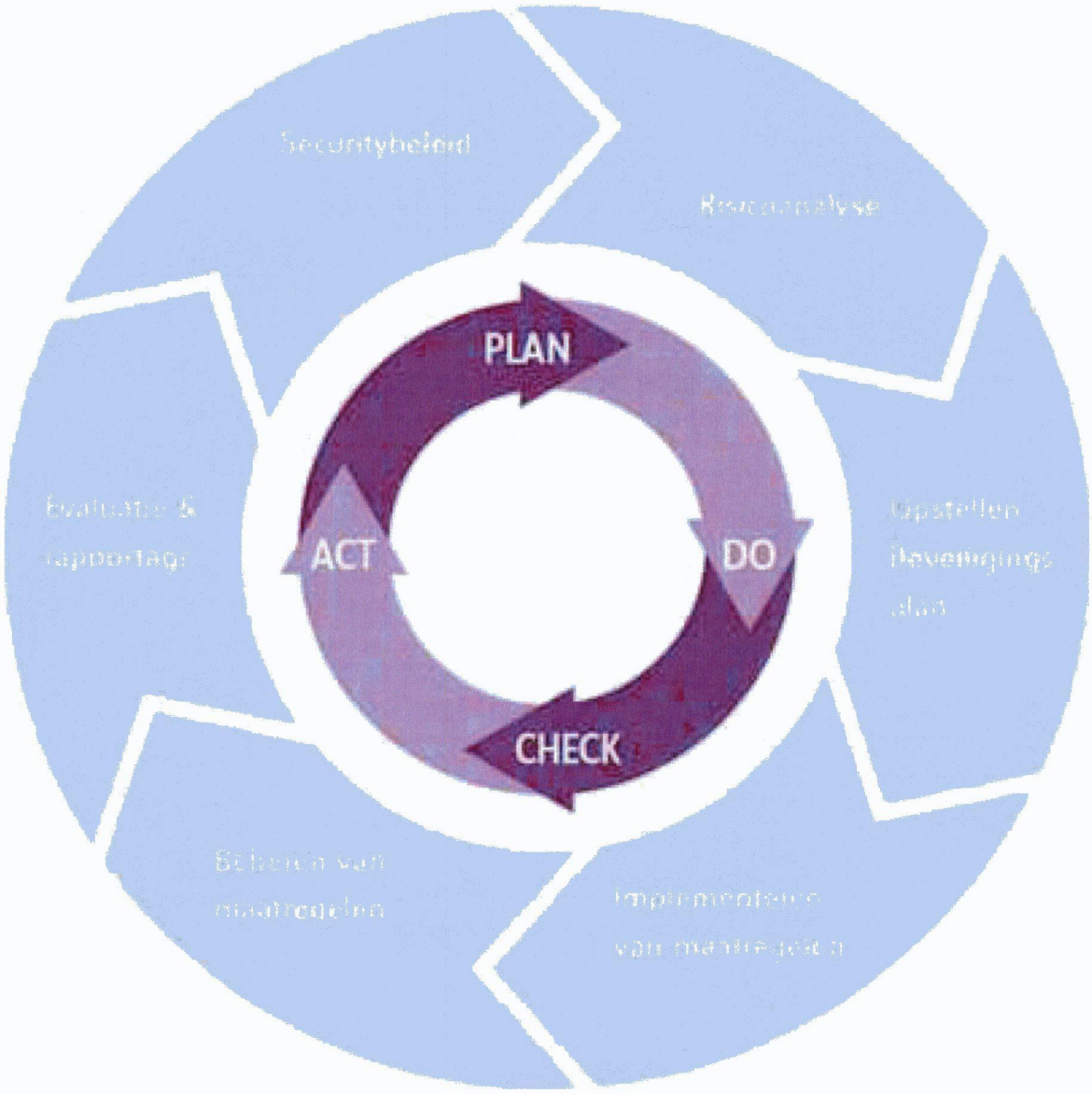
Voor wie
Dit beleid geldt voor de hele gemeentelijke organisatie en is gebaseerd op de landelijke Baseline Informatiebeveiliging Gemeenten.

Organisatie van informatiebeveiliging
De gemeente heeft een verantwoordelijke voor informatiebeveiliging aangesteld, zoals tevens wordt geadviseerd. Deze functie is geborgd in de vorm van de Information Security Manager (ISM), als staffunctionaris onder de clustermanager Info+, tevens rapporterend aan de directeur bedrijfsvoering en bestuur. Voor wat betreft de Wbp kennen grotere organisaties een eigen functionaris gegevensbescherming (FG), deze is formeel aangesteld door het College Bescherming Persoonsgegevens en functioneert als intern toezichthouder op privacy en persoonsgegevensbescherming in de informatieverwerking van de organisatie. Deze rol is ook geborgd bij de Information Security Manager.

Naast de ISM/FG zijn binnen de organisatie verschillende functies aanwezig met een bijzondere aandacht voor informatiebeveiliging. Zo kent de afdeling Burgerzaken een beveiligingsfunctionaris, heeft het cluster Sociale Dienstverlening beveiliging als aandachtsgebied geborgd in het takenpakket van de coördinator AO/IC, het cluster FM heeft binnen het team Services een coördinator beveiliging, bij HRM zijn de coördinator integriteit en ARBO-coördinator voor aanverwante gebieden van integriteit en veiligheid aangewezen.

Vier keer per jaar vind er een bijeenkomst plaats van de 'Beveiligingsadviescommissie' waaraan al deze functionarissen deelnemen. Hierin worden integrale beveiligings- en veiligheidsdiscussies gevoerd en aandachtsgebieden besproken.Verder vind zes keer per jaar een overleg beveiliging en veiligheid plaats met de directeur bedrijfsvoering.

Het proces Security Management is opgebouwd volgens een cyclische benadering, waarmee een zogenaamd Informatie Security Management System wordt gerealiseerd. De bedoeling hiervan is dat informatiebeveiliging als proces geborgd wordt in de organisatie en de cyclische benadering, de bekende Demming-cirkel, volgt. Hierbij worden verschillende fasen doorlopende die moeten zorgen dat er een continue verbetering van informatiebeveiliging wordt bewerkstelligd. Dit proces is in de figuur hieronder weergegeven.



Het proces van ISMS wordt uiteengezet in de ISO27001, de internationale standaard voor security management. Binnen de gemeente wordt gebruik gemaakt van dit proces voor borgen en bijhouden van security management. Binnen dit proces worden de Plan, Do, Check, Act stappen vastgelegd en kunnen de risicoanalyse resultaten opgeslagen.

Scope

De scope van dit beleid zijn de processen van de gemeente in de meest brede zin van het woord. Dit beleid is van toepassing op alle niet openbare ruimten van de gemeentelijke huisvestingspanden, alsmede op apparatuur die door gemeente ambtenaren gebruikt worden bij de uitoefening van hun taak op locatie en heeft betrekking op de informatie die daarbinnen verwerkt wordt. Binnen de scope van dit beleid vallen alle op dit moment geldende normen en regels op het gebied van informatiebeveiliging die door derden aan de gemeente opgelegd zijn. Dit beleid bevat minimaal al deze maatregelen en brengt ze met elkaar in verband. Binnen de scope is ook rekening gehouden met de verregaande digitalisering van de overheid en met de in de toekomst nog volgende basisregistraties of aanvullingen op bestaande basisregistraties.

Randvoorwaarden

Dit beleid kan niet gedeeltelijk worden geïmplementeerd, er bestaat geen stukje informatiebeveiliging. Dit beleid is het afgewogen minimale beveiligingsniveau waaraan een gemeente zou moeten willen voldoen. De maatregelen hebben een samenhang. Dus indien gekozen wordt voor het invoeren van dit beleid, dan kan dat alleen zoals deze is.

Doelgroepen

Dit beleid bevat aandachtsgebieden voor verschillende doelgroepen. Hieronder worden per doelgroep de hoofdstukken genoemd die relevant zijn.

IB functionarissen Informatiebeveiligingsfunctionarissen van alle niveaus	**Alle hoofdstukken**
Lijnmanager in zijn personeelsverantwoordelijkheid De lijnmanager is verantwoordelijk voor het handhaven van de personele beveiliging met eventuele ondersteuning door Personeelszaken.	**Zie hoofdstukken 6 en 8**
Lijnmanager in zijn verantwoordelijkheid voor de uitvoering van de processen De lijnmanager is verantwoordelijk voor het uitvoeren van activiteiten in processen (algemene procesverantwoordelijkheid) op basis van beschreven inrichting ervan. De verantwoordelijkheid voor de naleving van specifieke beveiligingsaspecten hangt af van het soort proces.	**Zie hoofdstukken 6, 10, 12, 13 en 14**
Beleidsmakers De beleidsmakers zijn verantwoordelijk voor het ontwikkelen van een veilig en werkbaar beleid. Het beleid moet goed uitvoerbaar en controleerbaar zijn.	**Zie hoofdstukken 5, 6, 10 en 12**
Personeelszaken Personeelszaken is verantwoordelijk voor werving, selectie en algemene zaken rond het functioneren van personeel, inclusief bewustwording en gedrag.	**Zie hoofdstukken 8 en 13**
Fysieke beveiliging Fysieke beveiliging is vaak belegd bij Facility Management of bewakingsdiensten. Zij zijn verantwoordelijk voor de beveiliging van percelen, panden en ruimtes.	**Zie hoofdstuk 9**
IT-diensten en IT-infrastructuren De IT diensten en infrastructuren zijn ondersteunend aan bijna alle processen. De eisen die aan IT voorzieningen gesteld worden zijn hierdoor zeer ingrijpend en bepalen voor een significant deel de inrichting van het IT landschap.	**Zie hoofdstukken 6, 10, 11 en 12**
Applicatie eigenaren en systeemeigenaren Applicatie eigenaren en systeemeigenaren zijn verantwoordelijk voor de veilige en correcte verwerking van de relevante data binnen de applicatie.	**Zie hoofdstukken 7, 10 en 12**
Eindgebruikers Een belangrijk onderdeel van informatiebeveiliging is de eindgebruiker.	**Alle hoofdstukken**
Informatiebeveiligingsadviseurs en IT auditors Bij het helpen bepalen welke maatregelen relevant zijn en het controleren of de maatregelen daadwerkelijk genomen zijn is het hele document relevant.	**Alle hoofdstukken**
Externe leveranciers De externe leveranciers zijn een bijzondere doelgroep. De opdrachtgever / systeemeigenaar is altijd verantwoordelijk voor de kwaliteit en veiligheid van uitbestede diensten. De opdrachtgever eist van de externe leveranciers dat zij voldoen aan alle aspecten van het beleid die voor de dienst of het betreffende systeem van belang zijn. Denk hier zeker ook aan de WBP en het afsluiten van een bewerkersovereenkomst en de jaarlijks audit hierop.	

Basis beveiligingsniveau
Binnen het vakgebied informatiebeveiliging wordt onderscheid gemaakt tussen beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid. Dit beleid sluit hierbij aan.

Beschikbaarheid
Dit beleid definieert een basis set aan eisen voor beschikbaarheid voor de gemeentelijke en (decentrale) overheid infrastructuur. Deze dient als basis voor het maken van afspraken over de beschikbaarheid tussen de eigenaar van het informatiesysteem en de dienstenleverancier. Dit houdt in dat voor de beschikbaarheid van de informatievoorziening een minimale set van normen wordt opgesteld waarbij per dienst en/of applicatie nadere afspraken gemaakt kunnen worden.

Integriteit
De integriteit op het vlak van informatievoorziening valt normaliter in twee delen uiteen: de integriteit van datacommunicatie en opslag enerzijds (d.w.z. niet gerelateerd aan het proces zelf), en de integriteit van de informatie in de applicaties (d.w.z. gerelateerd aan het proces zelf). Integriteit gekoppeld aan de applicatie is altijd situatieafhankelijk en afhankelijk van de eisen van een specifiek proces. Voor de functionele integriteit van de informatievoorziening wordt er een minimale set van normen opgesteld waarbij er per dienst en/of applicatie nadere afspraken gemaakt kunnen worden.

Vertrouwelijkheid
Het beleid beschrijft de maatregelen die nodig zijn voor het basisvertrouwelijkheidsniveau (gemeentelijk) Vertrouwelijk en Wbp risicoklasse 2.

Rubricering
Het basisvertrouwelijkheidniveau is vastgesteld als "Vertrouwelijk", zoals gedefinieerd in het Besluit Voorschrift Informatiebeveiliging Rijksdienst-Bijzondere Informatie (VIRBI:2012), en met betrekking tot de bescherming van privacygevoelige informatie wordt uitgegaan van de eisen die de Wbp stelt, en de beveiligingseisen die zijn gedefinieerd in het document 'Richtsnoeren Beveiliging Persoonsgegevens' van het College Bescherming Persoonsgegevens, gepubliceerd in februari 2013.

Dit betekent dat het standaard berichtenverkeer binnen de overheid behandeld wordt met middelen en processen die berekend zijn op de vertrouwelijkheidniveaus Wbp en Vertrouwelijk. Een medewerker hoeft zich dan niet per geval af te vragen of het medium waarover hij het bericht of informatie verstuurt voldoende veilig is en of de ontvangende organisatie het bericht wel voldoende veilig behandelt. De verzender kan er van uit gaan dat een ontvangende partij binnen de overheid de informatie op een voldoende vertrouwelijke manier behandelt. Het beleid beschrijft de beveiligingsmaatregelen daarvoor. Niet alleen voor werken op kantoor maar ook voor plaats en tijd onafhankelijk werken met vaste of mobiele apparatuur.

Op het moment dat een organisatie er bewust voor kiest bepaalde informatie openbaar te maken (overheidswebsites, correspondentie naar externe partijen e.d.) kiest de verantwoordelijke medewerker of die bepaalde informatie naar de beoogde ontvangers kan en of de kanalen daarvoor geschikt zijn. Dat is de verantwoording van de betreffende medewerker voor de specifieke, per geval door hem beoordeelde informatie. Hetzelfde geldt voor het doorsturen van informatie naar privé-mail. De medewerker bepaalt dan per geval of de betreffende informatie doorgestuurd kan worden. Automatisch doorzending van alle mail naar een privéadres of andere onveilige omgeving wordt dan ook niet toegestaan omdat dan niet per bericht door de medewerker beoordeeld kan worden of de informatie naar een onvoldoende veilige omgeving kan worden gestuurd.

VEILIGHEID

BEGRIPPEN

Audittrail	Vastlegging van de complete keten van opeenvolgende wijzigingen op een object in een bepaalde periode.
Basis beveiligingsniveau	Het geheel van maatregelen van beveiliging dat wordt bereikt door het implementeren en toepassen van de normen zoals geformuleerd in de Code voor Informatiebeveiliging, Business Continuïty Management en WBP risicoklasse 2 en waaraan de NORA een nadere uitwerking geeft, onder meer door normen voor IT-voorzieningen.
Bedrijfsmiddel	Elk middel waarin of waarmee bedrijfsgegevens kunnen worden opgeslagen en/of verwerkt en waarmee toegang tot gebouwen, ruimten en IT-voorzieningen kan worden verkregen: een bedrijfsproces, een gedefinieerde groep activiteiten, een gebouw, een apparaat, een IT-voorziening of een gedefinieerde groep gegevens.
Beschikbaarheid	De waarborg dat vanuit hun functie geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen (informatiesystemen).
Beveiliging	Het brede begrip van informatiebeveiliging, d.w.z. inclusief fysieke beveiliging, Business Continuïty Management (BCM), ofwel beschikbaarheid van bedrijfsprocessen en persoonlijke veiligheid en integriteit.
Beveiligingsincident	Het manifest worden van een beveiligingsrisico (dreiging, oorzaak) als gevolg van een overtreding van beveiligingsregel, bijv. onbevoegde toegang tot IT-voorzieningen.
Beveiligingsinstellingen	In IT-voorzieningen kunnen in veel gevallen functionaliteiten die invloed hebben op beveiliging geactiveerd, gewijzigd of uitgeschakeld worden door het opgeven van parameterwaarden.
Clear Desk	Anders dan Clean Desk, waarbij het bureau helemaal leeg is, betekent Clear Desk dat er geen vertrouwelijke informatie op het bureau ligt.
Controleerbaarheid	De mate waarin de werkelijkheid of representaties daarvan toetsbaar zijn, dat wil zeggen te vergelijken met andere "werkelijkheden of representaties daarvan" zodat objectieve oordeelsvorming mogelijk wordt.
Elektronische handtekening	Een elektronische handtekening is een methode voor het bevestigen van de juistheid van digitale informatie door middel van technieken van de asymmetrische cryptografie. De elektronische handtekening bestaat uit twee algoritmen: een om te bevestigen dat de informatie niet door derden veranderd is, de ander om de identiteit te bevestigen van degene die de informatie "ondertekent". De technieken worden toegepast met behulp van een PKI.
Filtering	Het gecontroleerd doorlaten van gegevens op het grensvlak tussen zones in een netwerk.
Firewall	Het geheel van software- en eventueel ook hardware voorzieningen dat voorkomt dat ongewenst verkeer van de ene netwerkzone terecht komt in de andere, teneinde de veiligheid in de laatstgenoemde te verhogen.
Hardening	Overbodige functies in besturingssystemen uitschakelen en/of van het systeem verwijderen en zodanige waarden toekennen aan beveiligingsinstellingen dat een maximale beveiliging ontstaat.
IB-functie	Een geheel van automatische informatiebeveiligingsverwerkingen die logisch met elkaar samenhangen.
IT-voorzieningen	Applicaties en technische infrastructuur, of wel het geheel van IT-voorzieningen.

In control statement	Binnen de gebruikelijke Planning en Control cyclus moet door B&W een in control statement worden afgegeven over informatiebeveiliging. De in control verklaring moet inzicht geven aan welke informatiebeveiligingsnormen wordt voldaan en voor welke normen een 'leg uit' is gedefinieerd.
Informatiebeveiliging	Het proces van vaststellen van de vereiste betrouwbaarheid van informatieverwerking in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.
Informatiesysteem	Een samenhangend geheel van gegevensverzamelingen en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie.
Integrale beveiliging	Integrale beveiliging is de beveiliging van vastgestelde te beschermen belangen (TBB) door op basis van risicomanagement en een kosten/batenanalyse een samenhangend stelsel van beveiligingsmaatregelen te selecteren en te implementeren. Het besturingsmodel voor integrale beveiliging sluit aan bij de besturingsuitgangspunten binnen de overheid: het lijnmanagement is integraal verantwoordelijk en dus ook voor de beveiliging.
Integriteit	Het waarborgen van de juistheid en volledigheid en tijdigheid van informatie en de verwerking ervan. Als de tijdigheid van gegevens bepaald wordt door omstandigheden buiten het systeem, kan deze vanzelfsprekend niet als integriteitseis voor het systeem gesteld worden.
Logging	Vastlegging van systeemhandelingen.
Malware	Software met ongewenste functies, zoals virussen en trojans.
Mobile code	Code afkomstig van een ander systeem die lokaal uitgevoerd wordt, bijv. Javascript, Flash of Silverlight.
Onvertrouwd	Geen zekerheid over het beveiligingsniveau of zekerheid over het lager dan vereiste beveiligingsniveau
Onweerlegbaarheid	Het niet kunnen ontkennen iets te hebben gedaan (bijvoorbeeld een bericht te hebben ontvangen dan wel te hebben verstuurd).
Patch	Klein onderdeel van software dat de leverancier van software uitgeeft om fouten aan door hem vervaardigde software te repareren
Query	Bevraging in een vraagtaal, die op basis van gebruikersvriendelijke en krachtige commando's selecties en berekeningen op bestanden kan uitvoeren, in eerste instantie alleen voor raadpleegdoeleinden.
Technische infrastructuur	Het geheel van IT-voorzieningen voor generiek gebruik, zoals servers, firewalls, netwerkapparatuur, besturingssystemen voor netwerken en servers, database management systemen en beheer- en beveiligingstools, inclusief bijbehorende systeembestanden.
Two-factor authenticatie	Two-factor authenticatie vereist het gebruik van twee van de drie volgende authenticatiemethoden: • Iets dat de gebruiker weet (b.v. wachtwoord, PIN); • Iets dat de gebruiker heeft (b.v. toegangspas, sleutel); en • Iets dat de gebruiker is (b.v. biometrische eigenschap zoals een vingerafdruk).
Vertrouwd	In overeenstemming met een door een bevoegde autoriteit vastgesteld beveiligingsniveau. Bijvoorbeeld vertrouwde zones of vertrouwde netwerken zoals in 10.6.1.2 en 10.6.1.3.
Vertrouwelijkheid	Het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe zijn geautoriseerd.
Vertrouwelijke informatie	Informatie die niet algemeen bekend mag worden (bron: van Dale) In het kader van de BIG worden maatregelen beschreven die voldoen voor de behandeling van gerubriceerde informatie tot en met vertrouwelijk en persoonsvertrouwelijke informatie zoals gedefinieerd in de Wbp.
Verwijderbare media	Opslagmiddelen die los van apparatuur kunnen worden verwijderd en meegenomen. Zoals CDROMs, USB sticks, verwijderbare schijven, tapes of gedrukte media.

VEILIGHEID

INFORMATIEBEVEILIGING ONDER ARCHITECTUUR

Beveiliging onder architectuur

Dit beleid bevat maatregelen en processen. De volgende processen ontstaan bij het invoeren van informatie beveiligingsbeleid:

- Informatiebeveiligingsbeleid

Het treffen en onderhouden van een samenhangend pakket van maatregelen ter waarborging van de betrouwbaarheid van het informatievoorzieningsproces.

- Risicomanagement

Risicomanagement is het systematisch opzetten, uitvoeren en bewaken van acties om risico's te identificeren, te prioriteren en te analyseren en voor deze risico's oplossingen te bedenken, te selecteren en uit te voeren.

- Incidentmanagement

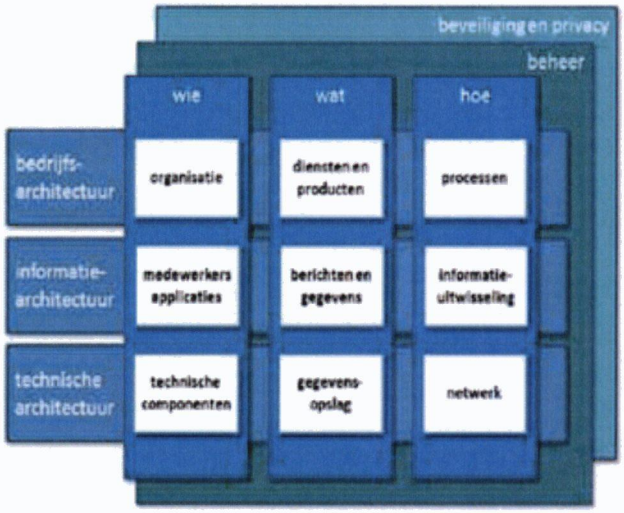
Een incident, in het kader van incident management, is een gebeurtenis die de bedrijfsvoering negatief kan beïnvloeden. Incidentmanagement is het geheel van organisatorische maatregelen dat ervoor moet zorgen dat een incident adequaat gedetecteerd, gemeld en behandeld wordt om daarmee de kans op uitval van bedrijfsvoering processen of schade ontstaan als gevolg van het incident te minimaliseren, dan wel te voorkomen.

- Bedrijfscontinuïteit management

Bedrijfscontinuïteit management is een proces waarbij de organisatie de nodige maatregelen treft om ongeacht de omstandigheden de continuïteit van de meest kritische processen te garanderen. In geval van een onderbreking van een of meerdere van deze processen moet de organisatie in staat zijn snel en kordaat op te treden opdat deze activiteiten binnen de kortst mogelijke termijn kunnen worden hersteld.

Een product van bedrijfscontinuïteit management is een bedrijfscontinuïteitsplan. Dit is het plan, waarin de maatregelen en belangrijke gegevens van de bedrijfsprocessen van uw organisatie worden beschreven, die tot doel hebben de onderbrekingstijd tot een minimum te beperken.

De scope van informatiebeveiliging
Informatiebeveiliging gaat over de betrouwbaarheid van de informatievoorziening van een organisatie, en heeft tot doel risico's tot een acceptabel niveau terug te brengen. Voor een juiste borging van dit kwaliteitsaspect is een evenwichtig stelsel van maatregelen nodig. Deze maatregelen zijn divers van aard, en verspreid over alle onderdelen en hiërarchische niveaus van een organisatie. Dit wordt geïllustreerd in het 9-vlaks architectuurmodel van NORA.



Informatiebeveiliging gaat uit van processen binnen een organisatie en de binnen deze processen gebruikte informatie en informatiesystemen. Informatiebeveiliging gaat dus niet alleen over systemen en reikt dan ook verder en zegt bijvoorbeeld ook iets over bijvoorbeeld toegangsbeveiliging, personeel en beleid.

In het document ***'Basis- en architectuurprincipes gemeente Haarlemmermeer'*** zijn de beveiligingsprincipes vastgelegd en verankerd als architectuurprincipes voor de gemeente Haarlemmermeer.

Informatiebeveiligingsmaatregelen zijn procedureel, technisch of organisatorisch van aard. En de verantwoordelijkheid voor het invoeren van bepaalde maatregelen ligt bij verschillende personen binnen een organisatie, HR maatregelen zullen vallen onder verantwoordelijkheid van HRM en bijvoorbeeld informatiesysteem technische maatregelen onder ICT en bijvoorbeeld toegangscontrole maatregelen bij Facility Management. Informatiebeveiliging is daarmee niet puur het domein van de cluster Info+! Informatiebeveiliging omvat alle informatie die een organisatie nodig heeft om haar processen naar behoren uit te kunnen voeren.

Samenhang in maatregelen
Het is van belang dat de focus op het geheel van de aandachtsgebieden Mens en Organisatie, Basisinfrastructuur en ICT gericht wordt. Het nemen van technische maatregelen alleen, is onvoldoende. Veelal wordt gesteld dat het bewustzijn van de gebruiker de belangrijkste basis is voor een goede informatiebeveiliging. Inderdaad: onbewuste gebruikers, nemen onbewust veel risico's. Er zijn ook gebruikers die bewust risico lopen zoals de medewerker die nog even een rapport op tijd af wil krijgen en vertrouwelijke informatie op een USB-stick zet om er thuis verder aan te werken.

Dit is met beveiliging op het gebied van ICT en toegangsbeveiliging slechts ten dele weg te nemen. De diverse maatregelen (uit de aandachtsgebieden Mens en Organisatie, Basisinfrastructuur en ICT) moeten daarom in samenhang worden genomen. Alleen op deze wijze kan er sprake zijn van een goed informatiebeveiligingsbeleid.

Noodzakelijkheid
Twee van de belangrijkste uitdagingen voor gemeenten zijn op dit moment:
1. Het optimaliseren van de kwaliteit van de dienstverlening waardoor deze blijft voldoen aan de verwachtingen van burgers en ondernemingen;
2. Het efficiënter laten functioneren van de gemeentelijke organisatie, met minder middelen, mensen en administratieve lasten voor burgers en ondernemingen.

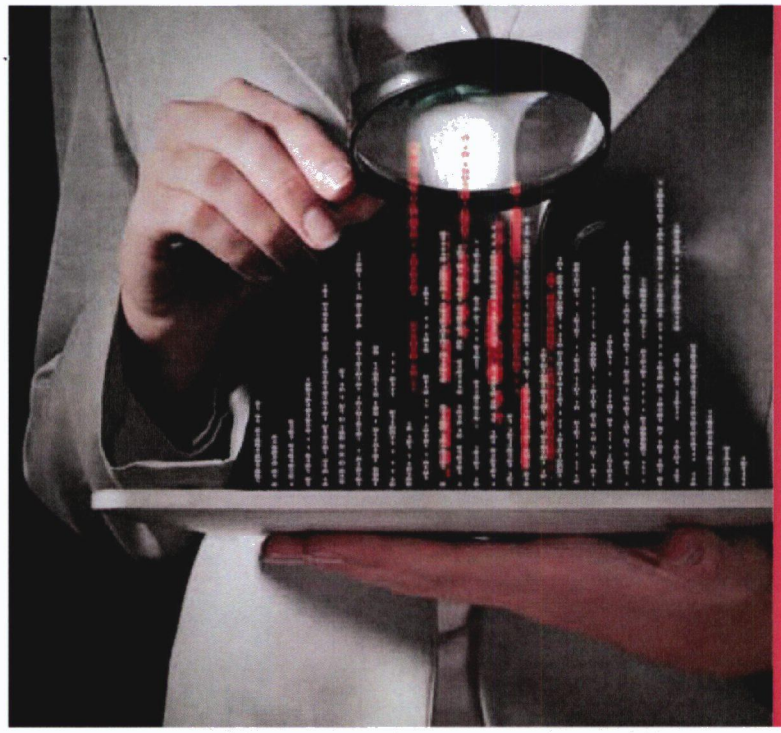
Die uitdagingen zullen door gemeenten verschillend tegemoet worden getreden, afhankelijk van bijvoorbeeld de omvang van de gemeente, de mate waarin al samenwerking met andere gemeenten plaatsvindt, de graad van informatisering, het gekozen besturingsmodel en de ontwikkelingsfase van de organisatie. Een aantal vragen is echter gemeenschappelijk:

- Hoe zorgen we ervoor dat de belanghebbenden zo optimaal mogelijk worden bediend?
- Hoe houden we in een complexe omgeving het overzicht?
- Hoe kunnen we de gemeentelijke organisatie verder verbeteren, goedkoper maken, professionaliseren?
- Hoe zorgen we dat de gemeente zich ontwikkelt tot dé poort van de overheid?
- Hoe vergroten we de greep op de informatiehuishouding waardoor deze een efficiënte organisatie mogelijk maakt?
- Op welke manier voldoen we aan de toenemende eis tot transparantie, doelmatigheid en rechtmatigheid BEVEILIGING en PRIVACY

De gemeente als informatieknooppunt
Met de verregaande decentralisatie van uitvoeringstaken en de centralisatie van de basisregistraties wordt de gemeente steeds meer een knooppunt waar veel ketens samenkomen. De gemeente wordt hierdoor een informatieknooppunt en daarmee is het belang van een goede informatiebeveiliging essentieel.

Het beveiligingsbeleid en de basisregistraties
Dit beleid is samengesteld uit maatregelen van de Baseline Informatiebeveiliging Rijksdienst en aangevuld met maatregelen uit diverse wetgeving, maar ook de specifieke maatregelen afkomstig uit de BAG, SUWI en GBA.

Door deze maatregelen mee te nemen in dit beleid ontstaat een geheel van maatregelen dat van toepassing is voor de gehele bedrijfsvoering van de gemeente. Dit sluit aan bij initiatieven waarbij steeds vaker in kantoortuinen gewerkt wordt en het is niet meer van belang is waar de ambtenaar zit/werkt.



VEILIGHEID

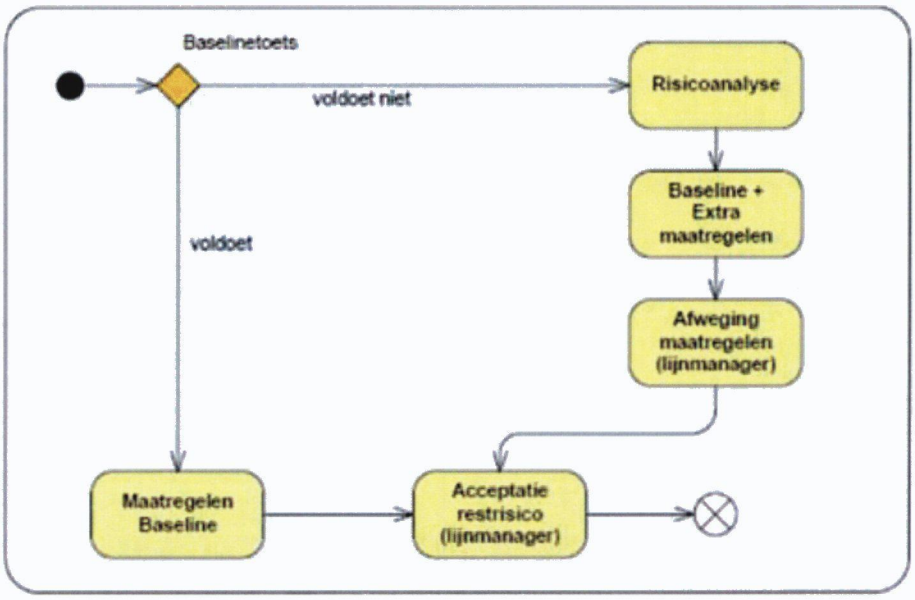
RISICOANALYSE ALS BASIS

Risico beoordeling en risico afweging
Volgens het "Beleid voor informatiebeveiliging" moet informatiebeveiliging op grond van een risicoafweging plaatsvinden. De mogelijke methodes hiervoor zijn risicoanalyse, baselinetoets, afhankelijkheid en kwetsbaarheid analyse of certificering. Het beveiligingsniveau van dit beleid is zo gekozen dat dit voor de meeste processen en ondersteunende IT voorzieningen bij de gemeente voldoende is.

Hiermee wordt voorkomen dat er voor ieder systeem een uitgebreide risicoanalyse uitgevoerd moet worden. Om vast te stellen dat het niveau van het beleid voldoende is, moet een baselinetoets uitgevoerd worden. Dit is schematisch weergegeven in het onderstaande figuur:

In de baselinetoets wordt onder meer bekeken of er geheime of geclassificeerde informatie verwerkt wordt, er sprake is van een WBP risicoklasse hoger dan 1, er hogere beschikbaarheid eisen vereist zijn of er dreigingen relevant zijn die niet in het dreiging profiel van dit beleid meegenomen zijn.

Voor wat betreft integriteit en vertrouwelijkheid is er sprake van hogere betrouwbaarheidseisen als het om geheimen (rubricering hoger dan Vertrouwelijk) of Wet Bescherming Persoonsgegevens risicoklasse 3 gaat. Hogere betrouwbaarheidseisen kunnen ook voorkomen als er een dreiging relevant is die niet in het dreiging profiel van dit beleid is meegenomen. Tot slot kan het mogelijk zijn dat een hogere beschikbaarheid noodzakelijk is. In deze gevallen zal een volledige risicoanalyse uitgevoerd moeten worden die kan leiden tot extra maatregelen.



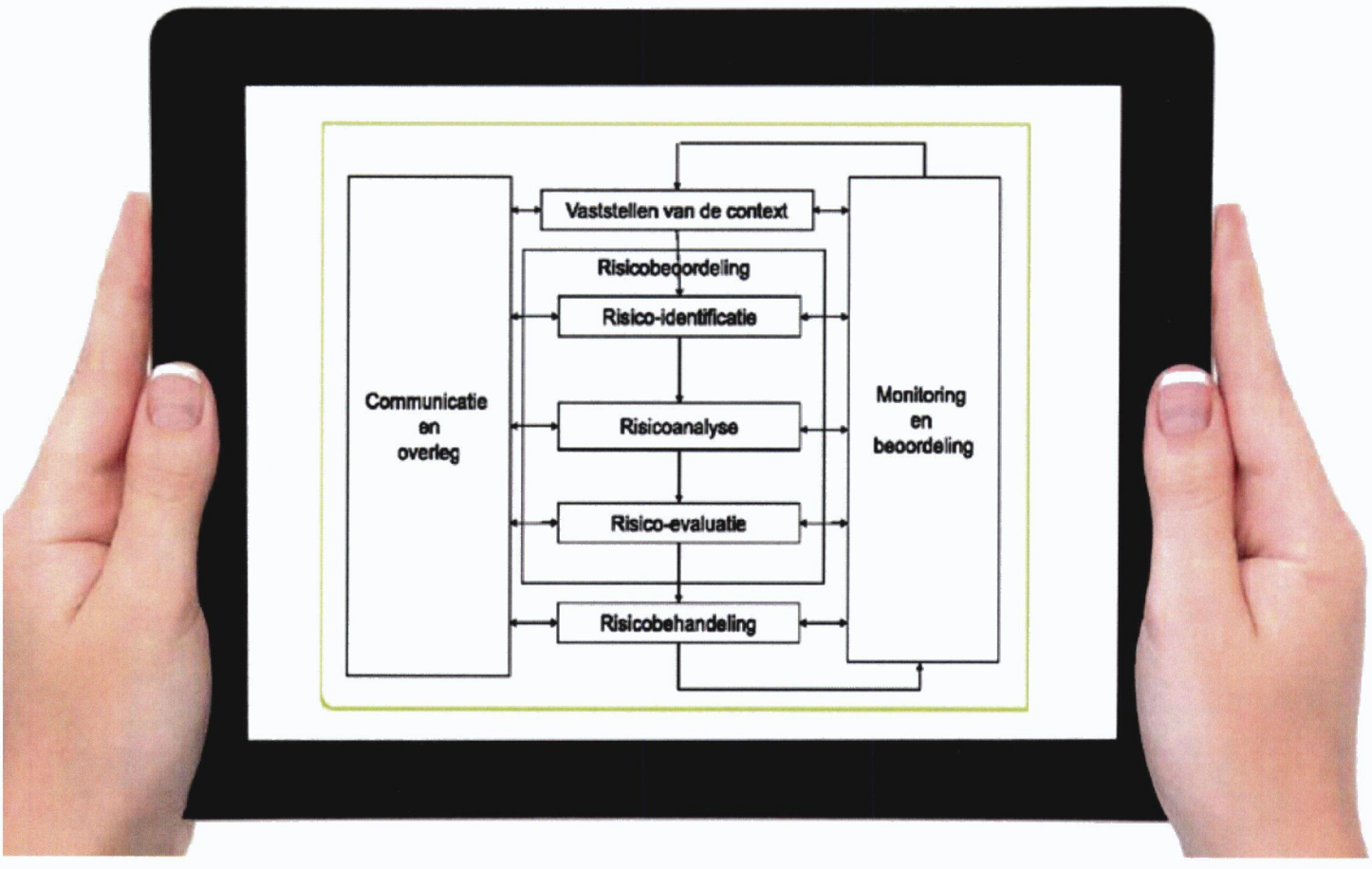
Acceptatie door de manager:
Er kan op verschillende manieren met (rest) risico's worden omgegaan. De meest gebruikelijke strategieën zijn:
1. Risicodragend.
2. Risiconeutraal.
3. Risicomijdend.

Risicodragend wil zeggen dat we sommige risico's accepteren. Dat kan zijn omdat de kosten van de beveiligingsmaatregelen de mogelijke schade overstijgen. Maar het management kan ook besluiten om niets te doen ondanks dat de kosten niet hoger zijn dan de schade die kan optreden.

- De maatregelen die een risicodragende organisatie neemt op het gebied van informatiebeveiliging zijn veelal van repressieve aard.
- Onder risiconeutraal wordt verstaan dat er dusdanige beveiligingsmaatregelen worden genomen dat dreigingen of niet meer manifest worden of, wanneer de dreiging wel manifest wordt, de schade als gevolg hiervan geminimaliseerd is. De meeste maatregelen die een risico neutrale organisatie neemt op het gebied van informatie beveiliging zijn een combinatie van preventieve, detec tieve en repressieve maatregelen.
- Onder risicomijdend verstaan we dat er zodanige maatregelen worden genomen dat de dreigingen zo veel mogelijk worden geneutraliseerd; zodat de dreiging niet meer tot een incident leidt.

Denk hierbij aan het invoeren van nieuwe software waardoor de fouten in de oude software geen dreiging meer vormen. In simpele bewoordingen: een ijzeren emmer kan roesten. Neem een kunststof emmer en de dreiging, roest, valt weg. Veel van de maatregelen binnen deze strategie hebben een preventief karakter.

De gekozen strategie zal bewust door het management moeten worden gemaakt en de gevolgen ervan gedragen. Bij de uitvoering van de risicoanalyse stappen wordt gehandeld conform de ISO27005 standaard voor risico management op het proces informatiebeveiliging, zie onderstaande schema.



VEILIGHEID

IMPLEMENTATIE EN RAPPORTAGE

Uitvoering van GAP-analyse
De GAP-analyse geeft als instrument antwoord op vragen als: 'Waar zijn we nu' en 'Waar willen we heen'. Met het gebruiken van het 'Normen kader informatiebeveiliging' weet de gemeente nog niet wat er gedaan moet worden om het 'Normen kader informatiebeveiliging' ingevoerd te krijgen. Door middel van de GAP-analyse kan de gemeente met het stellen van vragen vaststellen welke 'Normen kader informatiebeveiliging' -maatregelen al ingevoerd zijn, en belangrijker, welke maatregelen van het 'Normen kader informatiebeveiliging' nog niet ingevoerd zijn.

Met het gevonden resultaat kan vervolgens planmatig worden omgegaan en kunnen de actiehouders beginnen met het invoeren van maatregelen en hierover ook periodiek in de managementrapportages over rapporteren.
Na het uitvoeren van de GAP-analyse kan het beste worden begonnen met de maatregelen die het minste geld kosten. Relatief gezien wordt hier vaak ook het meeste resultaat behaald tegen de laagste kosten.

Information Security Management System
Het is noodzakelijk dat ontbrekende beveiligingsmaatregelen die veel tijd kosten of kostbaar zijn planmatig worden ingevoerd. Maak een plan om te komen tot implementatie van deze maatregelen en stuur op de voortgang. Daarbij horen goede rapportages van de verantwoordelijken die benoemd zijn om specifieke maatregelen in te voeren. Dit plan heet een Information Security Management System (ISMS). In overeenstemming met het gestelde beleidsuitgangspunt in het 'Beleid voor informatiebeveiliging' dient de beheersing van deze planning opgenomen te worden in de planning en control-cyclus en jaarlijks geëvalueerd te worden.

Implementatie plan
De combinatie van resultaten uit de GAP-analyse, risicoanalyse resultaten en de geformuleerde speerpunten m.b.t. beveiligingsbeleid kan in overleg met de verantwoordelijk managers worden afgestemd welke maatregelen worden getroffen, wat de kosten/baten analyse is die hierbij hoort, etc.

Rapportage
Voor de rapportage rondom informatiebeveiliging worden de volgende periodieke rapportage afgesproken;

Bestuursrapportage: Zal plaatsvinden als onderdeel van de PCC.
Directierapportage: Zal plaatsvinden als onderdeel van de PCC.
Directiebriefing: Briefing m.b.t. actuele trends en onderwerpen op het gebied van informatiebeveiliging in overleg met secretaris directie en de portefeuillehouder Bedrijfsvoering wordt de invulling en planning hiervan bepaald. Workshop voor risicoanalyse en speerpunt bepaling wordt hierin als belangrijk terugkerend onderdeel geadviseerd.
MT Briefing : Jaarlijks, wanneer een actueel onderwerp speelt of bijzondere aandacht behoeft, in overleg met de directie portefeuillehouder Bedrijfsvoering.
MT Info+ : Twee maandelijkse rapportage op verschillende ICT gerelateerde onderwerpen m.b.t. beveiliging.
MT's lijnorganisatie verbijzonderde beveiliging : Tenminste jaarlijks bij de clusters waar een specifiek beveiligingsplan van kracht is, momenteel cluster Klant Contact Centrum en cluster Sociale Dienstverlening.
MT's lijnorganisatie : Wanneer hier gevraagd behoefte aan is, of ongevraagd behoefte aan is vanuit de Information Security Manager. Met name bij beleidswijzigingen m.b.t. informatiebeveiliging kan hiertoe aanleiding zijn of wanneer structurele problemen op het gebied van informatiebeveiliging worden geconstateerd bij een organisatieonderdeel.

VEILIGHEID

INHOUDELIJK NORMENKADER

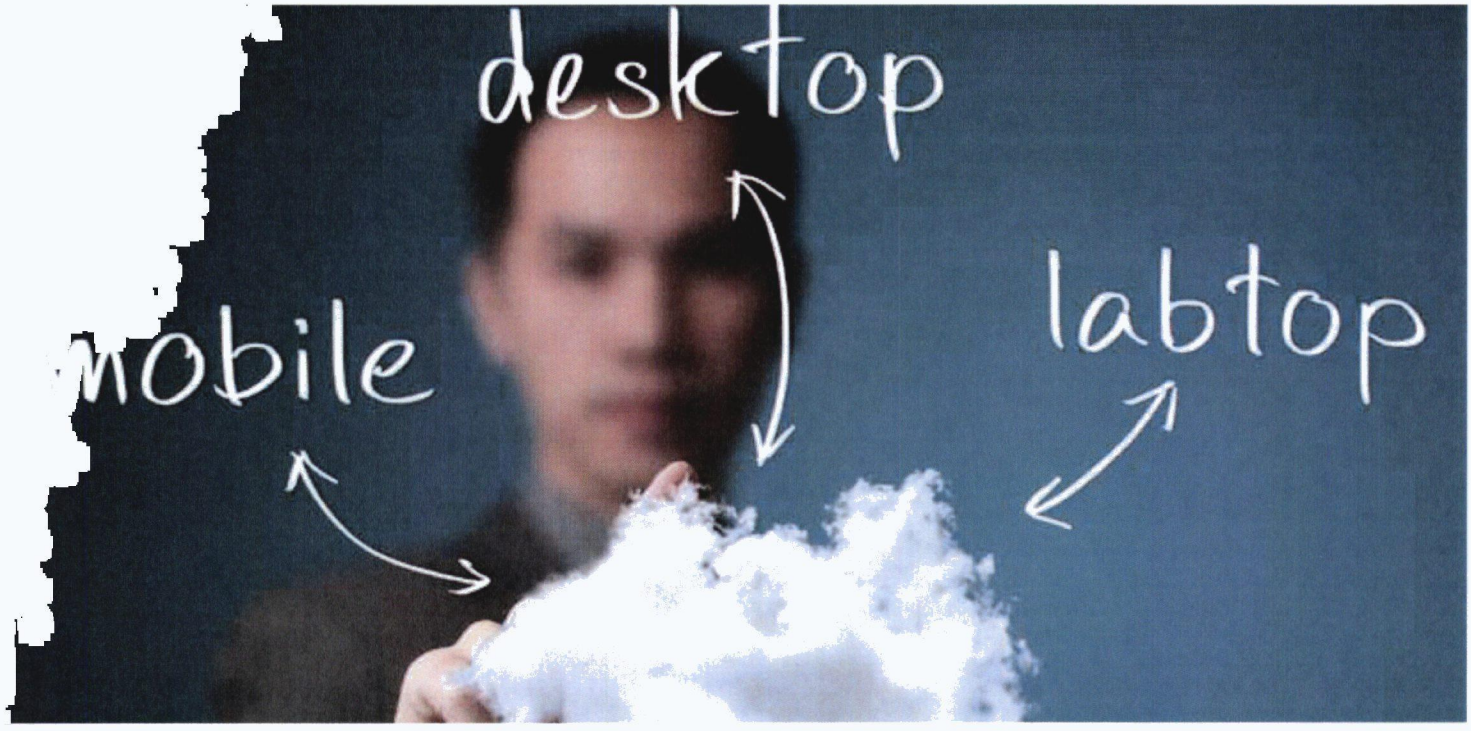
5.1 Informatiebeveiligingsbeleid

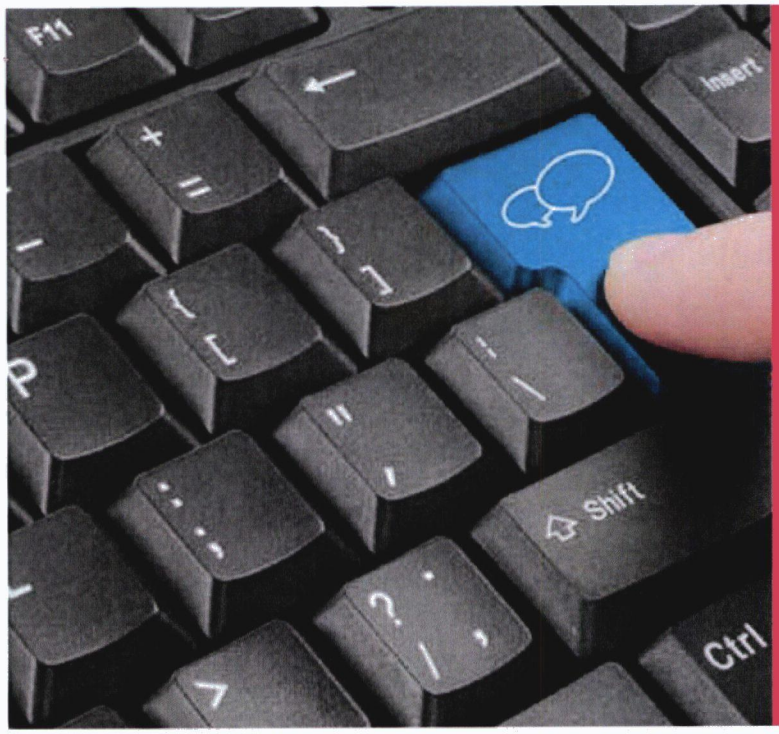
Doelstelling
Directie richting en ondersteuning bieden voor informatiebeveiliging overeenkomstig de bedrijfsmatige eisen en relevante wetten en voorschriften.

5.1.1 Beleidsdocumenten voor informatiebeveiliging
Een document met informatiebeveiligingsbeleid behoort door het College te worden goedgekeurd en gepubliceerd en kenbaar te worden gemaakt aan alle werknemers en relevante externe partijen.
Er is beleid voor informatiebeveiliging door het College vastgesteld, gepubliceerd en beoordeeld op basis van inzicht in risico's, kritische bedrijfsprocessen en toewijzing van verantwoordelijkheden en prioriteiten.

5.1.2 Beoordeling van het informatiebeveiligingsbeleid
Het informatiebeveiligingsbeleid behoort met geplande tussenpozen, of zodra zich belangrijke wijzigingen voordoen, te worden beoordeeld om te bewerkstelligen dat het geschikt, toereikend en doeltreffend blijft.

Het informatiebeveiligingsbeleid wordt minimaal één keer per vier jaar, of zodra zich belangrijke wijzigingen voordoen, beoordeeld en zo nodig bijgesteld. Zie ook 6.1.8.1.





VEILIGHEID

6. ORGANISATIE VAN DE INFORMATIEBEVEILIGING

6.1 Interne organisatie

Doelstelling
Beheren van de informatiebeveiliging binnen de organisatie.

6.1.1 Betrokkenheid van het college bij beveiliging

Het College behoort actief beveiliging binnen de organisatie te ondersteunen door duidelijk richting te geven, betrokkenheid te tonen en expliciet verantwoordelijkheden voor informatiebeveiliging toe te kennen en te erkennen. Het College waarborgt dat de informatiebeveiligingsdoelstellingen worden vastgesteld, voldoen aan de kaders zoals gesteld in dit document en zijn geïntegreerd in de relevante processen. Dit gebeurt door één keer per jaar opzet, bestaan en werking van de IB-maatregelen te bespreken in het overleg van de Raad en hiervan verslag te doen. Zie ook het in control statement zoals beschreven in het "Beleid voor informatiebeveiliging".

6.1.2 Coördineren van beveiliging

Activiteiten voor informatiebeveiliging behoren te worden gecoördineerd door vertegenwoordigers uit verschillende delen van de organisatie met relevante rollen en functies.

- De rollen van ISM (Information Security Manager) en het lijnmanagement zijn beschreven.
- De ISM (Information Security Manager) rapporteert rechtstreeks aan het hoogste management.
- De Information Security Manager bevordert en adviseert over de beveiliging van de gemeente, verzorgt rapportages over de status, controleert dat m.b.t. de beveiliging van de gemeente de maatregelen worden nageleefd, evalueert de uitkomsten en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging van de gemeente.

6.1.3 Verantwoordelijkheden

Alle verantwoordelijkheden voor informatiebeveiliging behoren duidelijk te zijn gedefinieerd.

- Elke lijnmanager is verantwoordelijk voor de integrale beveiliging van zijn of haar organisatieonderdeel.

6.1.4 Goedkeuringsproces voor it-voorzieningen

Er behoort een goedkeuringsproces voor nieuwe IT-voorzieningen te worden vastgesteld en geïmplementeerd.

- Er is een goedkeuringsproces voor nieuwe IT voorzieningen en wijzigingen in IT voorzieningen.

6.1.5 Geheimhoudingsovereenkomst

Eisen voor vertrouwelijkheid of geheimhoudingsovereenkomst die een weerslag vormen van de behoefte van de organisatie aan bescherming van informatie behoren te worden vastgesteld en regelmatig te worden beoordeeld.

- De algemene geheimhoudingsplicht voor ambtenaren is geregeld in de Ambtenarenwet art. 125a, lid 3. Daarnaast dienen personen die te maken hebben met Bijzondere Informatie een geheimhoudingsverklaring te ondertekenen, daaronder valt ook vertrouwelijke informatie. Hierbij wordt tevens vastgelegd dat na beëindiging van de functie, de betreffende persoon gehouden blijft aan die geheimhouding. Dit geldt ook voor externen die worden ingehuurd door de gemeente Haarlemmermeer.

6.1.6 Contact met overheidsinstanties
Er behoren geschikte contacten met relevante overheidsinstanties te worden onderhouden.

- Het lijnmanagement stelt vast in welke gevallen en door wie er contacten met autoriteiten (brandweer, toezichthouders, enz.) wordt onderhouden.

6.1.7 Contact met speciale belangengroepen
Er behoren geschikte contacten met speciale belangengroepen of andere specialistische platforms voor beveiliging en professionele organisaties te worden onderhouden.

- IB-specifieke informatie van relevante expertisegroepen, leveranciers van hardware, software en diensten wordt gebruikt om de informatiebeveiliging te verbeteren.
- De Information Security Manager onderhoud contact met de IBD en neemt zitting in het IBD-overleg.

6.1.8 Beoordeling van het informatiebeveiligingsbeleid
De benadering van de organisatie voor het beheer van informatiebeveiliging en de implementatie daarvan (d.w.z. beheers doelstellingen, beheersmaatregelen, beleid, processen en procedures voor informatiebeveiliging) behoren onafhankelijk en met geplande tussenpozen te worden beoordeeld, of zodra zich significante wijzigingen voordoen in de implementatie van de beveiliging.

- Het informatiebeveiligingsbeleid wordt minimaal één keer in de drie jaar geëvalueerd (door een externe onafhankelijke deskundige) en desgewenst bijgesteld. Zie ook 5.1.2.
- Periodieke beveiligingsaudits worden uitgevoerd in opdracht van het lijnmanagement.
- Over het functioneren van de informatiebeveiliging wordt, conform de P&C cyclus, jaarlijks gerapporteerd aan het lijnmanagement.

6.2 Externe Partijen

Doelstelling
Beveiligen van de informatie en IT-voorzieningen van de organisatie handhaven waartoe externe partijen toegang hebben of die door externe partijen worden verwerkt of beheerd, of die naar externe partijen wordt gecommuniceerd.

6.2.1 Identificatie van risico's die betrekking hebben op externe partijen
De risico's voor de informatie en IT-voorzieningen van de organisatie vanuit bedrijfsprocessen waarbij externe partijen betrokken zijn, behoren te worden geïdentificeerd en er behoren geschikte beheersmaatregelen te worden geïmplementeerd voordat toegang wordt verleend.

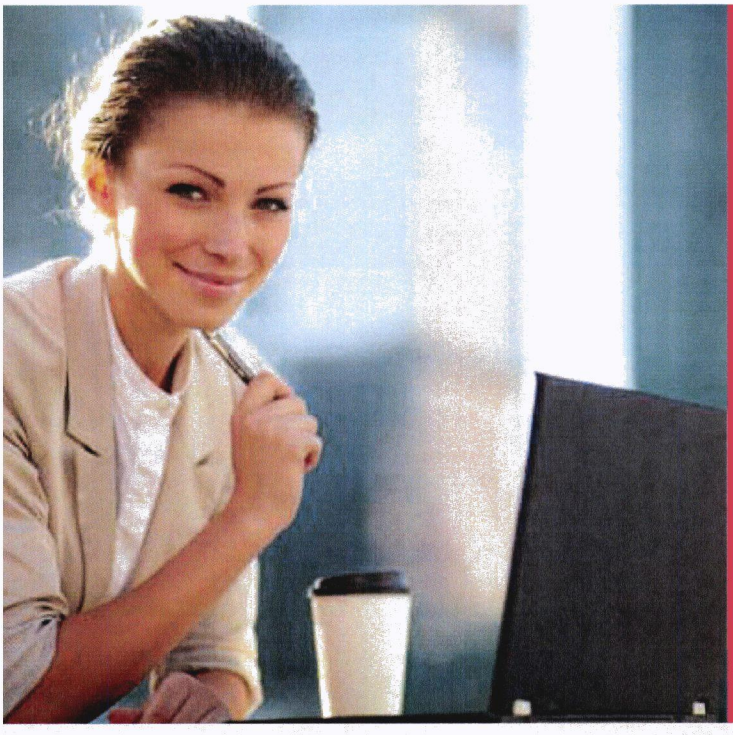
- Informatiebeveiliging is aantoonbaar (op basis van een risicoafweging) meegewogen bij het besluit een externe partij wel of niet in te schakelen.
- Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald welke toegang (fysiek, netwerk of tot gegevens) de externe 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 (bijv. risicoklasse II van WBP of de vertrouwelijkheidklasse) 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.
- Indien externe partijen systemen beheren waarin persoonsgegevens verwerkt worden, wordt een bewerkersovereenkomst (conform WBP artikel 14) 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. (zie ook 6.2.3.3). Ook wordt beschreven hoe die beveiligingsmaatregelen door de uitbestedende partij te controleren zijn (bijv. audits en penetratietests) en hoe het toezicht is geregeld.
- Over het naleven van de afspraken van de externe partij wordt jaarlijks gerapporteerd.

6.2.2 Beveiliging behandelen in de omgang met klanten
Alle geïdentificeerde beveiligingseisen behoren te worden behandeld voordat klanten toegang wordt verleend tot de informatie of bedrijfsmiddelen van de organisatie.

- Alle noodzakelijke beveiligingseisen worden op basis van een risicoafweging vastgesteld en geïmplementeerd voordat aan gebruikers toegang tot informatie op bedrijfsmiddelen wordt verleend.

6.2.3 Beveiliging behandelen in overeenkomsten met een derde partij
In overeenkomsten met derden waarbij toegang tot, het verwerken van, communicatie van of beheer van informatie of IT-voorzieningen van de organisatie, of toevoeging van producten of diensten aan IT-voorzieningen waarbij sprake is van toegang, behoren alle relevante beveiligingseisen te zijn opgenomen.

- De maatregelen behorend bij 6.2.1 zijn voorafgaand aan het afsluiten 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 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.
- Er is een plan voor beëindiging van de ingehuurde diensten waarin aandacht wordt besteed aan beschikbaarheid, vertrouwelijkheid en integriteit.
- 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 maakte 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.



VEILIGHEID

7. BEHEER VAN BEDRIJFSMIDDELEN / VERANTWOORDELIJKHEID VOOR BEDRIJFSMIDDELEN

Doelstelling
Bereiken en handhaven van een adequate bescherming van bedrijfsmiddelen van de organisatie.

7.1.1 Inventarisatie van bedrijfsmiddelen
Alle bedrijfsmiddelen behoren duidelijk te zijn geïdentificeerd en er behoort een inventaris van alle belangrijke bedrijfsmiddelen te worden opgesteld en bijgehouden.

- Er is een actuele registratie van bedrijfsmiddelen die voor de organisatie een belang vertegenwoordigen zoals informatie(verzamelingen), software, hardware, diensten, mensen en hun kennis/vaardigheden. Van elk middel is de waarde voor de organisatie, het vereiste beschermingsniveau en de verantwoordelijke lijnmanager bekend.

7.1.2 Eigendom van bedrijfsmiddelen
Alle informatie en bedrijfsmiddelen die verband houden met IT-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 verantwoordelijke lijnmanager benoemd.

7.1.3 Aanvaardbaar gebruik van bedrijfsmiddelen
Er behoren regels te worden vastgesteld, gedocumenteerd en geïmplementeerd voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met IT-voorzieningen.

- Er zijn regels voor acceptabel gebruik van bedrijfsmiddelen (met name internet, e-mail en mobiele apparatuur). Het CAR-UWO verplicht ambtenaren zich hieraan te houden. Voor extern personeel is dit in het contract vastgelegd.
- Gebruikers hebben kennis van de regels.
- Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen. De toestemming kan generiek geregeld worden in het kader van de functieafspraken tussen manager en medewerker.
- Informatiedragers worden dusdanig gebruikt dat vertrouwelijke informatie niet beschikbaar kan komen voor onbevoegde personen.
- Bij het gebruik van bedrijfsmiddelen zijn het ICT-middelen beleid en de Beveiligingsrichtlijnen voor mobiele apparaten (publicatie NCSC) van toepassing.

7.2 Classificatie van informatie

Doelstelling
Bewerkstelligen dat informatie een geschikt niveau van bescherming krijgt. Informatie behoort te worden geclassificeerd om bij het verwerken van de informatie de noodzaak, prioriteiten en verwachte graad van bescherming te kunnen aangeven.

7.2.1 Richtlijnen voor classificatie van informatie

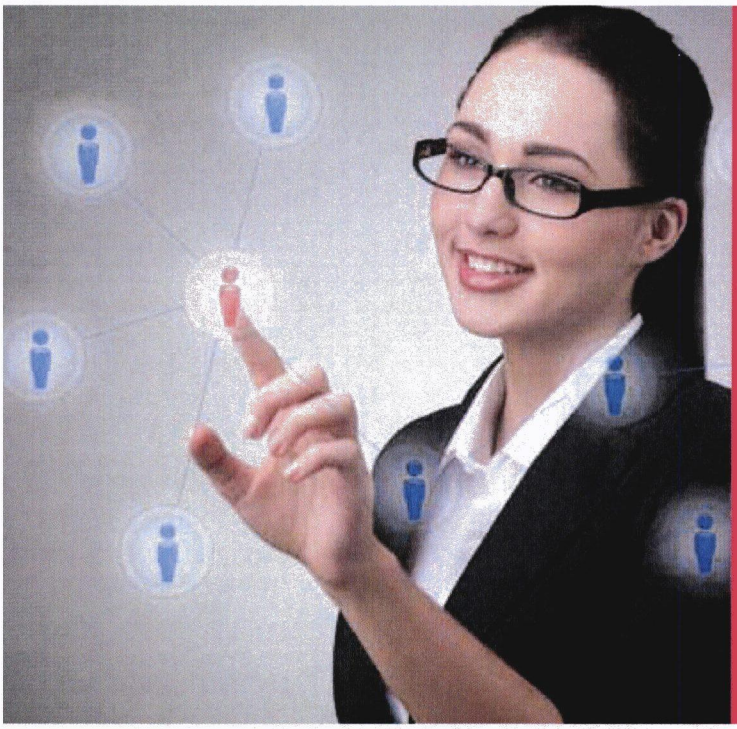
Informatie behoort te worden geclassificeerd met betrekking tot de waarde, wettelijke eisen, gevoeligheid en onmisbaarheid voor de organisatie.

- De organisatie heeft rubriceringrichtlijnen opgesteld.
- In overeenstemming met hetgeen in het WBP is vastgesteld, dient een helder onderscheid te zijn in de herleidbare (klasse II/III) en de niet herleidbare (klasse 0 en I) gegevens.

7.2.2 Labeling en verwerking van informatie

Er behoren geschikte, samenhangende procedures te worden ontwikkeld en geïmplementeerd voor de labeling en verwerking van informatie overeenkomstig het classificatiesysteem dat de organisatie heeft geïmplementeerd.

- De lijnmanager heeft maatregelen getroffen om te voorkomen dat niet-geautoriseerden kennis kunnen nemen van gerubriceerde informatie.
- De opsteller van de informatie doet een voorstel tot rubricering en brengt deze aan op de informatie. De vaststeller van de inhoud van de informatie stelt tevens de rubricering vast.



VEILIGHEID

8. PERSONELE BEVEILIGING

8.1 Beveiligen van personeel

Doelstelling

Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen, en geschikt zijn voor de rollen waarvoor zij worden overwogen, en om het risico van diefstal, fraude of misbruik van faciliteiten te verminderen.

8.1.1 Rollen en verantwoordelijkheden

De rollen en verantwoordelijkheden van werknemers, ingehuurd personeel en externe gebruikers ten aanzien van beveiliging behoren te worden vastgesteld en gedocumenteerd overeenkomstig het beleid voor informatiebeveiliging van de organisatie.

- De taken en verantwoordelijkheden van een medewerker zijn opgenomen in de functiebeschrijving (zie ook de Ambtenarenwet en WBP) en worden onderhouden. In de functiebeschrijving wordt minimaal aandacht besteed aan:
  - uitvoering van het informatiebeveiligingsbeleid bescherming van bedrijfsmiddelen
  - rapportage van beveiligingsincidenten
  - expliciete vermelding van de verantwoordelijkheden voor het beveiligen van persoonsgegevens
- Alle ambtenaren en ingehuurde medewerkers krijgen bij hun aanstelling hun verantwoordelijkheden ten aanzien van informatiebeveiliging ter inzage. De schriftelijk vastgestelde en voor hen geldende regelingen en instructies ten aanzien van informatiebeveiliging, welke zij bij de vervulling van hun dienst hebben na te leven, worden op een gemakkelijk toegankelijke plaats ter inzage gelegd. Overeenkomstige voorschriften maken deel uit van de contracten met externe partijen. Ook voor hen geldt de toegankelijkheid van geldende regelingen en instructies.
- Indien een medewerker speciale verantwoordelijkheden heeft t.a.v. informatiebeveiliging dan is hem dat voor indiensttreding (of bij functiewijziging), bij voorkeur in de aanstellingsbrief of bij het afsluiten van het contract, aantoonbaar duidelijk gemaakt.
- De algemene voorwaarden van het arbeidscontract van medewerkers bevatten de wederzijdse verantwoordelijkheden ten aanzien van beveiliging. Het is aantoonbaar dat medewerkers bekend zijn met hun verantwoordelijkheden op het gebied van beveiliging.

8.1.2 Screening

Verificatie van de achtergrond van alle kandidaten voor een dienstverband, ingehuurd personeel en externe gebruikers behoren te worden uitgevoerd overeenkomstig relevante wetten, voorschriften en ethische overwegingen, en behoren evenredig te zijn aan de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend, en de waargenomen risico's.

- Voor alle medewerkers (ambtenaren en externe medewerkers) is minimaal een relevante Verklaring Omtrent het Gedrag (VOG) vereist. Indien het een vertrouwensfunctie betreft wordt ook een veiligheidsonderzoek (Verklaring van Geen Bezwaar) uitgevoerd.
- Bij de aanstelling worden de gegevens die de medewerker heeft verstrekt over zijn arbeidsverleden en scholing geverifieerd (voor ambtenaren zie: CAR-UWO).

8.1.3 Arbeidsvoorwaarden
Als onderdeel van hun contractuele verplichting behoren werknemers, ingehuurd personeel en externe gebruikers de algemene voorwaarden te aanvaarden en te ondertekenen van hun arbeidscontract, waarin hun verantwoordelijkheden en die van de organisatie ten aanzien van informatiebeveiliging behoren te zijn vastgelegd.

8.2 Tijdens het dienstverband

Doelstelling
Bewerkstelligen dat alle werknemers, ingehuurd personeel en externe gebruikers zich bewust zijn van bedreigingen en gevaren voor informatiebeveiliging, van hun verantwoordelijkheid en aansprakelijkheid, en dat ze zijn toegerust om het beveiligingsbeleid van de organisatie in hun dagelijkse werkzaamheden te ondersteunen, en het risico van een menselijke fout te verminderen.

8.2.1 Directieverantwoordelijkheid
Het College behoort van werknemers, ingehuurd personeel en externe gebruikers te eisen dat ze beveiliging toepassen overeenkomstig vastgesteld beleid en vastgestelde procedures van de organisatie.

- Het lijnmanagement heeft een strategie ontwikkeld en geïmplementeerd om blijvend over specialistische kennis en vaardigheden van gemeenteambtenaren en ingehuurd personeel (die kritische bedrijfsactiviteiten op het gebied van IB uitoefenen) te kunnen beschikken.
- Het lijnmanagement bevordert dat gemeenteambtenaren, ingehuurd personeel en (waar van toepassing) externe gebruikers van interne systemen algemene beveiligingsaspecten toepassen in hun gedrag en handelingen overeenkomstig vastgesteld beleid.

8.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging
Alle werknemers van de organisatie en, voor zover van toepassing, ingehuurd personeel en externe gebruikers, behoren geschikte training en regelmatige bijscholing te krijgen met betrekking tot beleid en procedures van de organisatie, voor zover relevant voor hun functie.

- Alle medewerkers van de organisatie worden regelmatig attent gemaakt op het beveiligingsbeleid en de beveiligingsprocedures van de organisatie, voor zover relevant voor hun functie.

8.2.3 Disciplinaire Maatregelen
Er behoort een formeel disciplinair proces te zijn vastgesteld voor werknemers die inbreuk op de beveiliging hebben gepleegd.

- Er is een disciplinair proces vastgelegd voor medewerkers die inbreuk maken op het beveiligingsbeleid.

8.3 Beëindiging of wijziging van het dienstverband

Doelstelling
Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers ordelijk de organisatie verlaten of hun dienstverband wijzigen.

8.3.1 Beëindiging van verantwoordelijkheden
De verantwoordelijkheden voor beëindiging of wijziging van het dienstverband behoren duidelijk te zijn vastgesteld en toegewezen.

- Voor ambtenaren is in de ambtseed of belofte vastgelegd welke verplichtingen ook na beëindiging van het dienstverband of bij functiewijziging nog van kracht blijven en voor hoe lang. Voor ingehuurd personeel (zowel in dienst van een derde bedrijf als individueel) is dit contractueel vastgelegd. Indien nodig wordt een geheimhoudingsverklaring ondertekend.
- Het lijnmanagement heeft een procedure vastgesteld voor beëindiging van dienstverband, contract of overeenkomst waarin minimaal aandacht besteed wordt aan het intrekken van toegangsrechten, innemen van bedrijfsmiddelen en welke verplichtingen ook na beëindiging van het dienstverband blijven gelden.
- Het lijnmanagement heeft een procedure vastgesteld voor verandering van functie binnen de organisatie, waarin minimaal aandacht besteed wordt aan het intrekken van toegangsrechten en innemen van bedrijfsmiddelen die niet meer nodig zijn na het beëindigen van de oude functie.

8.3.2 Retournering van bedrijfsmiddelen
Alle werknemers, ingehuurd personeel en externe gebruikers behoren alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben te retourneren bij beëindiging van hun dienstverband, contract of overeenkomst.

Zie 8.3.1.3

8.3.3 Blokkering van toegangsrechten
De toegangsrechten van alle werknemers, ingehuurd personeel en externe gebruikers tot informatie en IT-voorzieningen behoren te worden geblokkeerd bij beëindiging van het dienstverband, het contract of de overeenkomst, of behoort na wijziging te worden aangepast.

Zie 8.3.1.3

VEILIGHEID

9. FYSIEKE BEVEILIGING EN BEVEILIGING VAN DE OMGEVING

9.1 Beveiligde ruimten

Doelstelling

Het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de organisatie.

9.1.1 Fysieke beveiliging van de omgeving

Er behoren toegangsbeveiligingen (barrières zoals muren, toegangspoorten met kaartsloten of een bemande receptie) te worden aangebracht om ruimten te beschermen waar zich informatie en IT-voorzieningen bevinden.

- De gemeente en haar omgeving worden ingedeeld in verschillende zones. Deze zones bestaan uit:
  - Zone 0: de omgeving en het gebouw
  - Zone 1: de wachtruimten en de spreekkamers
  - Zone 2: de werkruimten
  - Zone 3: de ICT-ruimte
- Voor voorzieningen (binnen of buiten het gebouw) zijn duidelijke beveiligingsgrenzen bepaald.
- Gebouwen bieden voldoende weerstand (bepaald op basis van een risicoafweging) bij gewelddadige aanvallen zoals inbraak en IT gericht vandalisme.
- Er zijn op verschillende plekken zogenaamde overval alarmknoppen geplaatst, dit is met name van belang voor de wachtruimten en de spreekkamers en die ruimtes waar bezoekers in contact komen met gemeente ambtenaren.
- Er is 24-uur, 7 dagen per week bewaking; een inbraakalarm gekoppeld aan alarmcentrale is het minimum.
- Van ingehuurde bewakingsdiensten is vooraf geverifieerd dat zij voldoen aan de wettelijke eisen gesteld in de Wet Particuliere Beveiligingsorganisaties en Rechercheburéaus. Deze verificatie wordt minimaal jaarlijks herhaald.
- In gebouwen met serverruimtes houdt beveiligingspersoneel toezicht op de toegang. Hiervan wordt een registratie bijhouden.

9.1.2 Fysieke toegangsbeveiliging

Beveiligde zones behoren te worden beschermd door geschikte toegangsbeveiliging, om te bewerkstelligen dat alleen bevoegd personeel wordt toegelaten.

- Toegang tot gebouwen of beveiligingszones is alleen mogelijk na autorisatie daartoe.
- De beveiligingszones en toegangsbeveiliging daarvan zijn ingericht conform het Kader Rijkstoegangsbeleid.
- In gebouwen met serverruimtes houdt beveiligingspersoneel toezicht op de toegang. Hiervan wordt een registratie bijhouden.
- De kwaliteit van toegangsmiddelen (deuren, sleutels, sloten, toegangspassen) is afgestemd op de zonering.
- De uitgifte van toegangsmiddelen wordt geregistreerd.
- Niet uitgegeven toegangsmiddelen worden opgeborgen in een beveiligd opbergmiddel.
- Apparatuur en bekabeling in kabelverdeelruimtes en patchruimtes voldoen aan dezelfde eisen t.a.v. toegangbeveiliging zoals die worden gesteld aan computerruimtes.
- Er vindt minimaal één keer per half jaar een periodieke controle/evaluatie plaats op de autorisaties voor fysieke toegang.

9.1.3 Beveiliging van kantoren, ruimten en faciliteiten
Er behoort fysieke beveiliging van kantoren, ruimten en faciliteiten te worden ontworpen en toegepast.

- Papieren documenten en mobiele gegevensdragers die vertrouwelijke informatie bevatten worden beveiligd opgeslagen.
- Er is actief beheer van sloten en kluizen met procedures voor wijziging van combinaties door middel van een sleutelplan. Ten behoeve van opslag van gerubriceerde informatie.
- Serverruimtes, datacenters en daar aan gekoppelde bekabelingsystemen zijn ingericht in lijn met geldende best practices. Een goed voorbeeld van zo'n best practice is Telecommunication Infrastructure Standard for Data Centers (TIA- 942).

9.1.4 Bescherming tegen bedreigingen van buitenaf
Er behoort fysieke bescherming tegen schade door brand, overstroming, aardschokken, explosies, oproer en andere vormen van natuurlijke of menselijke calamiteiten te worden ontworpen en toegepast.

- Bij maatregelen is rekening gehouden met specifieke bedreigingen van aangrenzende panden of terreinen.
- Reserve apparatuur en backups zijn op een zodanige afstand ondergebracht dat één en dezelfde calamiteit er niet voor kan zorgen dat zowel de hoofdlocatie als de backup/reserve locatie niet meer toegankelijk zijn.
- Beveiligde ruimten waarin zich bedrijf kritische apparatuur bevindt zijn voldoende beveiligd tegen wateroverlast.
- Bij het betrekken van nieuwe gebouwen wordt een locatie gekozen waarbij rekening wordt gehouden met de kans op en de gevolgen van natuurrampen en door mensen veroorzaakte rampen.
- Gevaarlijke of brandbare materialen zijn op een zodanige afstand van een beveiligde ruimte opgeslagen dat een calamiteit met deze materialen geen invloed heeft op de beveiligde ruimte.
- Er is door de brandweer goedgekeurde en voor de situatie geschikte brandblusapparatuur geplaatst en aangesloten. Dit wordt jaarlijks gecontroleerd.

9.1.5 Werken in beveiligde ruimten
Er behoren een fysieke bescherming en richtlijnen voor werken in beveiligde ruimten te worden ontworpen en toegepast.

- Medewerkers die zelf niet geautoriseerd zijn mogen alleen onder begeleiding van bevoegd personeel en als er een duidelijke noodzaak voor is toegang krijgen tot fysiek beveiligde ruimten waarin IT voorzieningen zijn geplaatst of waarin met vertrouwelijke informatie wordt gewerkt.
- Beveiligde ruimten (zoals een serverruimte of kluis) waarin zich geen personen bevinden zijn afgesloten en worden regelmatig gecontroleerd.
- Zonder expliciete toestemming mogen binnen beveiligde ruimten geen opnames (foto, video of geluid) worden gemaakt.

9.1.6 Openbare toegang en gebieden voor laden en lossen
Toegangspunten zoals gebieden voor laden en lossen en andere punten waar onbevoegden het terrein kunnen betreden, behoren te worden beheerst en indien mogelijk worden afgeschermd van IT voorzieningen, om onbevoegde toegang te voorkomen.

- Er bestaat een procedure voor het omgaan met verdachte pakketten en brieven in postkamers en laad- en losruimten.

9.2 Beveiliging van apparatuur

Doelstelling
Het voorkomen van verlies, schade, diefstal of compromitteren van bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten.

9.2.1 Plaatsing en bescherming van apparatuur
Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van schade en storing van buitenaf en de gelegenheid voor onbevoegde toegang wordt verminderd.

- Apparatuur wordt opgesteld en aangesloten conform de voorschriften van de leverancier. Dit geldt minimaal voor temperatuur en luchtvochtigheid, aarding, spanningsstabiliteit en overspanningsbeveiliging.
- Gebouwen zijn beveiligd tegen blikseminslag.
- Eten en drinken is verboden in serverruimten.
- Een informatiesysteem voldoet altijd aan de hoogste beveiligingseisen die voor kunnen komen bij het verwerken van informatie. Indien dit niet mogelijk is wordt een gescheiden systeem gebruikt voor de informatieverwerking waaraan hogere eisen gesteld worden.

9.2.2 Nutsvoorzieningen
Apparatuur behoort te worden beschermd tegen stroomuitval en andere storingen door onderbreking van nutsvoorzieningen.

9.2.3 Beveiliging van kabels
Voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt, behoren tegen interceptie of beschadiging te worden beschermd conform de norm NEN 1010.

9.2.4 Onderhoud van apparatuur
Apparatuur behoort op correcte wijze te worden onderhouden, om te waarborgen dat deze voortdurend beschikbaar is en in goede staat verkeert.

- Reparatie en onderhoud van apparatuur (hardware) vindt op locatie plaats door bevoegd personeel, tenzij er geen data op het apparaat aanwezig of toegankelijk is.

9.2.5 Beveiliging van apparatuur buiten het terrein
Apparatuur buiten de terreinen behoort te worden beveiligd waarbij rekening wordt gehouden met de diverse risico's van werken buiten het terrein van de organisatie.

- Alle apparatuur buiten de terreinen wordt beveiligd met adequate beveiligingsmaatregelen.

9.2.6 Veilig verwijderen of hergebruiken van apparatuur

Alle apparatuur die opslagmedia bevat, behoort te worden gecontroleerd om te bewerkstelligen dat alle gevoelige gegevens en in licentie gebruikte programmatuur zijn verwijderd of veilig zijn overschreven voordat de apparatuur wordt verwijderd.

- Bij beëindiging van het gebruik of bij een defect worden apparaten en informatiedragers bij de beheersorganisatie ingeleverd. De beheerorganisatie zorgt voor een verantwoorde afvoer zodat er geen data op het apparaat aanwezig of toegankelijk is. Als dit niet kan wordt het apparaat of de informatiedrager fysiek vernietigd. Het afvoeren of vernietigen wordt per bedrijfseenheid geregistreerd.
- Hergebruik van apparatuur buiten de organisatie is slechts toegestaan indien de informatie is verwijderd met een voldoende veilige methode. Een veilige methode is Secure Erase voor apparaten die dit ondersteunen. In overige gevallen wordt de data twee keer overschreven met vaste data, één keer met random data en vervolgens wordt geverifieerd of het overschrijven is gelukt.

9.2.7 Verwijdering van bedrijfseigendommen

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

VEILIGHEID

10. BEHEER VAN COMMUNICATIE- EN BEDIENINGSPROCESSEN

10.1 Bedieningsprocedures en verantwoordelijkheden

Doelstelling
Waarborgen van een correcte en veilige bediening van IT voorzieningen

10.1.1 Gedocumenteerde bedieningsprocedures

Bedieningsprocedures behoren te worden gedocumenteerd, te worden bijgehouden en beschikbaar te worden gesteld aan alle gebruikers die deze nodig hebben.

- Bedieningsprocedures bevatten informatie over opstarten, afsluiten, backup- en herstelacties, afhandelen van fouten, beheer van logs, contactpersonen, noodprocedures en speciale maatregelen voor beveiliging.
- Er zijn procedures voor de behandeling van digitale media die ingaan op ontvangst, opslag, rubricering, toegangsbeperkingen, verzending, hergebruik en vernietiging.

10.1.2 Wijzigingsbeheer

Wijzigingen in IT voorzieningen en informatiesystemen behoren te worden beheerst.

- In de procedure voor wijzigingenbeheer is minimaal aandacht besteed aan:
  - o het administreren van significante wijzigingen
  - o impactanalyse van mogelijke gevolgen van de wijzigingen
  - o goedkeuringsprocedure voor wijzigingen
- Instellingen van informatiebeveiligingsfuncties (b.v. security software) op het koppelvlak tussen vertrouwde en onvertrouwde netwerken, worden automatisch op wijzigingen gecontroleerd.

10.1.3 Functiescheiding

Taken en verantwoordelijkheidsgebieden behoren te worden gescheiden om gelegenheid voor onbevoegde of onbedoelde wijziging of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.

- Niemand in een organisatie of proces mag op uitvoerend niveau rechten hebben om een gehele cyclus van handelingen in een kritisch informatiesysteem te beheersen. Dit in verband met het risico dat hij of zij zichzelf of anderen onrechtmatig bevoordeelt of de organisatie schade toe brengt. Dit geldt voor zowel informatieverwerking als beheeracties.
- Er is een scheiding tussen beheertaken en overige gebruikstaken. Beheerswerkzaamheden worden alleen uitgevoerd wanneer ingelogd als beheerder, normale gebruikstaken alleen wanneer ingelogd als gebruiker.
- Vóór de verwerking van gegevens die de integriteit van kritieke informatie of kritieke informatie systemen kunnen aantasten worden deze gegevens door een tweede persoon geïnspecteerd en geaccepteerd. Van de acceptatie wordt een log bijgehouden.
- Verantwoordelijkheden voor beheer en wijziging van gegevens en bijbehorende informatiesysteemfuncties moeten eenduidig toegewezen zijn aan één specifieke (beheerders)rol.

10.1.4 Scheiding van faciliteiten voor ontwikkeling, testen en productie
Faciliteiten voor ontwikkeling, testen en productie behoren te zijn gescheiden om het risico van onbevoegde toegang tot of wijzigingen in het productiesysteem te verminderen.

- Er zijn minimaal logisch gescheiden systemen voor Ontwikkeling, Test en/of Acceptatie en Productie (OTAP). De systemen en applicaties in deze zones beïnvloeden systemen en applicaties in andere zones niet.
- Gebruikers hebben gescheiden gebruiksprofielen voor Ontwikkeling, Test en/of Acceptatie en Productiesystemen om het risico van fouten te verminderen. Het moet duidelijk zichtbaar zijn in welk systeem gewerkt wordt.
- Indien er een experimenteer of laboratorium omgeving is, is deze fysiek gescheiden van de productieomgeving.

10.2 Exploitatie door een derde partij

Doelstelling
Een geschikt niveau van informatiebeveiliging en dienstverlening implementeren en bijhouden in overeenstemming met de overeenkomsten voor dienstverlening door een derde partij.

10.2.1 Dienstverlening
Er behoort te worden bewerkstelligd dat de beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de overeenkomst voor dienstverlening door een derde partij worden geïmplementeerd en uitgevoerd en worden bijgehouden door die derde partij.

- De uitbestedende partij blijft verantwoordelijk voor de betrouwbaarheid van uitbestede diensten.
- Uitbesteding is goedgekeurd door de voor het informatiesysteem verantwoordelijke lijnmanager.

10.2.2 Controle en beoordeling van dienstverlening door een derde partij
De diensten, rapporten en registraties die door de derde partij worden geleverd, behoren regelmatig te worden gecontroleerd en beoordeeld en er behoren regelmatig audits te worden uitgevoerd.

- Er worden afspraken gemaakt over de inhoud van rapportages, zoals over het melden van incidenten en autorisatiebeheer.
- De in dienstverleningscontracten vastgelegde betrouwbaarheidseisen worden gemonitord. Dit kan bijvoorbeeld middels audits of rapportages en gebeurt minimaal eens per drie maanden.
- Er zijn voor beide partijen eenduidige aanspreekpunten.

10.2.3 Beheer van wijzigingen in dienstverlening door een derde partij
Wijzigingen in de dienstverlening door derden, waaronder het bijhouden en verbeteren van bestaande beleidslijnen, procedures en maatregelen voor informatiebeveiliging, behoren te worden beheerd, waarbij rekening wordt gehouden met de onmisbaarheid van de betrokken bedrijfssystemen en -processen en met heroverweging van risico's.

Zie 10.1.2

10.3 Systeemplanning en –acceptatie

Doelstelling
Het risico van systeemstoringen tot een minimum beperken.

10.3.1 Capaciteitsbeheer
Het gebruik van middelen behoort te worden gecontroleerd en afgestemd en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen, om de vereiste systeemprestaties te bewerkstelligen.

- De ICT-voorzieningen voldoen aan het voor de diensten overeengekomen niveau van beschikbaarheid. Er worden voorzieningen geïmplementeerd om de beschikbaarheid van componenten te bewaken (bijvoorbeeld de controle op aanwezigheid van een component en metingen die het gebruik van een component vaststellen). Op basis van voorspellingen van het gebruik wordt actie genomen om tijdig de benodigde uitbreiding van capaciteit te bewerkstelligen. Op basis van een risicoanalyse wordt bepaald wat de beschikbaarheid eis van een ICT-voorziening is en wat de impact bij uitval is. Afhankelijk daarvan worden maatregelen bepaald zoals automatisch werkende mechanismen om uitval van (fysieke) ICT-voorzieningen, waaronder verbindingen op te vangen.
- Er worden beperkingen opgelegd aan gebruikers en systemen ten aanzien van het gebruik van gemeenschappelijke middelen, zodat een enkele gebruiker (of systeem) niet meer van deze middelen kan opeisen dan nodig is voor de uitvoering van zijn of haar taak en daarmee de beschikbaarheid van systemen voor andere gebruikers (of systemen) in gevaar kan brengen.
- In koppelpunten met externe of onvertrouwde zones worden maatregelen getroffen om DDOS (Denial of Service attacks) aanvallen te signaleren en hierop te reageren. Het gaat hier om aanvallen die erop gericht zijn de verwerkingscapaciteit zodanig te laten vollopen, dat onbereikbaarheid of uitval van computers het gevolg is.

10.3.2 Systeem acceptatie
Er behoren aanvaardingscriteria te worden vastgesteld voor nieuwe informatiesystemen, upgrades en nieuwe versies en er behoort een geschikte test van het systeem of de systemen te worden uitgevoerd tijdens ontwikkeling en voorafgaand aan de acceptatie.

- Van acceptatietesten wordt een log bijgehouden.
- Er zijn acceptatiecriteria vastgesteld voor het testen van de beveiliging. Dit betreft minimaal OWASP of gelijkwaardig.

10.4 Bescherming tegen virussen en "mobile code"

Doelstelling
Beschermen van de integriteit van programmatuur en informatie.

10.4.1 Maatregelen tegen virussen
Er behoren maatregelen te worden getroffen voor detectie, preventie en herstellen om te beschermen tegen virussen en er behoren geschikte procedures te worden ingevoerd om het bewustzijn van de gebruikers te vergroten.

- Bij het openen van bestanden worden deze geautomatiseerd gecontroleerd op virussen, trojans en andere malware. De update voor de detectiedefinities vindt frequent, minimaal één keer per dag, automatisch plaats.
- Inkomende en uitgaande e-mails worden gecontroleerd op virussen, trojans en andere malware. De update voor de detectiedefinities vindt frequent, minimaal één keer per dag, (automatisch) plaats.
- In verschillende schakels van een keten binnen de infrastructuur van een organisatie wordt bij voorkeur antivirusprogrammatuur van verschillende leveranciers toegepast.
- Er zijn maatregelen om verspreiding van virussen tegen te gaan en daarmee schade te beperken (bijv. quarantaine en compartimentering).
- Er zijn continuïteitsplannen voor herstel na aanvallen met virussen waarin minimaal maatregelen voor back-ups en herstel van gegevens en programmatuur zijn beschreven.

10.4.2 Maatregelen tegen "mobile code"
Als gebruik van "mobile code" is toegelaten, behoort de configuratie te bewerkstelligen dat de geautoriseerde "mobile code" functioneert volgens een duidelijk vastgesteld beveiligingsbeleid, en behoort te worden voorkomen dat onbevoegde 'mobile code' wordt uitgevoerd.

- Mobile code wordt uitgevoerd in een logisch geïsoleerde omgeving (sandbox) om de kans op aantasting van de integriteit van het systeem te verkleinen. De mobile code wordt altijd uitgevoerd met minimale rechten zodat de integriteit van het host systeem niet aangetast wordt.
- Een gebruiker moet geen extra rechten kunnen toekennen aan programma's (bijv. internet browsers) die mobiele code uitvoeren.

10.5 Back-up

Doelstelling
Handhaven van de integriteit en beschikbaarheid van informatie en IT voorzieningen.

10.5.1 Reservekopieën maken (back-ups)
Er behoren back-upkopieën van informatie en programmatuur te worden gemaakt en regelmatig te worden getest overeenkomstig het vastgestelde back-upbeleid.

- Er zijn (geteste) procedures voor back-up en recovery van informatie voor herinrichting en foutherstel van verwerkingen.
- Back-upstrategieën zijn vastgesteld op basis van het soort gegevens (bestanden, databases, enz.), de maximaal toegestane periode waarover gegevens verloren mogen raken, en de maximaal toelaatbare back-up- en hersteltijd.
- Van back-upactiviteiten en de verblijfplaats van de media wordt een registratie bijgehouden, met een kopie op een andere locatie. De andere locatie is zodanig gekozen dat een incident/calamiteit op de oorspronkelijke locatie niet leidt tot schade aan of toegang tot de kopie van die registratie.
- Back-ups worden bewaard op een locatie die zodanig is gekozen dat een incident op de oorspronkelijke locatie niet leidt tot schade aan de back-up.
- Op back-ups staat de risicoklasse vermeld vanaf WBP Risicoklasse 3.
- De fysieke en logische toegang tot de back-ups, zowel van systeemschijven als van data, is zodanig geregeld dat alleen geautoriseerde personen zich toegang kunnen verschaffen tot deze back-ups.

10.6 Beheer van netwerkbeveiliging

Doelstelling
Bewerkstelligen van de bescherming van informatie in netwerken en bescherming van de ondersteunende infrastructuur.

10.6.1 Maatregelen voor netwerken
Netwerken behoren adequaat te worden beheerd en beheerst om ze te beschermen tegen bedreigingen en om beveiliging te handhaven voor de systemen en toepassingen die gebruikmaken van het netwerk, waaronder informatie die wordt getransporteerd.

- Het netwerk wordt gemonitord en beheerd zodat aanvallen, storingen of fouten ontdekt en hersteld kunnen worden en de betrouwbaarheid van het netwerk niet onder het afgesproken minimum niveau komt.
- Gegevensuitwisseling tussen vertrouwde en onvertrouwde zones dient inhoudelijk geautomatiseerd gecontroleerd te worden op aanwezigheid van malware.
- Bij transport van vertrouwelijke informatie over onvertrouwde netwerken, zoals het internet, dient altijd geschikte encryptie te worden toegepast. Zie hiertoe 12.3.1.3.
- Er zijn procedures voor beheer van apparatuur op afstand.

10.6.2 Beveiliging van netwerkdiensten
Beveiligingskenmerken, niveaus van dienstverlening en beheer eisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in elke overeenkomst voor netwerkdiensten, zowel voor diensten die intern worden geleverd als voor uitbestede diensten.

10.7 Behandeling van media

Doelstelling
Voorkomen van onbevoegde openbaarmaking, modificatie, verwijdering of vernietiging van bedrijfsmiddelen en onderbreking van bedrijfsactiviteiten.

10.7.1 Beheer van verwijderbare media
Er behoren procedures te zijn vastgesteld voor het beheer van verwijderbare media.

- Er zijn procedures opgesteld en geïmplementeerd voor opslag van vertrouwelijke informatie voor verwijderbare media.
- Verwijderbare media met vertrouwelijke informatie mogen niet onbeheerd worden achtergelaten op plaatsen die toegankelijk zijn zonder toegangscontrole.
- In het geval dat media een kortere verwachte levensduur hebben dan de gegevens die ze bevatten, worden de gegevens gekopieerd wanneer 75% van de levensduur van het medium is verstreken.
- Gegevensdragers worden behandeld volgens de voorschriften van de fabrikant.

10.7.2 Verwijdering van media
Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.

- Er zijn procedures vastgesteld en in werking voor verwijderen van vertrouwelijke data en de vernietiging van verwijderbare media. Verwijderen van data wordt gedaan met een Secure Erase voor apparaten waar dit mogelijk is. In overige gevallen wordt de data twee keer overschreven met vaste data, één keer met random data en vervolgens wordt geverifieerd of het overschrijven is gelukt. Zie ook 9.2.6.

10.7.3 Procedures voor de behandeling van informatie
Er behoren procedures te worden vastgesteld voor de behandeling en opslag van informatie om deze te beschermen tegen onbevoegde openbaarmaking of misbruik.

10.7.4 Beveiliging van systeemdocumentatie
Systeemdocumentatie behoort te worden beschermd tegen onbevoegde toegang.

- Systeemdocumentatie die vertrouwelijke informatie bevat is niet vrij toegankelijk.
- Wanneer de eigenaar er expliciet voor kiest om gerubriceerde systeemdocumentatie buiten de rijksdienst te brengen, doet hij dat niet zonder risicoafweging.

10.8 Uitwisseling van informatie

Doelstelling
Handhaven van beveiliging van informatie en programmatuur die wordt uitgewisseld binnen een organisatie en met enige externe entiteit.

10.9.1 Beleid en procedures voor informatie-uitwisseling
Er behoren formeel beleid, formele procedures en formele beheersmaatregelen te zijn vastgesteld om de uitwisseling van informatie via het gebruik van alle typen communicatiefaciliteiten te beschermen.

- Het meenemen van Vertrouwelijke informatie buiten gecontroleerd gebied vindt uitsluitend plaats indien dit voor de uitoefening van de functie noodzakelijk is.
- Medewerkers zijn geïnstrueerd om zodanig om te gaan met (telefoon)gesprekken, e-mail, faxen en ingesproken berichten op antwoordapparaten dat de kans op uitlekken van vertrouwelijke informatie geminimaliseerd wordt.
- Medewerkers zijn geïnstrueerd om zodanig om te gaan met mobiele apparatuur en verwijderbare media dat de kans op uitlekken van vertrouwelijke informatie geminimaliseerd wordt. Hierbij wordt ten minste aandacht besteed aan het risico van adreslijsten en opgeslagen boodschappen in mobiele telefoons.
- Medewerkers zijn geïnstrueerd om geen vertrouwelijke documenten bij de printer te laten liggen.
- Er zijn maatregelen getroffen om het automatisch doorsturen van interne e-mail berichten naar externe e-mail adressen te voorkomen.

10.9.2 Uitwisselingsovereenkomsten
Er behoren overeenkomsten te worden vastgesteld voor de uitwisseling van informatie en programmatuur tussen de organisatie en externe partijen.

- Er zijn afspraken gemaakt over de beveiliging van de uitwisseling van gegevens en software tussen organisaties waarin de maatregelen om betrouwbaarheid, waaronder traceerbaarheid en onweerlegbaarheid, van gegevens te waarborgen zijn beschreven en getoetst.
- Verantwoordelijkheid en aansprakelijkheid in het geval van informatiebeveiligingsincidenten zijn beschreven, alsmede procedures over melding van incidenten.
- Het eigenaarschap van gegevens en programmatuur en de verantwoordelijkheid voor de gegevensbescherming, auteursrechten, licenties van programmatuur zijn vastgelegd.
- Indien mogelijk wordt binnenkomende programmatuur (zowel op fysieke media als gedownload) gecontroleerd op ongeautoriseerde wijzigingen aan de hand van een door de leverancier via een gescheiden kanaal geleverde checksum of certificaat.

10.9.3 Fysieke media die worden getransporteerd
Media die informatie bevatten behoren te worden beschermd tegen onbevoegde toegang, misbruik of corrumperen tijdens transport buiten de fysieke begrenzing van de organisatie.

- Om vertrouwelijke informatie te beschermen worden maatregelen genomen, zoals:
  - versleuteling
  - bescherming door fysieke maatregelen, zoals
  - afgesloten containers
  - gebruik van verpakkingsmateriaal waaraan te zien is of getracht is het te openen
  - persoonlijke aflevering
  - opsplitsing van zendingen in meerdere delen en eventueel verzending via verschillende routes
- Fysieke verzending van bijzondere informatie dient te geschieden met ministerieel goedgekeurde middelen, waardoor de inhoud niet zichtbaar, niet kenbaar en inbreuk te detecteren is.

10.9.4 Elektronisch berichtenuitwisseling
Informatie die een rol speelt bij elektronische berichtuitwisseling behoort op geschikte wijze te worden beschermd.

- Digitale documenten binnen de rijksdienst waar eindgebruikers rechten aan kunnen ontlenen maken gebruik van PKI Overheid.
- Er is een (spam) filter geactiveerd voor e-mail berichten.

10.9.5 Systemen voor bedrijfsinformatie
Beleid en procedures behoren te worden ontwikkeld en geïmplementeerd om informatie te beschermen die een rol speelt bij de onderlinge koppeling van systemen voor bedrijfsinformatie.

- Er zijn richtlijnen met betrekking tot het bepalen van de risico's die het gebruik van kantoorapplicaties met zich meebrengen en richtlijnen voor de bepaling van de beveiliging van kantoorapplicaties. Hierin is minimaal aandacht besteed aan de toegang tot de interne informatievoorziening, toegankelijkheid van agenda's, afscherming van documenten, beschikbaarheid en backup.

10.10 Diensten voor e-commerce

Doelstelling
Bewerkstelligen van de beveiliging van diensten voor e-commerce, en veilig gebruik ervan.

10.10.1 E-commerce
Informatie die een rol speelt bij e-commerce en die via openbare netwerken wordt uitgewisseld, behoort te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en modificatie.

- Waar mogelijk worden authentieke basisregistraties van de overheid gebruikt (b.v. GBA).

10.10.2 Onlinetransacties
Informatie die een rol speelt bij onlinetransacties behoort te worden beschermd om onvolledige overdracht, onjuiste routing, onbevoegde wijziging van berichten, onbevoegde openbaarmaking, onbevoegde duplicatie of weergave van berichten te voorkomen.

- Een transactie wordt bevestigd door een (gekwalificeerde) elektronische handtekening of een andere wilsuiting (bijv. een TAN code) van de gebruiker.
- Een transactie is versleuteld, de partijen zijn geauthentiseerd en de privacy van betrokken partijen is gewaarborgd.

10.10.3 Openbaar beschikbare informatie
De betrouwbaarheid van de informatie die beschikbaar wordt gesteld op een openbaar toegankelijk systeem behoort te worden beschermd om onbevoegde modificatie te voorkomen.

- Er zijn procedures die waarborgen dat gepubliceerde informatie is aangeleverd door daartoe geautoriseerde medewerkers.

10.11 Controle - Doelstelling
Ontdekken van onbevoegde informatieverwerkingsactiviteiten.

10.11.1 Aanmaken audit-logbestanden
Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen behoren te worden vastgelegd in audit-logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole.

- Van logbestanden worden rapportages gemaakt die periodiek, minimaal maandelijks, worden beoordeeld.
- Een logregel bevat minimaal:
  - een tot een natuurlijk persoon herleidbare gebruikersnaam of ID
  - de gebeurtenis (zie 10.10.2.1)
  - waar mogelijk de identiteit van het werkstation of de locatie
  - het object waarop de handeling werd uitgevoerd
  - het resultaat van de handeling
  - de datum en het tijdstip van de gebeurtenis
- In een logregel worden in geen geval gevoelige gegevens opgenomen. Dit Betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden, inbelnummers, enz.).
- Logberichten worden overzichtelijk samengevat. Daartoe zijn systemen die logberichten genereren aangesloten op een Security Information and Event Management systeem (SIEM) waarmee meldingen en alarmoproepen aan de beheerorganisatie gegeven worden. Er is vastgelegd bij welke drempelwaarden meldingen en alarmoproepen gegenereerd worden.
- Controle op opslag van logging: het vollopen van het opslagmedium voor de logbestanden boven een bepaalde grens wordt gelogd en leidt tot automatische alarmering van de beheerorganisatie. Dit geldt ook als het bewaren van loggegevens niet (meer) mogelijk is (bijv. een logserver die niet bereikbaar is).

10.11.2 Controle van systeemgebruik
Er behoren procedures te worden vastgesteld om het gebruik van IT voorzieningen te controleren. Het resultaat van de controleactiviteiten behoort regelmatig te worden beoordeeld.

- De volgende gebeurtenissen worden in ieder geval opgenomen in de logging:
  - gebruik van technische beheerfuncties, zoals het wijzigingen van configuratie of instelling; uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore
  - gebruik van functioneel beheerfuncties, zoals het wijzigingen van configuratie en instellingen, release van nieuwe functionaliteit, ingrepen in gegevenssets (waaronder databases)
  - handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoordreset, uitgifte en intrekken van cryptosleutels
  - beveiligingsincidenten (zoals de aanwezigheid van malware, testen op vulnerabilities, foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet operatio nele systeemservices, het starten en stoppen van security services)
  - verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens executie van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of systemen)
  - handelingen van gebruikers, zoals goede en foute inlogpogingen, systeemtoegang, gebruik van online transacties en toegang tot bestanden door systeembeheerders.

10.11.3 Bescherming van informatie in logbestanden
Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen inbreuk en onbevoegde toegang.

- Het (automatisch) overschrijven of verwijderen van logbestanden wordt gelogd in de nieuw aangelegde log.
- Het raadplegen van logbestanden is voorbehouden aan geautoriseerde gebruikers. Hierbij is de toegang beperkt tot leesrechten.
- Logbestanden worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden.
- De instellingen van logmechanismen worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden. Indien de instellingen aangepast moeten worden zal daarbij altijd het vier ogen principe toegepast worden.
- De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht, met een minimum van drie maanden, conform de wensen van de systeemeigenaar. Bij een (vermoed) informatiebeveiligingsincident is de bewaartermijn minimaal drie jaar.
- Controle op opslag van logging: het vollopen van het opslagmedium voor de logbestanden boven een bepaalde grens wordt gelogd en leidt tot automatische alarmering van de beheerorganisatie. Dit geldt ook als het bewaren van loggegevens niet (meer) mogelijk is (bijv. een logserver die niet bereikbaar is).

10.11.4 Logbestanden van administrators en operators
Activiteiten van systeemadministrators en systeemoperators behoren in logbestanden te worden vastgelegd.

Zie 10.10.1

10.11.5 Registratie van storingen
Storingen behoren in logbestanden te worden vastgelegd en te worden geanalyseerd en er behoren geschikte maatregelen te worden genomen.

Zie 10.10.1

10.11.6 Synchronisatie van systeemklokken
De klokken van alle relevante informatiesystemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met een overeengekomen nauwkeurige tijdsbron.

- Systeemklokken worden zodanig gesynchroniseerd dat altijd een betrouwbare analyse van logbestanden mogelijk is.

VEILIGHEID

11. TOEGANGSBEVEILIGING

11.1 Toegangsbeleid

Doelstelling

Beheersen van de toegang tot informatie.

11.1.1 Toegangsbeleid
Er behoort toegangsbeleid te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfseisen en beveiligingseisen voor toegang.

11.2 Beheer van toegangsrechten van gebruikers

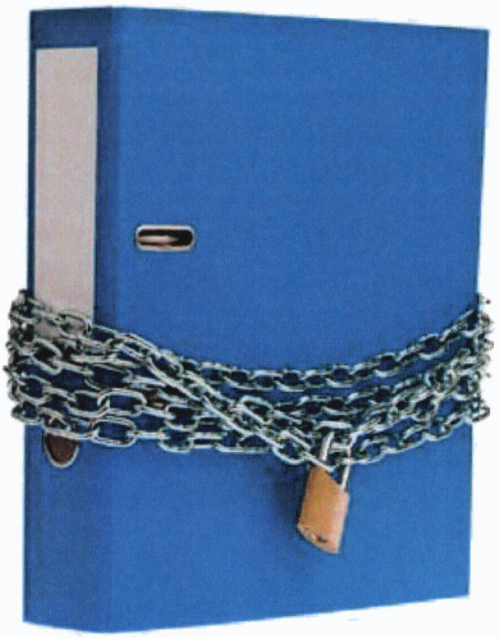
Doelstelling
Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot informatiesystemen voorkomen.

11.2.1 Registratie van gebruikers
Er behoren formele procedures voor het registreren en afmelden van gebruikers te zijn vastgesteld, voor het verlenen en intrekken van toegangsrechten tot alle informatiesystemen en -diensten.

- Gebruikers worden vooraf geïdentificeerd en geautoriseerd. Van de registratie wordt een administratie bijgehouden.
- Authenticatiegegevens worden bijgehouden in één bronbestand) zodat consistentie is gegarandeerd.
- Op basis van een risicoafweging wordt bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.

11.2.2 Beheer van (speciale) bevoegdheden
De toewijzing en het gebruik van speciale bevoegdheden behoren te worden beperkt en beheerst.

- Gebruikers hebben toegang tot speciale bevoegdheden voor zover dat voor de uitoefening van hun taak noodzakelijk is (need to know, need to use).
- Systeemprocessen draaien onder een eigen gebruikersnaam (een functioneel account), voor zover deze processen handelingen verrichten voor andere systemen of gebruikers.
- Gebruikers krijgen slechts toegang tot een noodzakelijk geachte set van applicaties en commando's.



11.2.3 Beheer van gebruikerswachtwoorden
De toewijzing van wachtwoorden behoort met een formeel beheerproces te worden beheerst.

- Wachtwoorden worden nooit in originele vorm (plaintext) opgeslagen of verstuurd, maar in plaats daarvan wordt bijvoorbeeld de hashwaarde van het wachtwoord opgeslagen.

Ten aanzien van wachtwoorden geldt:
- Wachtwoorden worden op een veilige manier uitgegeven (controle identiteit van de gebruiker).
- Tijdelijke wachtwoorden of wachtwoorden die standaard in software worden meegegeven worden bij eerste gebruik vervangen door een persoonlijk wachtwoord.
- Gebruikers bevestigen de ontvangst van een wachtwoord.
- Wachtwoorden zijn alleen bij de gebruiker bekend.
- Wachtwoorden bestaan uit minimaal 8 karakters, waarvan tenminste 1 hoofdletter, 1 cijfer en 1 vreemd teken.
- Wachtwoorden zijn maximaal 35 dagen geldig en mogen niet binnen 6 keer herhaald worden.

11.2.4 Beoordeling van toegangsrechten van gebruikers
Het College behoort de toegangsrechten van gebruikers regelmatig te beoordelen in een formeel proces.

- Toegangsrechten van gebruikers worden periodiek, minimaal jaarlijks, geëvalueerd. Het interval is beschreven in het toegangsbeleid en is bepaald op basis van het risiconiveau.

11.3 Verantwoordelijkheden van gebruikers

Doelstelling
Voorkomen van onbevoegde toegang door gebruikers, en van beschadiging of diefstal van informatie en IT-voorzieningen.

11.3.1 Gebruik van wachtwoorden
Gebruikers behoren goede beveiligingsgewoontes in acht te nemen bij het kiezen en gebruiken van wachtwoorden.

- Aan de gebruikers is een set gedragsregels aangereikt met daarin minimaal het volgende:
  - Wachtwoorden worden niet opgeschreven.
  - Gebruikers delen hun wachtwoord nooit met anderen.
  - Een wachtwoord wordt onmiddellijk gewijzigd indien het vermoeden bestaat dat het bekend is geworden aan een derde.
  - Wachtwoorden worden niet gebruikt in automatische inlogprocedures (bijv. opgeslagen onder een functietoets of in een macro).

11.3.2 Onbeheerde gebruikersapparatuur
Gebruikers behoren te bewerkstelligen dat onbeheerde apparatuur passend is beschermd.

- De gebruiker vergrendelt de werkplek tijdens afwezigheid.

11.3.3 Clear desk en clear screen
Er behoort een 'clear desk'-beleid voor papier en verwijderbare opslagmedia en een 'clear screen'-beleid voor IT-voorzieningen te worden ingesteld.

- In het clear desk beleid staat minimaal dat de gebruiker geen vertrouwelijke informatie op het bureau mag laten liggen. Deze informatie moet altijd worden opgeborgen in een afsluitbare opbergmogelijkheid (kast, locker, bureau of kamer).
- Bij afdrukken van gevoelige informatie wordt, wanneer mogelijk, gebruik gemaakt van de functie "beveiligd afdrukken" (pincode verificatie).
- Schermbeveiligingsprogrammatuur (een screensaver) maakt na een periode van inactiviteit van maximaal 15 minuten alle informatie op het beeldscherm onleesbaar en ontoegankelijk.

- Toegangsbeveiliging lock wordt automatisch geactiveerd bij het verwijderen van een token (indien aanwezig).

11.4 Toegangsbeheersing voor netwerken

Doelstelling
Het voorkomen van onbevoegde toegang tot netwerkdiensten.

11.4.1 Beleid ten aanzien van het gebruik van netwerkdiensten
Gebruikers behoort alleen toegang te worden verleend tot diensten waarvoor ze specifiek bevoegd zijn.

- Er is een gedocumenteerd beleid met betrekking tot het gebruik van netwerken en netwerkdiensten. Gebruikers krijgen slechts toegang tot de netwerkdiensten die voor het werk noodzakelijk zijn. Zie ook 11.2.2.3.

11.4.2 Authenticatie van gebruikers bij externe verbindingen
Er behoren geschikte authenticatiemethoden te worden gebruikt om toegang van gebruikers op afstand te beheersen.

Zie ook 11.6.1.3.

11.4.3 Identificatie van (netwerk)apparatuur
Automatische identificatie van apparatuur behoort te worden overwogen als methode om verbindingen vanaf specifieke locaties en apparatuur te authentiseren.

- Alleen geïdentificeerde en geauthentiseerde apparatuur kan worden aangesloten op een vertrouwde zone. Eigen, geauthentiseerde, apparatuur (Bring Your Own Device) wordt alleen aangesloten op een onvertrouwde zone.

11.4.4 Bescherming op afstand van poorten voor diagnose en configuraties
De fysieke en logische toegang tot poorten voor diagnose en configuratie behoort te worden beheerst.

- Poorten, diensten en soortgelijke voorzieningen op een netwerk of computer die niet vereist zijn voor de dienst dienen te worden afgesloten.

11.4.5 Scheiding van netwerken
Groepen informatiediensten, gebruikers en informatiesystemen behoren op netwerken te worden gescheiden.

- Werkstations worden zo ingericht dat routeren van verkeer tussen verschillende zones of netwerken niet mogelijk is.
- De indeling van zones binnen de technische infrastructuur vindt plaats volgens een operationeel beleidsdocument waarin is vastgelegd welke uitgangspunten voor zonering worden gehanteerd. Van systemen wordt bijgehouden in welke zone ze staan. Er wordt periodiek, minimaal één keer per jaar, geëvalueerd of het systeem nog steeds in de optimale zone zit of verplaatst moet worden.
- Elke zone heeft een gedefinieerd beveiligingsniveau Zodat de filtering tussen zones is afgestemd op de doelstelling van de zones en het te overbruggen verschil in beveiligingsniveau. Hierbij vindt controle plaats op protocol, inhoud en richting van de communicatie.
- Beheer en audit van zones vindt plaats vanuit een minimaal logisch gescheiden, separate zone.
- Zonering wordt ingericht met voorzieningen waarvan de functionaliteit is beperkt tot het strikt noodzakelijke (hardening van voorzieningen).

11.4.6 Beheersmaatregelen voor netwerkverbindingen
Voor gemeenschappelijke netwerken, vooral waar deze de grenzen van de organisatie overschrijden, behoren de toegangsmogelijkheden voor gebruikers te worden beperkt, overeenkomstig het toegangsbeleid en de eisen van bedrijfstoepassingen (zie 11.1).

11.4.7 Beheersmaatregelen voor netwerkroutering
Netwerken behoren te zijn voorzien van beheersmaatregelen voor netwerkroutering, om te bewerkstelligen dat computerverbindingen en informatiestromen niet in strijd zijn met het toegangsbeleid voor de bedrijfstoepassingen.

- Netwerken zijn voorzien van beheersmaatregelen voor routering gebaseerd op mechanismen ter verificatie van bron en bestemmingsadressen.

11.5 Toegangsbeveiliging voor besturingssystemen

Doelstelling
Voorkomen van onbevoegde toegang tot besturingssystemen.

11.5.1 Beveiligde inlogprocedures
Toegang tot besturingssystemen behoort te worden beheerst met een beveiligde inlogprocedure.

- Toegang tot kritische toepassingen of toepassingen met een hoog belang wordt verleend op basis van twee-factor authenticatie.
- Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven. Er wordt geen informatie getoond die herleidbaar is tot de authenticatiegegevens.
- Voorafgaand aan het aanmelden wordt aan de gebruiker een melding getoond dat alleen geautoriseerd gebruik is toegestaan voor expliciet door de organisatie vastgestelde doeleinden.
- Bij een succesvol loginproces wordt de datum en tijd van de voorgaande login of loginpoging getoond. Deze informatie kan de gebruiker enige informatie verschaffen over de authenticiteit en/of misbruik van het systeem.
- Nadat voor een gebruikersnaam 3 keer een foutief wachtwoord gegeven is, wordt het account minimaal 10 minuten geblokkeerd. Indien er geen lockout periode ingesteld kan worden, dan wordt het account geblokkeerd totdat de gebruiker verzoekt deze lockout op te heffen of het wachtwoord te resetten.

11.5.2 Gebruikersindentificatie en –authenticatie
Elke gebruiker behoort over een unieke identificatiecode te beschikken (gebruikers-ID) voor uitsluitend persoonlijk gebruik, en er behoort een geschikte authenticatietechniek te worden gekozen om de geclaimde identiteit van de gebruiker te bewijzen.

- Bij uitgifte van authenticatiemiddelen wordt minimaal de identiteit vastgesteld evenals het feit dat de gebruiker recht heeft op het authenticatiemiddel.
- Bij het intern gebruik van IT voorzieningen worden gebruikers minimaal geauthentiseerd op basis van wachtwoorden.
- Applicaties mogen niet onnodig en niet langer dan noodzakelijk onder een systeemaccount (een privileged user zoals administrator of root) draaien. Direct na het uitvoeren van handelingen waar hogere rechten voor nodig zijn, wordt weer teruggeschakeld naar het niveau van een gewone gebruiker (een unprivileged user).

11.5.3 Systemen voor wachtwoordenbeheer
Systemen voor wachtwoordbeheer behoren interactief te zijn en moeten bewerkstelligen dat wachtwoorden van geschikte kwaliteit worden gekozen.

- Er wordt automatisch gecontroleerd op goed gebruik van wachtwoorden (o.a. voldoende sterke wachtwoorden, regelmatige wijziging, directe wijziging van initieel wachtwoord).
- Wachtwoorden hebben een geldigheidsduur van maximaal 3 maanden. Daarbinnen dient het wachtwoord te worden gewijzigd. Wanneer het wachtwoord verlopen is, wordt het account geblokkeerd.
- Wachtwoorden die gereset zijn en initiële wachtwoorden hebben een zeer beperkte geldigheidsduur en moeten bij het eerste gebruik worden gewijzigd.
- De gebruikers hebben de mogelijkheid hun eigen wachtwoord te kiezen en te wijzigen. Hierbij geldt het volgende:
    - Voordat een gebruiker zijn wachtwoord kan wijzigen, wordt de gebruiker opnieuw geauthenticeerd.
    - Ter voorkoming van typefouten in het nieuw gekozen wachtwoord is er een bevestigingsprocedure.

VEILIGHEID

11.5.4 Gebruik van systeemhulpmiddelen
Het gebruik van hulpprogrammatuur waarmee systeem- en toepassingsbeheersmaatregelen zouden kunnen worden gepasseerd behoort te worden beperkt en behoort strikt te worden beheerst.

11.5.5 Time-out van sessies
Inactieve sessies behoren na een vastgestelde periode van inactiviteit te worden uitgeschakeld.

- De periode van inactiviteit van een werkstation is vastgesteld op maximaal 15 minuten. Daarna wordt de PC vergrendeld. Bij remote desktop sessies geldt dat na maximaal 15 minuten inactiviteit de sessie verbroken wordt.

11.5.6 Beperking van verbindingstijd
De verbindingstijd behoort te worden beperkt als aanvullende beveiliging voor toepassingen met een verhoogd risico.

- De toegang voor onderhoud op afstand door een leverancier wordt alleen opengesteld op basis een wijzigingsverzoek of storingsmelding.

11.6 Toegangsbeheersing voor toepassingen en informatie

Doelstelling
Voorkomen van onbevoegde toegang tot informatie in toepassingssystemen.

11.6.1 Beperken van toegang tot informatie
Toegang tot informatie en functies van toepassingssystemen door gebruikers en ondersteunend personeel behoort te worden beperkt overeenkomstig het vastgestelde toegangsbeleid.

- In de soort toegangsregels wordt ten minste onderscheid gemaakt tussen lees- en schrijfbevoegdheden.
- Managementsoftware heeft de mogelijkheid gebruikerssessies af te sluiten.
- Bij extern gebruik vanuit een onvertrouwde omgeving vindt sterke authenticatie (two-factor) van gebruikers plaats.
- Een beheerder gebruikt two-factor authenticatie voor het beheer van kritische apparaten. Bijv. een sleutel tot beveiligde ruimte en een password of een token en een password.

11.6.2 Isoleren van gevoelige systemen
Gevoelige systemen behoren een eigen, vast toegewezen (geïsoleerde) computeromgeving te hebben.

- Gevoelige systemen (met hoge beschikbaarheid of grote vertrouwelijkheid) behoren een eigen vast toegewezen (geïsoleerde) computeromgeving te hebben. Isoleren kan worden bereikt door fysieke of logische methoden.

11.7 Draagbare computers en telewerken

Doelstelling
Waarborgen van informatiebeveiliging bij het gebruik van draagbare computers en faciliteiten voor telewerken.

11.7.1 Draagbare computers en communicatievoorzieningen
Er behoort formeel beleid te zijn vastgesteld en er behoren geschikte beveiligingsmaatregelen te zijn getroffen ter bescherming tegen risico's van het gebruik van draagbare computers en communicatiefaciliteiten.

- Het mobiele apparaat is waar mogelijk zo ingericht dat geen bedrijfsinformatie wordt opgeslagen ("zero footprint"). Voor het geval dat zero footprint (nog) niet realiseerbaar is, of functioneel onwenselijk is, geldt: een mobiel apparaat (zoals een handheld computer, tablet, smartphone, PDA) biedt de mogelijkheid om de toegang te beschermen d.m.v. een wachtwoord en versleuteling van die gegevens. Voor printen in onvertrouwde omgevingen vindt een risicoafweging plaats. De Beveiligingsrichtlijnen mobiele apparaten (NCSC) worden als norm gehanteerd.
- Er zijn, waar mogelijk, voorzieningen om de actualiteit van anti-malware programmatuur op mobiele apparaten te garanderen.
- Bij melding van verlies of diefstal wordt de communicatiemogelijkheid met de centrale applicaties afgesloten.

11.7.2 Telewerken
Er behoort beleid, operationele plannen en procedures voor telewerken te worden ontwikkeld en geïmplementeerd.

- Er wordt een beleid met gedragsregels en een geschikte implementatie van de techniek opgesteld t.a.v. telewerken.
- De telewerkvoorzieningen zijn waar mogelijk zo ingericht dat op de werkplek (thuis of op een andere locatie) geen bedrijfsinformatie wordt opgeslagen ("zero footprint") en mogelijke malware vanaf de werkplek niet in het vertrouwde deel terecht kan komen. Voor printen in onvertrouwde omgevingen vindt een risicoafweging plaats.

VEILIGHEID

12. VERWERVING, ONTWIKKELING EN ONDERHOUD VAN INFORMATIE-SYSTEMEN

12.1 Beveiligingseisen voor informatiesystemen

Doelstelling

Bewerkstelligen dat beveiliging integraal deel uitmaakt van informatiesystemen.

12.1.1 Analyse en specificatie van beveiligingseisen
In bedrijfseisen voor nieuwe informatiesystemen of uitbreidingen van bestaande 2700 informatiesystemen behoren ook eisen voor beveiligingsmaatregelen te worden opgenomen.

- In projecten worden een beveiligingsrisicoanalyse en maatregelbepaling opgenomen als onderdeel van het ontwerp. Ook bij wijzigingen worden de veiligheidsconsequenties meegenomen.
- In standaarden voor analyse, ontwikkeling en testen van informatiesystemen wordt structureel aandacht besteed aan beveiligingsaspecten. Waar mogelijk wordt gebruikt gemaakt van bestaande richtlijnen (bijv. secure coding guidelines7).
- Bij aanschaf van producten wordt een proces gevolgd waarbij beveiliging een onderdeel is van de specificatie.
- Waar het gaat om beveiligingsrelevante producten wordt de keuze voor een bepaald product verantwoord onderbouwd.
- Voor beveiliging worden componenten gebruikt die aantoonbaar voldoen aan geaccepteerde beveiligingscriteria zoals NBV goedkeuring of certificering volgens ISO/IEC 15408 (common criteria).

12.2 Correcte verwerking in toepassingen

Doelstelling
Voorkomen van fouten, verlies, onbevoegde modificatie of misbruik van informatie in toepassingen.

12.2.1 Validatie van invoergegevens
Gegevens die worden ingevoerd in toepassingen behoren te worden gevalideerd om te bewerkstelligen dat deze gegevens juist en geschikt zijn.

- Er moeten controles worden uitgevoerd op de invoer van gegevens. Daarbij wordt minimaal gecontroleerd op grenswaarden, ongeldige tekens, onvolledige gegevens, gegevens die niet aan het juiste format voldoen en inconsistentie van gegevens.

12.2.2 Beheersing van interne gegevensverwerking
Er behoren validatiecontroles te worden opgenomen in toepassingen om eventueel corrumperen van informatie door verwerkingsfouten of opzettelijke handelingen te ontdekken.

- Er bestaan voldoende mogelijkheden om reeds ingevoerde gegevens te kunnen corrigeren door er gegevens aan te kunnen toevoegen.
- Het informatiesysteem moet functies bevatten waarmee vastgesteld kan worden of gegevens correct verwerkt zijn. Hiermee wordt een geautomatiseerde controle bedoeld waarmee (duidelijke) transactie- en verwerkingsfouten kunnen worden gedetecteerd.
- Stapelen van fouten wordt voorkomen door toepassing van "noodstop" mechanismen.
- Verwerkingen zijn bij voorkeur herstelbaar zodat bij het optreden van fouten en/of wegraken van informatie dit hersteld kan worden door het opnieuw verwerken van de informatie.

12.2.3 Integriteit van berichten
Er behoren eisen te worden vastgesteld, en geschikte beheersmaatregelen te worden vastgesteld en geïmplementeerd, voor het bewerkstelligen van authenticiteit en het beschermen van integriteit van berichten in toepassingen.

12.2.4 Validatie van uitvoergegevens
Gegevensuitvoer uit een toepassing behoort te worden gevalideerd, om te bewerkstelligen dat de verwerking van opgeslagen gegevens op de juiste manier plaatsvindt en geschikt is gezien de omstandigheden.

- De uitvoerfuncties van programma's maken het mogelijk om de volledigheid en juistheid van de gegevens te kunnen vaststellen (bijv. door checksums).
- Bij uitvoer van gegevens wordt gegarandeerd dat deze met het juiste niveau van vertrouwelijkheid beschikbaar gesteld worden (bijv. beveiligd printen).
- Alleen gegevens die noodzakelijk zijn voor de doeleinden van de gebruiker worden uitgevoerd (need to know).

12.3 Cryptografische beheersmaatregelen

Doelstelling
Beschermen van de vertrouwelijkheid, authenticiteit of integriteit van informatie met behulp van cryptografische middelen.

12.3.1 Beleid voor het gebruik van cryptografische beheersmaatregelen
Er behoort beleid te worden ontwikkeld en geïmplementeerd voor het gebruik van cryptografische beheersmaatregelen voor de bescherming van informatie.

- De gebruikte cryptografische algoritmen voor versleuteling zijn als open standaard gedocumenteerd en zijn door onafhankelijke betrouwbare deskundigen getoetst.
- Bij de inzet van cryptografische producten volgt een afweging van de risico's aangaande locaties, processen en behandelende partijen.
- De cryptografische beveiligingsvoorzieningen en componenten voldoen aan algemeen gangbare beveiligingscriteria (zoals FIPS 140-2 en waar mogelijk NBV).

12.3.2 Sleutelbeheer
Er behoort sleutelbeheer te zijn vastgesteld ter ondersteuning van het gebruik van cryptografische technieken binnen de organisatie.

- In het sleutelbeheer is minimaal aandacht besteed aan het proces, de actoren en hun verantwoordelijkheden.
- De geldigheidsduur van cryptografische sleutels wordt bepaald aan de hand van de beoogde toepassing en is vastgelegd in het cryptografisch beleid.
- De vertrouwelijkheid van cryptografische sleutels dient te zijn gewaarborgd tijdens generatie, gebruik, transport en opslag van de sleutels.
- Er is een procedure vastgesteld waarin is bepaald hoe wordt omgegaan met gecompromitteerde sleutels.
- Bij voorkeur is sleutelmanagement ingericht volgens PKI Overheid

12.4 Beveiliging van systeembestanden

Doelstelling
Beveiliging van systeembestanden bewerkstelligen.

12.4.1 Beheersing van operationele programmatuur
Er behoren procedures te zijn vastgesteld om de installatie van programmatuur op productiesystemen te beheersen.

- Alleen geautoriseerd personeel kan functies en software installeren of activeren.
- Programmatuur behoort pas te worden geïnstalleerd op een productieomgeving na een succesvolle test en acceptatie.
- Geïnstalleerde programmatuur, configuraties en documentatie worden bijgehouden in een configuratiedatabase.
- Er worden alleen door de leverancier onderhouden (versies van) software gebruikt.
- Van updates wordt een log bijgehouden.
- Er is een rollback strategie.

12.4.2 Bescherming van testdata
Testgegevens behoren zorgvuldig te worden gekozen, beschermd en beheerst.

- Het gebruik van kopieën van operationele databases voor testgegevens wordt vermeden. Indien toch noodzakelijk, worden de gegevens zoveel mogelijk geanonimiseerd en na de test zorgvuldig verwijderd.

12.4.3 Toegangsbeheersing voor broncode van programmatuur
De toegang tot broncode van programmatuur behoort te worden beperkt.

- De toegang tot broncode wordt zoveel mogelijk beperkt om de code tegen onbedoelde wijzigingen te beschermen. Alleen geautoriseerde personen hebben toegang.

12.5 Beveiliging bij ontwikkelings- en ondersteuningsprocessen

Doelstelling
Beveiliging van toepassingsprogrammatuur en -informatie handhaven.

12.5.1 Procedures voor wijzigingsbeheer
De implementatie van wijzigingen behoort te worden beheerst door middel van formele procedures voor wijzigingsbeheer.

- Er is aantoonbaar wijzigingsmanagement ingericht volgens gangbare best practices zoals ITIL.

12.5.2 Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem
Bij wijzigingen in besturingssystemen behoren bedrijf kritische toepassingen te worden beoordeeld en getest om te bewerkstelligen dat er geen nadelige gevolgen zijn voor de activiteiten of beveiliging van de organisatie.

- Van aanpassingen (zoals updates) aan softwarematige componenten van de technische infrastructuur wordt vastgesteld dat deze de juiste werking van de technische componenten niet in gevaar brengen.

12.5.3 Restricties op wijzigingen in programmatuurpakketten
Wijzigingen in programmatuurpakketten behoren te worden ontmoedigd, te worden beperkt tot noodzakelijke wijzigingen, en alle wijzigingen behoren strikt te worden beheerst.

- Bij het instellen van besturingsprogrammatuur en programmapakketten wordt uitgegaan van de aanwijzingen van de leverancier.

12.5.4 Uitlekken van informatie
Er behoort te worden voorkomen dat zich gelegenheden voordoen om informatie te laten uitlekken.

- Op het grensvlak van een vertrouwde en een onvertrouwde omgeving vindt content-scanning plaats.

12.5.5 Uitbestede ontwikkeling van programmatuur
Uitbestede ontwikkeling van programmatuur behoort onder supervisie te staan van en te worden gecontroleerd door de organisatie.

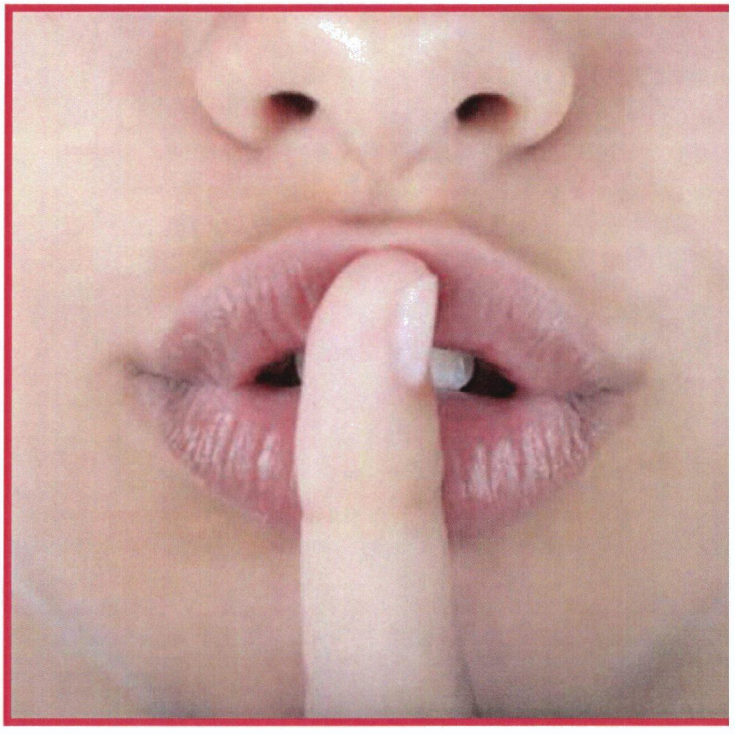
- Uitbestede ontwikkeling van programmatuur komt tot stand onder supervisie en verantwoordelijkheid van de uitbestedende organisatie. Er worden maatregelen getroffen om de kwaliteit en vertrouwelijkheid te borgen (bijv. stellen van veiligheidseisen, regelen van beschikbaarheid en eigendomsrecht van de code, certificatie, kwaliteitsaudits, testen en aansprakelijkheidsregelingen).

12.6 Beheer van technische kwetsbaarheden

Doelstelling
Risico's verminderen als gevolg van benutting van gepubliceerde technische kwetsbaarheden.

12.6.1 Beheersing van technische kwetsbaarheden
Er behoort tijdig informatie te worden verkregen over technische kwetsbaarheden van de gebruikte informatiesystemen. De mate waarin de organisatie blootstaat aan dergelijke kwetsbaarheden behoort te worden geëvalueerd en er behoren geschikte maatregelen te worden genomen voor behandeling van daarmee samenhangende risico's.

- Er is een proces ingericht voor het beheer van technische kwetsbaarheden; dit omvat minimaal periodieke penetratietests, risicoanalyses van kwetsbaarheden en patching.
- Van softwarematige voorzieningen van de technische infrastructuur kan (bij voorkeur geautomatiseerd) gecontroleerd worden of de laatste updates (patches) in zijn doorgevoerd. Het doorvoeren van een update vindt niet geautomatiseerd plaats, tenzij hier speciale afspraken over zijn met de leverancier.
- Indien een patch beschikbaar is, dienen de risico's verbonden met de installatie van de patch te worden geëvalueerd (de risico's verbonden met de kwetsbaarheid dienen vergeleken te worden met de risico's van het installeren van de patch).
- Updates/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is worden zo spoedig mogelijk doorgevoerd, echter minimaal binnen één week. Minder kritische beveiligingsupdates/patches moeten worden ingepland bij de eerst volgende onderhoudsronde.



VEILIGHEID

13. BEHEER VAN INFORMATIE-BEVEILIGINGSINCIDENTEN

13.1 Rapportage van informatiebeveiligingsgebeurtenissen en zwakke plekken - Doelstelling
Bewerkstelligen dat informatiebeveiligingsgebeurtenissen en zwakheden die verband houden met informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen.

13.1.1 Rapportage van informatiebeveiligingsgebeurtenissen
Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.

- Er is een procedure voor het rapporteren van beveiligingsgebeurtenissen vastgesteld, in combinatie met een reactie- en escalatieprocedure voor incidenten, waarin de handelingen worden vastgelegd die moeten worden genomen na het ontvangen van een rapport van een beveiligingsincident.
- Er is een procedure voor communicatie met de CERT van de IBD.
- Er is een contactpersoon aangewezen voor het rapporteren van beveiligingsincidenten. Voor integriteitsschendingen is ook een vertrouwenspersoon aangewezen die meldingen in ontvangst neemt.
- Beveiligingsincidenten worden vastgelegd in een systeem en geëscaleerd aan de CERT van de IBD.
- Vermissing of diefstal van apparatuur of media die gegevens van de Rijksdienst kunnen bevatten wordt altijd ook aangemerkt als informatiebeveiligingsincident.
- Informatie over de beveiligingsrelevante handelingen van de gebruiker wordt regelmatig nagekeken. De CISO bekijkt maandelijks een samenvatting van de informatie.

13.1.2 Rapportage van zwakke plekken in de beveiliging
Van alle werknemers, ingehuurd personeel en externe gebruikers van informatiesystemen en –diensten behoort te worden geëist dat zij alle waargenomen of verdachte zwakke plekken in systemen of diensten registreren en rapporteren.

- Er is een proces om eenvoudig en snel beveiligingsincidenten en zwakke plekken in de beveiliging te melden.

13.2 Beheer van informatiebeveiligingsincidenten en –verbeteringen

Doelstelling
Bewerkstelligen dat een consistente en doeltreffende benadering wordt toegepast voor het beheer van informatiebeveiligingsincidenten.

13.2.1 Verantwoordelijkheden en procedures
Er behoren leidinggevende verantwoordelijkheden en procedures te worden vastgesteld om een snelle, doeltreffende en ordelijke reactie op informatiebeveiligingsincidenten te bewerkstelligen.

- Er zijn procedures voor rapportage van gebeurtenissen en escalatie. Alle medewerkers behoren op de hoogte te zijn van deze procedures.

VEILIGHEID

13.2.2 Leren van informatiebeveiligingsincidenten

Er behoren mechanismen te zijn ingesteld waarmee de aard, omvang en kosten van informatiebeveiligingsincidenten kunnen worden gekwantificeerd en gecontroleerd.

- De informatie verkregen uit het beoordelen van beveiligingsmeldingen wordt geëvalueerd met als doel beheersmaatregelen te verbeteren.

13.2.3 Verzamelen van bewijsmateriaal

Waar een vervolgprocedure tegen een persoon of organisatie na een informatiebeveiligingsincident juridische maatregelen omvat (civiel of strafrechtelijk), behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.

- Voor een vervolgprocedure naar aanleiding van een beveiligingsincident behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.

VEILIGHEID

14. BEDRIJFSCONTINUÏTEITSBEHEER

14.1 Informatiebeveiligingsaspecten van bedrijfscontinuiteït beheer -

Doelstelling
Tegengaan van onderbreking van bedrijfsactiviteiten en bescherming van kritische bedrijfsprocessen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.

14.1.1 Informatiebeveiliging opnemen in het proces van bedrijfscontinuïteitsbeheer
Er behoort een beheerd proces voor bedrijfscontinuïteit in de gehele organisatie te worden ontwikkeld en bijgehouden, voor de naleving van eisen voor informatiebeveiliging die nodig zijn voor de continuïteit van de bedrijfsvoering.

- Calamiteitenplannen worden gebruikt in de jaarlijkse bewustwording-, training- en testactiviteiten.

14.1.2 Bedrijfscontinuïteit en risicobeoordeling
Gebeurtenissen die tot onderbreking van bedrijfsprocessen kunnen leiden, behoren te worden geïdentificeerd, tezamen met de waarschijnlijkheid en de gevolgen van dergelijke onderbrekingen en hun gevolgen voor informatiebeveiliging.

- Er is een Business Impact Analyse (BIA) waarin de gebeurtenissen worden geïdentificeerd die kunnen leiden tot discontinuïteit in het bedrijfsproces. Aan de hand van een risicoanalyse zijn de waarschijnlijkheid en de gevolgen van de discontinuïteit in kaart gebracht in termen van tijd, schade en herstelperiode.

14.1.3 Continuïteitsplannen ontwikkelen en implementeren waaronder informatiebeveiliging
Er behoren plannen te worden ontwikkeld en geïmplementeerd om de bedrijfsactiviteiten te handhaven of te herstellen en om de beschikbaarheid van informatie op het vereiste niveau en in de vereiste tijdspanne te bewerkstelligen na onderbreking of uitval van kritische bedrijfsprocessen.

- In de continuïteitsplannen wordt minimaal aandacht besteed aan:
  - Identificatie van essentiële procedures voor bedrijfscontinuïteit.
  - Wie het plan mag activeren en wanneer, maar ook wanneer er weer gecontroleerd teruggaan wordt.
  - Veilig te stellen informatie (aanvaardbaarheid van verlies van informatie).
  - Prioriteiten en volgorde van herstel en recon structie.
  - Documentatie van systemen en processen.
  - Kennis en kundigheid van personeel om de processen weer op te starten.

14.1.4 Kader voor de bedrijfscontinuïteitsplanning
Er behoort een enkelvoudig kader voor bedrijfscontinuïteitsplannen te worden gehandhaafd om te bewerkstelligen dat alle plannen consistent zijn, om eisen voor informatiebeveiliging op consistente wijze te behandelen en om prioriteiten vast te stellen voor testen en onderhoud.

14.1.5 Testen, onderhoud en herbeoordelen van bedrijfscontinuïteitsplannen
Bedrijfscontinuïteitsplannen behoren regelmatig te worden getest en ge-update, om te bewerkstelligen dat ze actueel en doeltreffend blijven.

- Er worden minimaal jaarlijks oefeningen en testen gehouden om de bedrijfscontinuïteitsplannen en mate van readiness van de organisatie te toetsen (opzet, bestaan en werking). Aan de hand van de resultaten worden de plannen bijgesteld en wordt de organisatie bijgeschoold.

VEILIGHEID

15. NALEVING

15.1 Naleving van wettelijke voorschriften - Doelstelling
Voorkomen van schending van enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen, en van enige beveiligingseisen.

15.1.1 Identificatie van toepasselijke wetgeving
Alle relevante wettelijke en regelgevende eisen en contractuele verplichtingen en de benadering van de organisatie in de naleving van deze eisen, behoren expliciet te worden vastgesteld, gedocumenteerd en actueel te worden gehouden voor elk informatiesysteem en voor de organisatie.

Er is vastgesteld welke wetten en wettelijke maatregelen van toepassing zijn op de organisatie of organisatieonderdelen.

Voor gemeenten zijn dit (niet uitputtend):

- Wet BAG
- Wet Bescherming Persoonsgegevens / Richtsnoeren Beveiliging Persoonsgegevens
- Wet GBA
- Regeling SUWI
- Ambtenarenwet
- Beveiligingsnorm DigiD
- Verantwoordingsrichtlijn SUWI

15.1.2 Intellectuele eigendomsrechten (intellectual property rights)
Er behoren geschikte procedures te worden geïmplementeerd om te bewerkstelligen dat wordt voldaan aan de wettelijke en regelgevende eisen en contractuele verplichtingen voor het gebruik van materiaal waarop intellectuele eigendomsrechten kunnen berusten en het gebruik van programmatuur waarop intellectuele eigendomsrechten berusten.

- Er is toezicht op het naleven van wettelijke verplichtingen m.b.t. intellectueel eigendom, auteursrechten en gebruiksrechten.

15.1.3 Bescherming van bedrijfsdocumenten
Belangrijke registraties behoren te worden beschermd tegen verlies, vernietiging en vervalsing, overeenkomstig wettelijke en regelgevende eisen, contractuele verplichtingen en bedrijfsmatige eisen.

15.1.4 Bescherming van gegevens en geheimhouding van persoonsgegevens
De bescherming van gegevens en privacy behoort te worden bewerkstelligd overeenkomstig relevante wetgeving, voorschriften en indien van toepassing contractuele bepalingen.

15.1.5 Voorkomen van misbruik van it voorzieningen
Gebruikers behoren ervan te worden weerhouden IT voorzieningen te gebruiken voor onbevoegde doeleinden.

- Er is een beleid met betrekking tot het gebruik van IT voorzieningen door gebruikers. Dit beleid is bekendgemaakt en op de goede werking ervan wordt toegezien.

15.1.6 voorschriften voor het gebruik van cryptografische beheersmaatregelen
Cryptografische beheersmaatregelen behoren overeenkomstig alle relevante overeenkomsten, wetten en voorschriften te worden gebruikt.

- Er is vastgesteld aan welke overeenkomsten, wetten en voorschriften de toepassing van cryptografische technieken moet voldoen. Zie ook 12.3.

15.2 Naleving van beveiligingsbeleid en -normen en technische naleving

Doelstelling
Bewerkstelligen dat systemen voldoen aan het beveiligingsbeleid en de beveiligingsnormen van de organisatie.

15.2.1 Naleving van beveiligingsbeleid en -normen
Managers behoren te bewerkstelligen dat alle beveiligingsprocedures die binnen hun verantwoordelijkheid vallen correct worden uitgevoerd om naleving te bereiken van beveiligingsbeleid en -normen.

- Het lijnmanagement is verantwoordelijk voor uitvoering en beveiligingsprocedures en toetsing daarop (o.a. jaarlijkse in control verklaring). Conform het BVR zorgt de Beveiligingsambtenaar, namens de Secretaris Generaal, voor het toezicht op de uitvoering van het beveiligingsbeleid. Daarbij behoren ook periodieke beveiligingsaudits. Deze kunnen worden uitgevoerd door of vanwege de CISO dan wel door interne of externe auditteams.
- In de P&C cyclus wordt gerapporteerd over informatiebeveiliging aan de hand van het in control statement.

15.2.2 Controle op technische naleving
Informatiesystemen behoren regelmatig te worden gecontroleerd op naleving van implementatie van beveiligingsnormen.

- Informatiesystemen worden regelmatig gecontroleerd op naleving van beveiligingsnormen. Dit kan door bijv. kwetsbaarheidsanalyses en penetratietesten. Zie ook 12.6.1.1.

15.3 Overwegingen bij audits van informatiesystemen

Doelstelling
Doeltreffendheid van audits van het informatiesysteem maximaliseren en verstoring als gevolg van systeemaudits minimaliseren.

15.3.1 Beheersmaatregelen voor audits van informatiesystemen
Eisen voor audits en andere activiteiten waarbij controles worden uitgevoerd op productiesystemen, behoren zorgvuldig te worden gepland en goedgekeurd om het risico van verstoring van bedrijfsprocessen tot een minimum te beperken.

15.3.2 bescherming van hulpmiddelen voor audits van informatiesystemen
Toegang tot hulpmiddelen voor audits van informatiesystemen behoort te worden beschermd om mogelijk misbruik of compromittering te voorkomen.

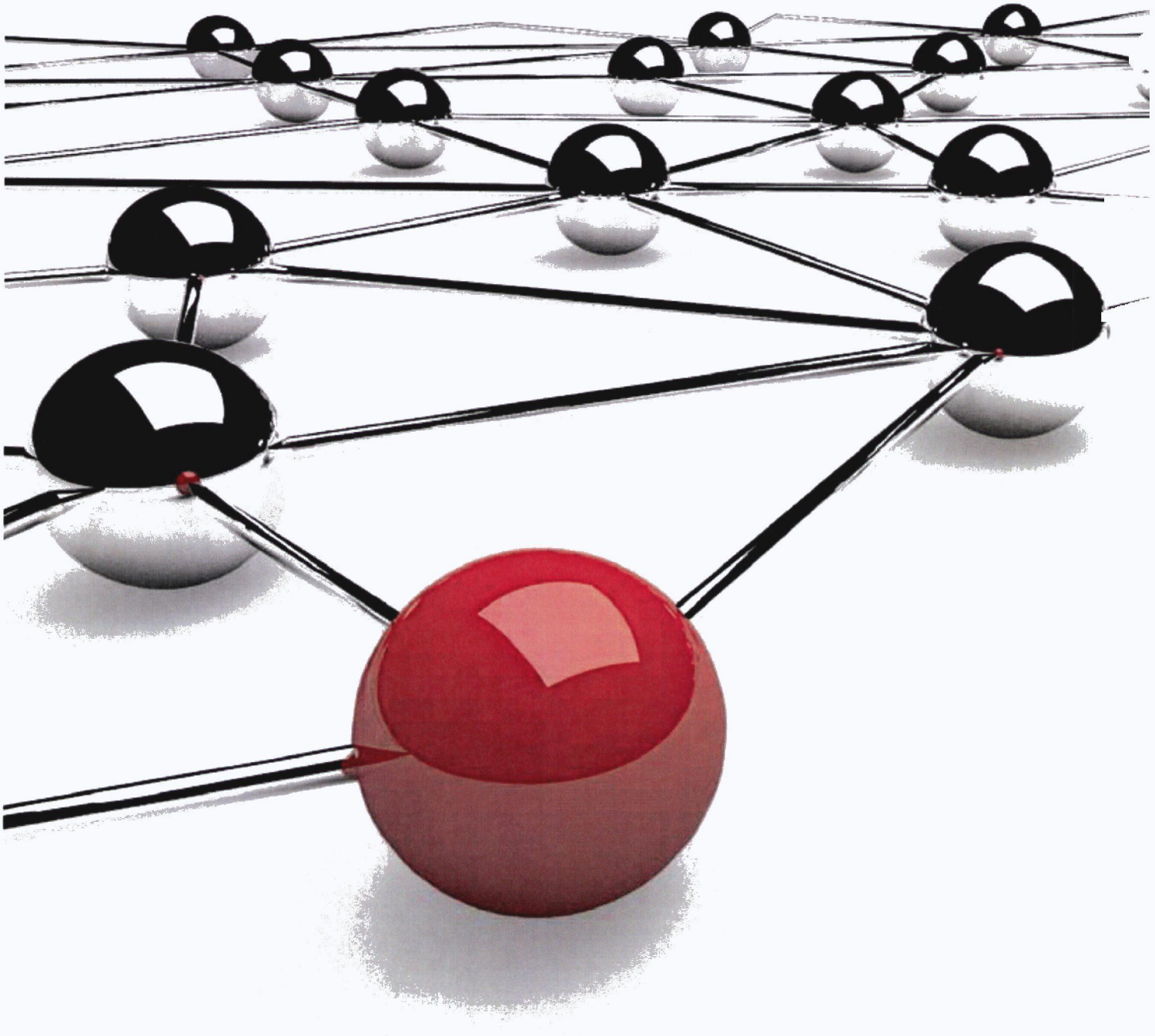
BIJLAGE MAPPING MAATREGELEN

Sectie	SubSectie	Gebied	Omschrijving	GBA	SUWI	BAG	WBP	PUN
5	1	1	Beleidsdocument voor informatiebeveiliging	X	X		X	X
5	1	2	Beoordeling van het informatiebeveiligingsbeleid	X	X		X	X
6	1	1	Betrokkenheid van het College bij informatiebeveiliging	X	X		X	X
6	1	2	Coördinatie van informatiebeveiliging	X	X		X	X
6	1	3	Toewijzing van verantwoordelijkheden voor informatiebeveiliging	X	X		X	X
6	1	4	Goedkeuringsproces voor ICT-voorzieningen	X	X		X	X
6	1	5	Geheimhoudingsovereenkomst	X	X		X	X
6	1	6	Contact met overheidsinstanties					
6	1	7	Contact met speciale belangengroepen					
6	1	8	Onafhankelijke beoordeling van informatiebeveiliging	X	X		X	X
6	2	1	Identificatie van risico's die betrekking hebben op externe partijen	X	X		X	X
6	2	2	Beveiliging behandelen in de omgang met klanten		X			X
6	2	3	Beveiliging behandelen in overeenkomsten met een derde partij	X	X		X	X
7	1	1	Inventarisatie van bedrijfsmiddelen	X	X		X	X
7	1	2	Eigendom van bedrijfsmiddelen	X	X		X	X
7	1	3	Aanvaardbaar gebruik van bedrijfsmiddelen	X	X		X	X
7	2	1	Richtlijnen voor het classificeren		X		X	
7	2	2	Labeling en verwerking van informatie		X		X	
8	1	1	Rollen en verantwoordelijkheden	X	X		X	X
8	1	2	Screening	X	X		X	X
8	1	3	Arbeidsvoorwaarden	X	X		X	X
8	2	1	Directieverantwoordelijkheid	X	X		X	X
8	2	2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	X	X		X	X
8	2	3	Disciplinaire maatregelen	X	X		X	X
8	3	1	Beëindiging van verantwoordelijkheden	X	X		X	X
8	3	2	Retournering van bedrijfsmiddelen	X	X		X	X
8	3	3	Blokkering van toegangsrechten	X	X		X	X
9	1	1	Fysieke beveiliging van de omgeving	X	X		X	X
9	1	2	Fysieke toegangsbeveiliging	X	X		X	X
9	1	3	Beveiliging van kantoren, ruimten en faciliteiten	X	X		X	X
9	1	4	Bescherming tegen bedreigingen van buitenaf	X	X		X	X
9	1	5	Werken in beveiligde ruimten	X	X		X	X
9	1	6	Openbare toegang en gebieden voor laden en lossen		X			X
9	2	1	Plaatsing en bescherming van apparatuur	X	X		X	X
9	2	2	Nutsvoorzieningen	X	X		X	X
9	2	3	Beveiliging van kabels		X			
9	2	4	Onderhoud van apparatuur	X	X		X	X
9	2	5	Beveiliging van apparatuur buiten het terrein	X	X		X	X

Sectie	SubSectie	Gebied	Omschrijving	GBA	SUWI	BAG	WBP	PUN
9	2	6	Veilig verwijderen en hergebruiken van apparatuur	X	X		X	X
9	2	7	Verwijdering van bedrijfseigendommen	X	X		X	X
10	1	1	Gedocumenteerde bedieningsprocedures	X	X		X	X
10	1	2	Wijzigingsbeheer	X	X		X	X
10	1	3	Functiescheiding	X	X		X	X
10	1	4	Scheiding van faciliteiten voor ontwikkeling, testen en productie		X			X
10	2	1	Dienstverlening	X	X		X	X
10	2	2	Controle en beoordeling van dienstverlening door een derde partij	X	X		X	X
10	2	3	Beheer van wijzigingen in dienstverlening door een derde partij	X	X		X	X
10	3	1	Capaciteitsbeheer	X	X		X	
10	3	2	Systeemacceptatie	X	X		X	
10	4	1	Maatregelen tegen virussen	X	X		X	X
10	4	2	Maatregelen tegen 'mobile code'	X	X		X	X
10	5	1	Reservekopieën maken (back-ups)	X	X		X	X
10	6	1	Maatregelen voor netwerken	X	X		X	X
10	6	2	Beveiliging van netwerkdiensten	X	X		X	X
10	7	1	Beheer van verwijderbare media	X	X		X	X
10	7	2	Verwijdering van media	X	X		X	X
10	7	3	Procedures voor de behandeling van informatie	X	X		X	X
10	7	4	Beveiliging van systeemdocumentatie	X	X		X	X
10	8	1	Beleid en procedures voor informatie-uitwisseling	X	X		X	X
10	8	2	Uitwisselingsovereenkomsten	X	X		X	X
10	8	3	Fysieke media die worden getransporteerd	X	X		X	X
10	8	4	Elektronische berichtuitwisseling	X	X		X	X
10	8	5	Systemen voor bedrijfsinformatie	X	X		X	X
10	9	1	E-commerce					
10	9	2	Online transacties	X	X		X	X
10	9	3	Openbaar beschikbare informatie	X	X		X	
10	10	1	Aanmaken auditlogbestanden	X	X		X	X
10	10	2	Controle van systeemgebruik	X	X		X	X
10	10	3	Bescherming van informatie in logbestanden	X	X		X	X
10	10	4	Logbestanden van administrators en operators	X	X		X	X
10	10	5	Registratie van storingen	X	X		X	X
10	10	6	Synchronisatie van systeemklokken					
11	1	1	Toegangsbeleid	X	X		X	X
11	2	1	Registratie van gebruikers	X	X		X	X
11	2	2	Beheer van speciale bevoegdheden	X	X		X	X
11	2	3	Beheer van gebruikerswachtwoorden	X	X		X	X
11	2	4	Beoordeling van toegangsrechten van gebruikers	X	X		X	X
11	3	1	Gebruik van wachtwoorden	X	X		X	X
11	3	2	Onbeheerde gebruikersapparatuur	X	X		X	X
11	3	3	'Clear desk'- en 'clear screen'-beleid	X	X		X	X
11	4	1	Beleid ten aanzien van het gebruik van netwerkdiensten	X	X		X	X
11	4	2	Authenticatie van gebruikers bij externe verbindingen.	X	X		X	X
11	4	3	Identificatie van (netwerk)apparatuur	X	X		X	X

Sectie	SubSectie	Gebied	Omschrijving	GBA	SUWI	BAG	WBP	PUN
11	4	4	Bescherming op afstand van poorten voor diagnose en configuratie	X	X		X	X
11	4	5	Scheiding van netwerken	X	X		X	X
11	4	6	Beheersmaatregelen voor netwerkverbindingen	X	X		X	X
11	4	7	Beheersmaatregelen voor netwerkroutering	X	X		X	X
11	5	1	Beveiligde inlogprocedures	X	X		X	X
11	5	2	Gebruikersidentificatie en -authenticatie	X	X		X	X
11	5	3	Systemen voor wachtwoordbeheer	X	X		X	X
11	5	4	Gebruik van systeemhulpmiddelen	X	X		X	X
11	5	5	Time-out van sessies	X	X		X	X
11	5	6	Beperking van verbindingstijd	X	X		X	X
11	6	1	Beperking van toegang tot informatie	X	X		X	X
11	6	2	Isolatie van gevoelige systemen	X	X		X	X
11	7	1	Draagbare computers en communicatievoorzieningen	X	X		X	
11	7	2	Telewerken	X	X		X	
12	1	1	Analyse en specificatie van beveiligingseisen	X	X		X	X
12	2	1	Validatie van invoergegevens	X	X		X	X
12	2	2	Beheersing van interne gegevensverwerking	X	X	X	X	X
12	2	3	Integriteit van berichten	X	X	X	X	X
12	2	4	Validatie van uitvoergegevens	X	X		X	X
12	3	1	Beleid voor het gebruik van cryptografische beheersmaatregelen	X	X		X	X
12	3	2	Sleutelbeheer	X	X		X	X
12	4	1	Beheersing van operationele software	X	X		X	X
12	4	2	Bescherming van test data					
12	4	3	Toegangsbeheersing voor broncode van programmatuur					
12	5	1	Procedures voor wijzigingsbeheer				X	X
12	5	2	Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem				X	X
12	5	3	Restricties op wijzigingen in programmatuurpakketten					
12	5	4	Uitlekken van informatie	X	X		X	X
12	5	5	Uitbestede ontwikkeling van programmatuur					
12	6	1	Beheersing van technische kwetsbaarheden	X			X	X
13	1	1	Rapportage van informatiebeveiligingsgebeurtenissen	X	X		X	X
13	1	2	Rapportage van zwakke plekken in de beveiliging	X	X		X	X
13	2	1	Verantwoordelijkheden en procedures	X	X		X	X
13	2	2	Leren van informatiebeveiligingsincidenten	X	X		X	X
13	2	3	Verzamelen van bewijsmateriaal	X	X		X	X
14	1	1	Informatiebeveiliging opnemen in het proces van bedrijfscontinuïteitsbeheer	X	X	X	X	
14	1	2	Bedrijfscontinuïteit en risicobeoordeling	X	X	X	X	
14	1	3	Continuïteitsplannen ontwikkelen en implementeren waaronder informatiebeveiliging	X	X	X	X	
14	1	4	Kader voor de bedrijfscontinuïteitsplanning	X	X	X	X	
14	1	5	Testen, onderhoud en herbeoordelen van continuïteitsplannen	X	X	X	X	
15	1	1	Identificatie van toepasselijke wetgeving	X	X		X	X
15	1	2	Intellectuele eigendomsrechten (Intellectual Property Rights, IPR)					

15	1	3	Bescherming van bedrijfsdocumenten	X	X		X	X
15	1	4	Bescherming van gegevens en geheimhouding van persoonsgegevens	X	X		X	X
15	1	5	Voorkoming van misbruik van ICT-voorzieningen	X	X		X	
15	1	6	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	X	X		X	
15	2	1	Naleving van beveiligingsbeleid en -normen	X	X		X	X
15	2	2	Controle op technische naleving	X	X		X	
15	3	1	Beheersmaatregelen voor audits van informatiesystemen	X	X		X	X
15	3	2	Bescherming van hulpmiddelen voor audits van informatiesystemen	X	X		X	X



Vervolg 'Beleid voor informatiebeveiliging' in het 'Normenkader informatiebeveiliging'.

gemeente Haarlemmermeer

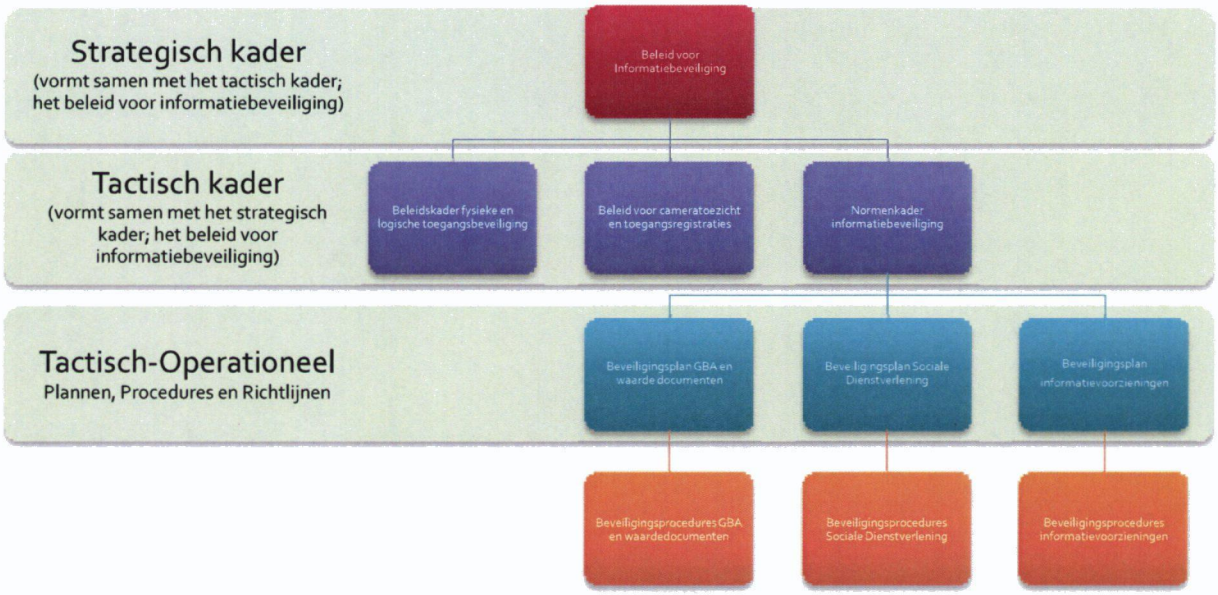
Beveiligingsplan Sociale Dienstverlening

Tactisch beveiligingsplan 2013-2014,
gebaseerd op risicoanalyse maart 2013

INHOUDSOPGAVE

Inleiding

De gemeente Haarlemmermeer heeft als organisatie een beleid voor informatiebeveiliging. Dit beleid is ingericht conform het onderstaande schema. Het Beleid voor informatiebeveiliging en het Normenkader informatiebeveiliging vormen gezamenlijk het gemeentelijk beleid voor informatiebeveiliging.



Dit document beschrijft het beveiligingsplan op tactisch-operationeel niveau opgesteld voor het cluster Sociale Dienstverlening en andere organisatieonderdelen die gebruik maken van de SUWI-ketenvoorzieningen.

Dit plan wordt door het managementteam van het cluster vastgesteld. Dit cluster heeft een eigen beveiligingsplan, omdat Sociale Dienstverlening binnen de gemeente als organisatieonderdeel wordt gezien, waar meer dan in andere organisatieonderdelen met privacygevoelige informatie wordt gewerkt en verbijzonderde aandacht voor beveiliging nodig is.

Doel is tevens om hiermee tegemoet te komen aan de in de SUWI-keten geldende Verantwoordingsrichtlijn ten aanzien van beveiliging en dat de daaruit gelden verplichtingen nader worden bekeken in een jaarlijkse risicoanalyse sessie. De resultaten van die sessie zijn in dit beveiligingsplan terug te vinden en vormen de basis voor het advies en implementatievoorstel.

Organisatie en proces

Binnen dit document wordt het beveiligingsproces voor Sociale Dienstverlening beschreven. Organisatie breed geldende processen op het gebied van informatiebeveiliging worden reeds benoemd en beschreven in het Normenkader Informatiebeveiliging. Hier treft u een verdiepende toelichting op het proces in de context van Sociale Dienstverlening. Daarnaast worden de resultaten uit de jaarlijkse risicoanalyse in dit document weergegeven.

1.1 Ontwikkelingen

Ten tijde van schrijven van dit document is de cluster Sociale Dienstverlening sterk in ontwikkeling. Naast het optimaliseren van de ICT, zijn diverse projecten gaande als het beschrijven en LEAN maken van de belangrijkste werkprocessen, het opstellen en mogelijk maken van uitvoer van een Informatieplan, en, als onderdeel van het opgestelde Kwaliteitsplan, het verder borgen van de Administratieve Organisatie en de Interne Controle. In 2013 is bovendien sprake van een reorganisatie van de cluster.

De cluster Sociale Dienstverlening is verantwoordelijk voor het uitvoeren van sociale zekerheidswetten als de WWB, IOAW, IOAZ, Bbz 2004, wet Gemeentelijke Schuldhulpverlening, Wet Inburgering en de Wmo*. In het kader van de geplande transities van taken van rijk naar gemeenten, wordt cluster Sociale Dienstverlening in de toekomst naar verwachting verantwoordelijk voor uitvoer van een Participatiewet (of een variant daarop). De wet is een bundeling van de WWB, WSW en (deels) de WAJONG. Ook voor Wmo en de jeugdzorg staan transities gepland. Ten tijde van schrijven van dit document heeft het kabinet nog geen besluit genomen over alle transities. Voor zover mogelijk, is rekening gehouden met de geplande transities bij het opstellen van de beveiligingsprocedures.

Medio 2013 staat de omslag naar het werken met de LEAN-werkprocessen gepland. Kenmerkend hierbij is:

- 1 Toetsmoment aan het begin van het proces (integrale intake voor werk, inkomen en zorg)
- Standaardiseren en automatiseren meldingen SDV (via Green Valley)
- 1 Balie (Frontoffice SDV vervalt, rol Haarlemmermeers Contact Centre wordt groter)
- Geen aanvraag zonder integrale intake/melding
- Automatisch inlezen van klantgegevens in GWS4ALL (o.a. van integraal meldingsformulier in Green Valley)
- Generieke processen voor werk, inkomen en zorg
- Het vervangen van fiatteringen door een nieuwe vorm van Interne Controle
- Maximaal gebruik van brongegevens die al beschikbaar zijn (koppelingen tussen de diverse applicaties: GBA-V - Suwinet - Green Valley - GWS4ALL).

De omslag naar LEAN-werkprocessen, brengt nieuwe aandachtspunten met zich mee voor de beveiligingsprocedures. Lag de focus voorheen op een veilig en zorgvuldig gebruik van de applicatie Suwinet, anno 2013 is het noodzakelijk verder te kijken in verband met de koppelingen tussen de diverse applicaties (GBA-V - Suwinet - Green Valley - GWS4ALL – Suites en Keys GWS4ALL). Ook de integraliteit van het nieuwe werkproces Poortwachter brengt voor wat betreft beveiligingsprocedures aandachtspunten met zich mee. Brongegevens uit Suwinet mogen immers enkel worden benut voor aanvragen Werk en Inkomen en niet voor Zorg (bijv. Wmo).

* De handhaving van de Leerplichtwet geschiedt ook vanuit cluster SDV, echter is buiten beschouwing gelaten bij dit document.

2.2 LEAN Processen Sociale Dienstverlening

Per juli 2013 wordt de omslag naar de LEAN werkprocessen gemaakt. De primaire dienstverleningsprocessen voor Werk, Inkomen en Zorg zijn:

1. Melding en Poortwachter
   Integrale klantmelding en poortwachter (intakegesprek aan de keukentafel dan wel in spreekkamer) .
   Beoordeling en Besluit (indien melding tot productaanvraag van SDV leidt).
2. Afhandeling Aanvraag
   Administratieve afhandeling van het besluit van de poortwachter (vullen applicaties als GWS4ALL, beschikking verzenden en archiveren, leveren door betaling in GWS4ALL te zetten dan wel opdracht geven tot levering derde).
3. Begeleiding
   Beoordelen voortgang of beëindigen traject van klant.
4. Mutatie / Beëindiging
   Beoordelen, besluiten en afhandelen van signalen wijziging lopend product.
5. Terugvordering
   Terugvordering en incasso van ten onrechte uitbetaald geld o.g.v. de diverse regelingen.

   Debiteurenonderzoek.
6. Verhaal
   Verhaal en incasso van bijstand op onderhoudsplichtigen.
   Verhaalsonderzoek.
7. Fraude
   Beoordelen (onderzoeken) en indien nodig besluiten op fraudesignalen.
8. Betalingsverkeer

   Betreft al het betalingsverkeer met SDV-cliënten, onafhankelijk van uitvoering.

In het kader van ondersteuning, controle en verantwoording bestaan de volgende processen:

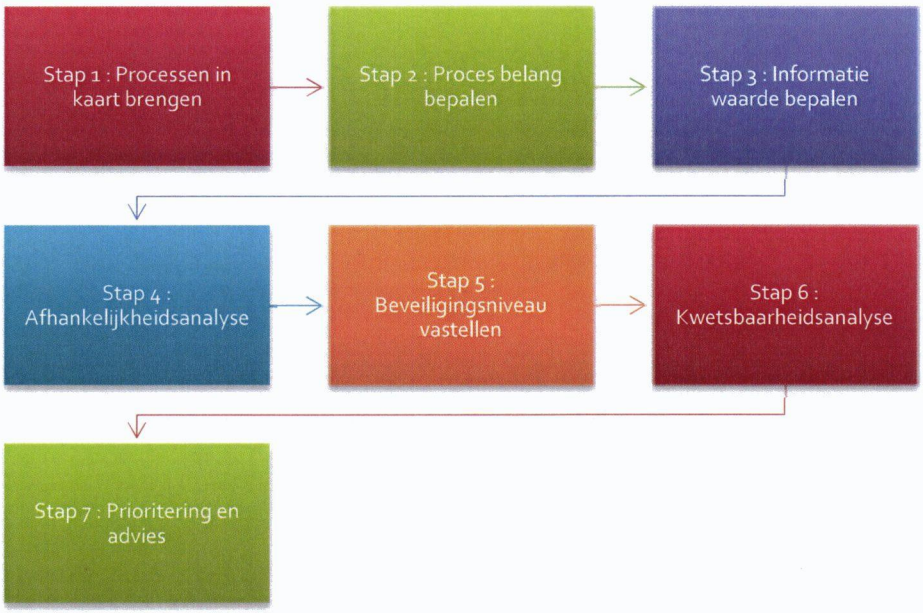
1. Interne Controle (IC)
   IC-maatregelen hebben plaats in de uitvoering (toetsing-op-maat door controlerend medewerkers) alsmede onafhankelijk van de uitvoering (diverse script- en bestandsanalyses)
2. Verbijzonderde Interne Controle (VIC)
   Onafhankelijk van de uitvoering vindt structureel dan wel thematisch IC-onderzoek plaats op de uitvoering.
3. Verantwoording aan de accountant
   Middels aanlevering van rechtmatigheidsonderzoeken vanuit de VIC en het financiële jaaroverzicht wordt verantwoording afgelegd aan de accountant.
4. Ondersteuning vanuit Bedrijfsbureau

   Relevant m.b.t. o.a. herstelacties fouten GWS4all door applicatiebeheer / financieel kwaliteitsmedewerkers.

Risico-inventarisatie

Belang van proces en informatie

Het inschalen van het belang van het proces, het bepalen van de waarde van de gebruikte informatie en de mate van afhankelijkheid van de informatie in het proces resulteert in het te kiezen beveiligingsniveau. Uitgaande van het proces, de informatie en het beveiligingsniveau worden de bedreigingen en tegenmaatregelen geïnventariseerd.



2.1 Inschatten procesbelang

Ter ondersteuning van de informatiebeveiliging worden drie procesniveaus onderscheiden. Iedere proceseigenaar dient zijn proces in te delen in één van de drie niveaus.

1. Maatschappelijk vitaal
Verstoring van dit proces resulteert in schade voor de burger en aanmerkelijke (imago)schade voor uw gemeente.

2. Bedrijf vitaal
Verstoring van dit proces resulteert in aanmerkelijke schade voor uw gemeente en/of aan haar gelieerde partners.

3. Ondersteunend
Verstoring van dit proces resulteert uitsluitend in interne schade binnen uw gemeente.

2.2 Vaststellen informatiewaarde

Informatie vertegenwoordigt op ieder moment in de tijd een bepaalde waarde. Gedurende de levensduur van de informatie kan deze waarde toe- of afnemen. De intrinsieke waarde van de informatie wordt onder andere bepaald door het belang dat anderen er aan hechten, wat het afbreukrisico is voor de organisatie en het tijdstip. De waarde wordt uitgedrukt in de begrippen Hoog, Midden en Laag.

2.3 Afhankelijkheidsanalyse

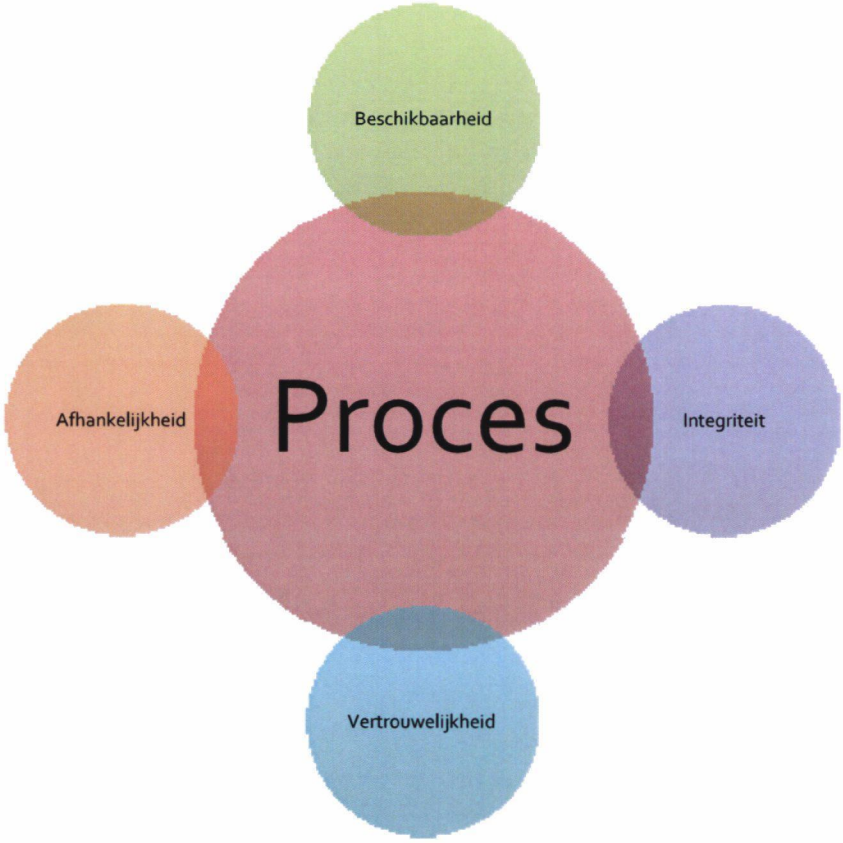
Ieder proces steunt in meer of mindere mate op informatie. Er moet worden vastgesteld in hoeverre het proces kan blijven functioneren zonder informatie, met beperkte informatie of met onjuiste informatie. Daarbij moet rekening worden gehouden met alternatieve manieren van het verkrijgen van informatie of andere manieren van werken. Elke informatiebron wordt beoordeeld.

De afhankelijkheid van informatie is uit te drukken in drie niveaus: Aanvullend, Nuttig en Noodzakelijk.

Afhankelijkheid	Omschrijving
Noodzakelijk	Dit is de pilaar waarop het werkproces rust. Deze informatie wordt direct gemist. Doorwerken zonder deze informatie betekent een gevoelige terugval in het proces.
Nuttig	Deze informatie ondersteunt het werkproces, en zal gemist worden. Het is wel mogelijk tijdelijk zonder de informatie door te werken.
Aanvullend	Deze informatie bevestigt andere bronnen binnen het werkproces en zal niet direct gemist worden.

2.4 Niveau van beveiliging

Op basis van de waarde van de informatie, het belang van het proces en de afhankelijkheid van de informatie bepaalt de proceseigenaar het gewenste beveiligingsniveau. De informatie-eigenaar heeft hierin een aanvullende rol, aangezien deze op basis van de waarde van de informatie eisen kan stellen aan de proceseigenaar. Voor beveiliging worden, conform het beleid, drie niveaus onderkend. Deze niveaus zijn Hoog, Midden en Laag. Per niveau zijn eisen gesteld ten aanzien van beschikbaarheid, exclusiviteit en integriteit. Om deze eisen meetbaar te maken, zijn ze uitgesplitst naar de vier typen maatregelen: voorkomen, beperken, opsporen en herstellen.



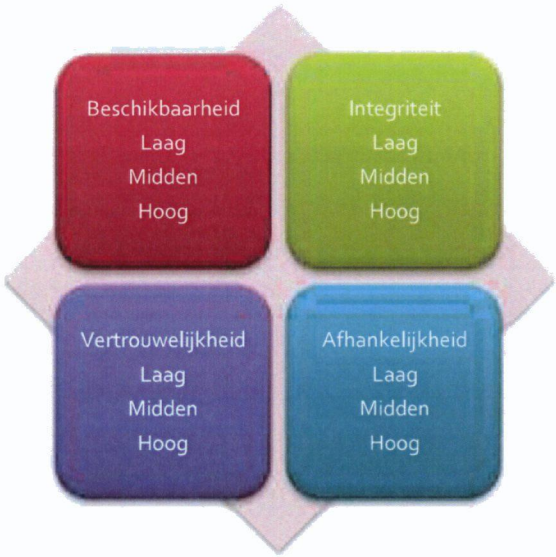
De eisen gelden voor het totaal van het proces en de informatievoorziening. Bijvoorbeeld de inbraakbestendigheid: de tijd dat het iemand kost voor hij informatie bereikt. Het vertragen van de inbraak kan mogelijk worden gemaakt door bewaking, deuren en sloten, het versleutelen van informatie, etc. Per proces en informatietype ontstaat een combinatie van maatregelen om aan de eisen te voldoen.

Proces	Proces belang (MV, OV, O)	Informatie waarde B	Informatie waarde I	Informatie waarde V	Afhankelijkheid systeem (Nood, Nut of Aanvullend)	Beveiligingsniveau
Melding en Poortwachter	MV=3	Hoog=3	Hoog=3	Hoog=3	Nut/Nood	27+2.5=29.5 **HOOG**
Afhandeling Aanvraag	MV=3	Hoog=3	Hoog=3	Midden=2	Nood Voor betaling systeem afhankelijk. Overige niet.	24+3=27 **HOOG**
Begeleiding	MV=3	Midden =2	Midden=2	Hoog=3	Aanvullend/Nut (SRG gegevens)	21+1.5=22.5 **MIDDEN/HOOG**
Mutatie / Beëindiging	MV=3	Hoog=3	Hoog=3	Hoog=3	Nood	27+3=30 **HOOG**
Terugvordering	MV=3	Hoog=3	Hoog=3	Hoog=3	Nood	27+3=30 **HOOG**
Verhaal	MV=3	Hoog=3	Hoog=3	Hoog=3	Nut	27+2=29 **HOOG**
Fraude	MV=3	Hoog=3	Hoog=3	Hoog=3	Nood	27+3=30 **HOOG**
IC	OV=2	Hoog=3	Hoog=3	Hoog=3	Nood	18+3=21 **MIDDEN/HOOG**
VIC	OV=2	Hoog=3	Hoog=3	Hoog=3	Nood	18+3=21 **MIDDEN/HOOG**
Functioneel Applicatiebeheer (bijv. correctie maatregelen)	OV=2	Hoog=3	Hoog=3	Midden=2	Nood	16+3=19 **MIDDEN/HOOG**
Betalingsverkeer	MV=3	Hoog=3	Hoog=3	Hoog=3	Nood	27+3=30 **HOOG**

Vertaal tabel				
Proces belang	Maatschappelijk Vitaal=3	Organisatie Vitaal=2	Ondersteunend=1	
Informatiewaarde Beschikbaarheid	Noodzaak=3	Nut=2	Aanvullend=1	
Informatiewaarde Integriteit (correctheid, volledigheid)	Hoog=3	Midden=2	Laag=1	
Informatiewaarde Vertrouwelijkheid	Hoog=3	Midden=2	Laag=1	
Afhankelijkheid informatie = Informatiewaarde B	Zie informatiewaarde B			
Afhankelijkheid systeem	Noodzaak=3	Nut=2	Aanvullend=1	
Kans	Maandelijks of vaker=4	Jaarlijks= 3	Eens in 10 jaar = 2	Eens in 100 jaar =1
Impact	Ernstig = 3	Gemiddeld = 2	Klein =1	
Verwijtbaar	Ja=1.3	Nee=1		

2.5 Bijstelling niveau

Vanuit de aanpak volgt een niveau van informatiebeveiliging. De proceseigenaar en de informatie eigenaar kunnen van dit niveau afwijken. De afwijking mag hooguit één stap omhoog of omlaag en kan verbijzonderd zijn naar de termen beschikbaarheid, exclusiviteit en integriteit.



2.6 Kwetsbaarheidsanalyse

De eerdere stappen bepaalden het niveau van de treffen maatregelen. De afhankelijkheidsanalyse (2.3) bepaalt mede een prioritering in het veiligstellen van delen van de informatiestroom. De kwetsbaarheid analyse bepaalt welke bedreigingen kunnen optreden in de informatievoorziening. Het identificeert de risico's en bedreigingen. Bij risico's kan gedacht worden aan de toegang, de opslag en het transport van informatie. Op ieder risicopunt zijn bedreigingen te identificeren die de basis vormen voor tegenmaatregelen. Vanzelfsprekend is er een verband met de afhankelijkheidsanalyse. Dit verband zit vooral in de prioritering: eerst analyses van bedreigingen uitvoeren voor de noodzakelijke informatie, vervolgens de bedreigingen analyseren voor de nuttige informatie en tenslotte voor de aanvullende informatie.

Bedreiging	Kans	Impact	Verwijtbaar	Uitkomst	Prioriteit
de organisatie					
▲ TAKEN EN VERANTWOORDELIJKHEDEN (ONVERENIGBAARHEID VAN TAKEN)	3	1	1.33	4	4
▲ BEDRIJFSCULTUUR	4	3	1.33	16	1
▲ BEWUST ONJUIST MENSELIJK HANDELEN	3	3	1.33	12	2
▲ MISDAAD, FRAUDE OF DIEFSTAL OP EIGEN INITIATIEF OF ONDER DRUK VAN DERDEN	2	3	1.33	7,5	4
▲ VANDALISME, BESCHADIGING, VERNIELING OF SABOTAGE	1	1	1.33	1,33	4
▲ FUNCTIEVERANDERING OF –TOEVOEGING	4	3	1.33	16	1
▲ NIET IN ACHT NEMEN VAN VOORSCHRIFTEN	4	3	1.33	16	1

▲ ONGEAUTORISEERDE TOEGANG (KRAKEN OF OMZEILEN TOEGANGSCONTROLE DOOR EIGEN PERSONEEL OF BUITENSTAANDERS)	4	2	1.33	10,66	3
▲ MEELUISTEREN / ONTKENNEN VAN BERICHTOVERDRACHT	3	1	1.33	4	4
▲ ONBEWUST ONJUIST MENSELIJK HANDELEN	4	2	1.33	10,66	3
▲ MENSELIJK FALEN (ONKUNDE, SLORDIGHEID OF STRESS)	4	2	1.33	10,66	3
▲ VERGISSING (BEDIENINGSFOUTEN)	3	1	1.33	4	4
▲ COMPLEXE FOUTGEVOELIGE BEDIENING	3	1	1.33	4	4
▲ ONZORGVULDIG OMGAAN MET WACHTWOORDEN (RAADBAAR, VINDBAAR)	4	3	1.33	16	1
▲ VERLIES OF ZOEKRAKEN VAN GEGEVENS OF GEGEVENSDRAGERS	3	3	1.33	12	2
▲ ONZORGVULDIGE VERNIETIGING VAN GEGEVENS OF GEGEVENSDRAGERS	4	2	1.33	10,66	3
▲ ZIEKTE, DOOD, STAKING	4	3	1.33	16	1
▲ JUISTE HANDELING OP VERKEERD MOMENT (FOUTIEVE, STRIJDIGE PROCEDURES)	4	1	1.33	5,25	4
▲ VAKANTIE, ONTSLAG	4	2/3 (ontslag 3)	1.33	13,33	2
de processen					
▲ ONTWERP, IMPLEMENTATIE, UITVOERING	4	2 (moet blijken bij implentatie)	1.33	10,66	3
▲ ONVOLLEDIGHEID	3	2	1.33	8	3
▲ GEBREK AAN FORMALISATIE, DOCUMENTATIE, CONTROLE, VERANTWOORDING	2	3	1.33	8	3
▲					
de sociale omgeving					
▲ ONGEAUTORISEERDE TOEGANG (KRAKEN OF OMZEILEN TOEGANGSCONTROLE DOOR EIGEN PERSONEEL OF BUITENSTAANDERS),	3	3	1.33	12	2
▲ CRIMINALITEIT/MISDAAD (INBRAAK, DIEFSTAL OF FRAUDE (OP EIGEN INITIATIEF OF ONDER DRUK VAN DERDEN)	4	2	1.33	10,66	3
▲ SOCIAL ENGINEERING	4	3	1.33	16	1
▲ VANDALISME, BESCHADIGING, VERNIELING, SABOTAGE OF VERSPREIDEN VAN VIRUSSEN	3	3	1	9	2
▲ STAKING, DEMONSTATIES, BLOKKADE	1	1	1	1	0

▲ MENSELIJK FALEN (ONKUNDE, SLORDIGHEID OF STRESS)	4	3	1	12	2
▲ VERGISSING (BEDIENINGSFOUTEN)	4	1	1	4	4
▲ COMPLEXE FOUTGEVOELIGE BEDIENING	4	1	1	4	4
▲ ONZORGVULDIG OMGAAN MET WACHTWOORDEN (RAADBAAR, VINDBAAR)	4	1	1	4	4
▲ (NIEUWS)MEDIA	4	3	1.33	16	1
▲ POLITIEK	4	3	1.33	16	1
▲					
de fysieke omgeving					
▲ OMGEVING BEDRIJFSLOCATIE (GEVAARLIJKE OBJECTEN, INFRASTRUCTUUR	2	1	1	2	4
▲ NUTSBEDRIJVEN E.D. (UITVAL VAN STROOM, WATER, TELEFOON, OVERLAST DOOR LEKKAGE, BLUSWATER)	2	2	1	4	4
▲ INFRASTRUCTUUR BEDRIJFSLOCATIE (TOEGANKELIJKHEID PAND, UITVAL VAN LICHT-, KLIMAAT-, SPRINKLERINSTALLATIE)	2	2	1	4	4
▲ NATUURGEWELD (OVERSTROMING, BLIKSEMINSLAG, STORM, AARDBEVING)	1	3	1	3	4
▲ ALGEMEEN GEWELD (RAMPEN, OORLOG, TERRORISME, EXPLOSIES)	1	3	1	3	4
▲ BRAND	1	3	1	3	4
de techniek (de systemen, de applicaties, het netwerk, het rekencentrum)					
▲					
▲ ARCHITECTUUR EN STANDAARDEN	2	1	1	2	4
▲ BEWEZEN TECHNOLOGIE (PROVEN TECHNOLOGY) VERSUS NIEUWSTE TECHNOLOGIE (LEADING EDGE)	2	1	1	2	4
▲ ONTWERP-, FABRICAGE-, CONFIGURATIE-, INSTALLATIE-, IMPLEMENTATIE- OF TOEPASSINGS- OF ONDERHOUDSFOUTEN	4	3	1.33	16	1
▲ SPONTAAN FALENDE TECHNIEK (VERBORGEN GEBREKEN, TECHNISCH FALEN OF MECHANISCHE STORING)	4	1	1.33	5,25	4
▲ AFHANKELIJKHEID VAN EXTERNE OMSTANDIGHEDEN BEHEER & ONDERHOUD VERODUDERING, SLIJTAGE OF ECONOMISCHE LEVENSDUUR	3	1	1.33	4	4
▲ TECHNISCH FALEN DOOR INVLOEDEN VAN BUITEN (SPANNINGSSCHOMMELINGEN OF PIEKSPANNINGEN, ELEKTROSTATISCHE SPANNING, (ELEKTROMAGNETISCHE) STRALING, TEMPERATUUR, VOCHTIGHEID, VUIL, STOF)	2	2	1.33	5,25	4
▲ OVERBELASTING	2	2	1.33	5,25	4

In de bijlage: Afhankelijkheids- en kwetsbaarheidsanalyse, wordt een uitgebreidere beschrijving gegeven van de te volgen stappen voor het uitvoeren van de afhankelijkheidsanalyse en de kwetsbaarheidsanalyse.

2.7 Beveiligingseisen richtlijn

In onderstaande tabel is de situatie m.b.t. de beveiligingseisen uit de verantwoordingsrichtlijn geschetst. Voor iedere richtlijn is kort weergegeven wat de situatie is en eventueel opmerking ter toelichting. De volledige richtlijn is terug te vinden als bijlage bij dit document.

Verantwoordingsrichtlijn beveiligingseisen	Situatie	Opmerkingen
1.1	AANDACHTSPUNT	Met het maken van dit beveiligingsplan en procedures + normenkader wordt hieraan invulling gegeven
1.2	AANDACHTSPUNT	Met het maken van dit beveiligingsplan en procedures + normenkader wordt hieraan invulling gegeven
1.3	AANDACHTSPUNT	Vaststellen in MT staat op de planning
1.4	AANDACHTSPUNT	Bedoeling is deze plannen in de teamoverleggen te gaan bespreken
1.5	AANDACHTSPUNT	Met risicoanalyse wordt dit opgebouwd
2.1	Op orde	Coördinator Procescontrole wordt als functie geborgd in de nieuwe cluster opzet
2.2	AANDACHTSPUNT	Uitwerken van deze rollen en vastleggen in het document beveiligingsprocedures
2.3	AANDACHTSPUNT	Ja, maar formaliseren in beveiligingsplan en beveiligingsprocedures
2.4	AANDACHTSPUNT	Zijn aandachtspunten om mee te nemen in de beveiligingsprocedures
2.5	BKWI	
3.1	BKWI, aandachtspunt	Koppeling GreenValley moet op grond van de gestelde specificaties worden gedaan. Belang is bij beheer om goed versiebeheer uit te voeren.
3.2	BKWI	
3.3	BKWI	Releasenotes geven inzicht in wijzigingen m.b.t. berichtverkeer en dataopbouw
3.4	BKWI	
4.1		Niet bekend wat dit inhoud en of dit van belang is
4.2	n.v.t.	
4.3	n.v.t.	
5.1	AANDACHTSPUNT	Proces niet vastgelegd en er zijn vraagtekens m.b.t. borging
5.2	AANDACHTSPUNT	In principe wel, maar niet vastgelegd
5.3	BKWI	
5.4	Op orde	Monitoring kan nog verbeteren
6.1	AANDACHTSPUNT	Ontbreekt nu
6.2	AANDACHTSPUNT	Ontbreekt nu
6.3	AANDACHTSPUNT	Ontbreekt nu
6.4	AANDACHTSPUNT	Ontbreekt nu
6.5	AANDACHTSPUNT	Ontbreekt nu
7.1	Op orde	Overzicht landschap is helder gedocumenteerd
7.2	Op orde	Licentiebeheer ligt bij functioneel beheer
7.3	BKWI	
7.4	BKWI	

8.1	AANDACHTSPUNT	Nu nog niet, onderdeel van beveiligingsprocedures in plan en Topdesk proces in oprichting
8.2	Op orde	Topdesk
8.3	Op orde	Topdesk
8.4	Op orde	ITIL Info+
8.5	BKWI	
9.1	Op orde	Evaluatie beveiligingsincidenten
9.2	Op orde	
10.1	Op orde	
10.2	Op orde	
10.3	Op orde	
10.4	Op orde	
10.5	Op orde	
10.6	Op orde	
11.1	AANDACHTSPUNT	Testen onderbelicht Acceptatie door lijnorganisatie gebeurt nu onvoldoende
11.2	AANDACHTSPUNT	Testen onderbelicht Acceptatie door lijnorganisatie gebeurt nu onvoldoende
11.3	AANDACHTSPUNT	Testen onderbelicht Acceptatie door lijnorganisatie gebeurt nu onvoldoende
11.4	AANDACHTSPUNT	Nu livedata in de testomgeving
11.5	BKWI	
11.6	BKWI	
12.1	AANDACHTSPUNT	Aandachtsgebied voor netwerkbeheer
12.2	BKWI	
12.3	AANDACHTSPUNT	Herstelproces beschrijven. GEMNET ontsluiting Overige aspecten zijn op orde, alleen procesmatig
12.4	BKWI	
13.1	AANDACHTSPUNT	Tijdig wijzigen en intrekken is aandachtspunt, ook bij Gws4all
13.2	Op orde	Klopt, na BKWI audit is dit opgeruimd.
13.3	Op orde	
13.4	Op orde	Standaard functionaliteit van SUWInet
13.5	Op orde	Na audit BKWI is dit ingezet, 2 geautoriseerden Bert H. draait script voor controle inlog Gws4all
13.6	Op orde	Gws4all logt alles, gebeurt
13.7	Op orde	Gws4all is SSO
13.8	Op orde	
13.9	Op orde	
13.10	BKWI	
14.1	Op orde	
14.2	Op orde	
15.1	AANDACHTSPUNT	Belangrijk voor SUWInet koppeling GreenValley
15.2	AANDACHTSPUNT	Belangrijk voor SUWInet koppeling GreenValley
15.3	AANDACHTSPUNT	Belangrijk voor SUWInet koppeling GreenValley
15.4	AANDACHTSPUNT	Belangrijk voor SUWInet koppeling GreenValley

15.5	AANDACHTSPUNT	Belangrijk voor SUWInet koppeling GreenValley
16.1	AANDACHTSPUNT	Belangrijk voor SUWInet koppeling GreenValley
16.2	AANDACHTSPUNT	Belangrijk voor SUWInet koppeling GreenValley
16.3	AANDACHTSPUNT	Belangrijk voor SUWInet koppeling GreenValley
16.4	AANDACHTSPUNT	Belangrijk voor SUWInet koppeling GreenValley
16.5	AANDACHTSPUNT	Belangrijk voor SUWInet koppeling GreenValley
17.1	AANDACHTSPUNT	DKD software (AANDACHTSPUNT)
17.2	AANDACHTSPUNT	DKD software (AANDACHTSPUNT)
17.3	AANDACHTSPUNT	DKD software (AANDACHTSPUNT)
17.4	AANDACHTSPUNT	DKD software (AANDACHTSPUNT)
17.5	AANDACHTSPUNT	DKD software (AANDACHTSPUNT)
18.1	N.V.T.	
18.2	N.V.T.	
18.3	N.V.T.	
18.4	N.V.T.	
18.5	N.V.T.	
18.6	N.V.T.	
19.1	Op orde	
19.2	Op orde	
19.3	Op orde	
19.4	Op orde	
19.5	Op orde	
19.6	Op orde	
19.7	Op orde	
20.1	AANDACHTSPUNT	Security patches en OS hardening issue
20.2	Op orde	
20.3	Op orde	
20.4	Op orde	
20.5	Op orde	
20.6	Op orde	
20.7	BKWI	
21.1	Op orde	
21.2	Op orde	
21.3	Op orde	
21.4	Op orde	
21.5	Op orde	
21.6	Op orde	
21.7	Op orde	
21.8	Op orde	
22.1	Op orde	
22.2	Op orde	
22.3	Op orde	
22.4	Op orde	
22.5	Op orde	
22.6	Op orde	
22.7	Op orde	

Beveiligingsadvies

Advies en afweging

In dit hoofdstuk is een informatiebeveiligingsadvies geformuleerd, de gemaakte keuzes en de argumentatie worden tevens aangegeven. Bij de afweging zijn kostenconsequenties meegenomen.

3.1 Analyse

In het advies aan de proces- en informatie-eigenaar over de informatiebeveiliging worden de adviezen van de Information Security Manager, de coördinator AO/IC en andere betrokken specialisten meegenomen. Op basis van de afhankelijkheid- en kwetsbaarheidsanalyse, kosten van maatregelen en het advies maken de proces- en informatie-eigenaar een afweging tussen de kosten en de baten. Dus van onbewust risico lopen naar bewust risico nemen. Het besluit wordt vastgelegd, aan het college voorgelegd en teruggekoppeld aan de Information Security Manager.

Kijkend naar de risicoanalyse resultaten zijn de volgende aandachtpunten geïdentificeerd;

PROCESSEN

Van de in paragraaf 2.4 in kaart gebrachte processen zijn bijna alle processen beoordeeld met een hoog niveau op de verschillende beveiligingspijlers. Van de klantprocessen is alleen het proces 'begeleiding' lichter beoordeeld. De overige processen hebben allen een indicatie HOOG. De interne processen worden ook iets lichter beoordeeld, het gaat dan om de IC, VIC en beheer processen.

BEDREIGINGEN

Bij de kwetsbaarheidsanalyse is gekeken naar zaken die een negatieve invloed kunnen hebben op een van de beveiligingscriteria voor de processen bij het cluster Sociale Dienstverlening. Daarbij is gekeken naar de kans dat dit zich voordoet en de impact die het in dat geval heeft. De risico's die een hoge kans van voordoen en een zware impact toegekend hebben gekregen scoren 8 punten of meer. Deze hebben een prioriteit 1 of 2 gekregen. Die risico's zijn hieronder weergegeven;

- **Bedrijfscultuur**
  Beveiligingsbewustzijn en aandacht voor informatiebeveiliging zijn niet heel hoog. Dit vormt een reële dreiging.
- **Functieverandering of –toevoeging**
  Binnen het cluster is veel verandering gaande, dit vormt mogelijk een risico voor beveiligingsprocessen, omdat niet alles voor iedereen duidelijk is.
- **Onzorgvuldig omgaan met wachtwoorden (raadbaar, vindbaar)**
  Dit kan als onderdeel van beveiligingsbewustzijn en veilig handelen worden beschouwd.
- **Niet beschikbaar zijn van cruciaal personeel**
  Continuïteit van bepaalde processen kan sterk afhankelijk zijn van specifieke medewerkers.
- **Social engineering**
  Ook wel de kunst van het misleiden genoemd. Het manipuleren van personen om via die manier informatie los te krijgen, die normaal gesproken niet voor diegene bedoeld is.
- **(Nieuws)media**
  Hierin schuilt met name het risico van imagoschade.
- **Politiek**
  Politieke druk of negatieve aandacht rondom beveiligingssituatie, governance en incidenten.
- **Configuratie-, installatie-, implementatie- of toepassings- of onderhoudsfouten**
  Hierin liggen verscheidene risico's die met name op technisch vlak voor verstoring kunnen zorgen.
- **Ongeautoriseerde toegang (kraken of omzeilen toegangscontrole door eigen personeel of buitenstaanders)**
  Het risico dat iemand anders dan een geautoriseerde medewerker, toegang heeft tot de gegevens. Of dat een medewerker gebruik maakt van het systeem op naam van een andere medewerker.
- **Onbewust menselijk falen**
  Het onbewust handelen van medewerkers met een beveiligingsrisico, incident of verstoring als gevolg.
- **Onzorgvuldige vernietiging van gegevens of gegevensdragers**
  Het niet zorgvuldig vernietigen kan leiden tot informatielekkage en onbedoelde openbaarmaking van persoonsgegevens of andere gevoelige informatie. Ook kan hier sprake zijn van niet gevoelige informatie, maar leidt de situatie dat de organisatie slordig omgaat met informatie toch tot negatieve media aandacht en imagoschade.

- **Proces ontwerp, implementatie en uitvoering**
  Veel veranderende processen binnen het cluster kunnen in het begin tot verwarring leiden, daarnaast zal in de praktijk moeten blijken of de processen helemaal goed functioneren, hierin zit ook een risico.
- **Gebrek aan formalisatie, documentatie, controle en verantwoording**
  Veel zaken gebeuren wel, maar zijn niet formeel vastgelegd en zwart op wit terug te vinden. Bij controle en de noodzaak om hierover te verantwoorden kan dit problemen opleveren.
- **Criminaliteit/misdaad (inbraak, diefstal of fraude (op eigen initiatief of onder druk van derden)**
  Diefstal is een reeel risico ook in de gemeentelijke kantoorruimten. Fraude kan mogelijk plaatsvinden en omdat de impact hiervan heel groot kan zijn, heeft deze dreiging hoog gescored.

BEVEILIGINGSRICHTLIJNEN

Kijkend naar de beveiligingsrichtlijnen vanuit SUWI, zijn de volgende opmerkingen gemaakt;

Aan de richtlijnen m.b.t. beleid, plannen en proces wordt met het nieuwe beveiligingsbeleid en o.a. dit beveiligingsplan invulling gegeven.

Capaciteitsbeheer is een aandachtsgebied om zowel technisch als organisatorisch goed te borgen. Het gaat dan om beschikbaarheid van systeemcapaciteit, maar ook valt te denken aan de capaciteit van cruciale kennis en kunde.

Continuïteitsbeheer is een aandachtspunt. Momenteel is er m.b.t. voorzieningen voor continuïteit t.b.v. de Sociale Dienstverlening niet veel geregeld. De nieuwe systeemomgeving wordt gebackuped en er zijn vereenvoudigde en versnelde mogelijkheden om de systemen technisch te herstellen. Echter officiële continuïteitsplannen, uitwijk of calamiteitenprocessen t.b.v. serieuze verstoring van de bedrijfsprocessen bij het cluster SDV zijn niet aanwezig.

Incidentmelding voor beveiligingsincidenten is nu nog niet geformaliseerd, vastgelegd en bekend. De bedoeling is dat hiervoor een organisatie brede procedure beschikbaar komt vanuit het beveiligingsbeleid. Hier hoeft door het cluster geen eigen invulling aan gegeven te worden.

Testen en Acceptatie worden maar beperkt uitgevoerd en niet op de juiste en correcte wijze. Deze processen zouden beter moeten worden beschreven, uitgevoerd en geborgd.

Autorisatiebeheer is een blijvend aandachtspunt. Het actueel houden en toezien op autorisatie gebruik is een proces wat continu scherp moet blijven.

XML koppelingen SuwiNET staan voor komend jaar op de planning om uitgevoerd te worden. Het gaat daarbij om vulling van SUWI-gegevens in een e-formulier. Dit kan en mag, maar belangrijk is dat daarbij de beveiligingsvereisten, ontwerpprincipes en architectuuruitgangspunten uit de richtlijn worden gehandhaafd. Hiermee dient dus bij het ontwerpproces direct rekening gehouden te worden.

De DKD server is geïdentificeerd als een beveiligingsrisico. Uit analyse van de technische omgeving blijkt deze server onvoldoende gepatched te zijn en beschikt daardoor over sterk verouderde software onderdelen. Daardoor vormt dit systeem een ongewenst beveiligingsrisico. Na mislukte pogingen om de serverlekken te dichten, is reeds contact opgenomen met leverancier Centric om dit probleem aanhangig te maken, INFO+ kan dit niet oplossen zonder leverancier Centric, aangezien de software specifiek is gemaakt en hierdoor niet zomaar gepatched kan worden.

SUWInet is een webapplicatie en kan daardoor in principe ook via de virtuele desktop omgeving (Citrix) benaderd worden. Dit betekent dat medewerkers eventueel ook de mogelijkheid hebben om de SUWInet omgeving elders te raadplegen, buiten de kantoor omgeving van de gemeente. Aan het MT wordt de vraag voorgelegd of zij dit wenselijk acht en hoe zij hiermee om willen gaan.

3.2 Advies

Kijkend naar de dreigingen en de situatie t.o.v. de beveiligingsrichtlijnen gelden de volgende adviezen;

1. Besteed aandacht aan beveiligingsbewustzijn, de meeste van de dreigingen hebben te maken met de factor 'mens' in het proces van beveiliging. Vanuit het nieuwe organisatie brede beveiligingsbeleid zal komend jaar aandacht zijn voor beveiligingsbewustzijn, presentaties aan de verschillende clusters, management commitment, etc. Bewustzijn geldt voor zowel de uitvoerende medewerkers als voor het management.

   Verantwoordelijkheid : cluster Sociale Dienstverlening en organisatie breed informatiebeveiliging beleid

2. Besteed aandacht aan borging van kennis en kunde en cruciaal personeel. Belangrijke processen zijn in veel gevallen van 'sleutelfiguren' afhankelijk voor hun goed functioneren. Het is belangrijk dit goed te borgen, zodat voor deze processen de continuïteit is geborgd.

   Verantwoordelijkheid : cluster Sociale Dienstverlening

3. Denk na over de continuïteitsbehoefte van het cluster en welke middelen, medewerkers, processen hiervoor nodig zijn en ga dit vastleggen in een continuïteitsplan. Voorstel is om in een 'brainstormsessie' met het MT een beeld te vormen van de continuïteitsbehoefte bij het cluster en hierop vervolgens een plan maken om in deze behoefte te voorzien. Daarnaast moet er een draaiboek worden gemaakt, waarin staat uitgewerkt welke processen ingang treden bij een grote calamiteit, wie waarvoor verantwoordelijk is, wat de gemaakte afspraken zijn, etc.

   Verantwoordelijkheid : cluster Sociale Dienstverlening

4. Besteed aandacht aan het vastleggen van een test- en acceptatieproces bij software wijzigingen. Er wordt nu wel getest, maar formele acceptatie vind in de praktijk niet tot nauwelijks plaats. Het is belangrijk om dit proces goed te beschrijven en er op toe te zien dat deze in de praktijk ook worden gevolgd.

   Verantwoordelijkheid : cluster Sociale Dienstverlening

5. Autorisatiebeheer van nieuwe medewerkers en het afvoeren van medewerkers die niet meer werkzaam zijn dient uiterst zorgvuldig te gebeuren, het belang van dit proces moet absoluut niet onderschat worden. Dit proces wordt uitgevoerd door de functioneel beheerder(s), maar staat in de uitvoering van dit proces ook vaak onder druk. Het is belangrijk dat het management ook het belang van dit proces inziet en aan een goede uitvoering waarde hecht. Er wordt momenteel gewerkt aan het project in-, door- en uitstroom. Hierin wordt geprobeerd de instroom van nieuwe medewerkers en de uitstroom van medewerkers, administratief goed maar ook snel te realiseren. Bedoeling is daarmee het proces rondom het verkrijgen van autorisaties van medewerkers en het intrekken daarvan zodra ze uitdienst treden, goed georganiseerd te krijgen, aangezien dit nu organisatie breed en bekend probleem punt is. Aanhaking op dit proces kan voor cluster Sociale Dienstverlening een verbetering op het gebied van autorisatiebeheer bewerkstelligen.

   Verantwoordelijkheid : cluster Sociale Dienstverlening

6. Benadruk en draag zorg voor beveiliging in het ontwikkelen van e-formulieren of andere digitale dienstverleningstoepassingen m.b.t. SUWInet. Daar waar SUWI-gegevens worden gebruikt, dient aan de verantwoordingsrichtlijnen (zie bijlage 2) te worden voldaan. Ga na vanuit het project of de eisen vanuit de verantwoordingsrichtlijn zijn meegenomen en of hieraan wordt voldaan.

   Verantwoordelijkheid : cluster Sociale Dienstverlening en team Innovatie, Info+

a. Denk na over de nieuwe risico's die het flexwerken en 'Nieuwe Werken' mogelijk met zich meebrengen en stel duidelijk richtlijnen op voor medewerkers over omgang met informatie en toegang tot systemen voor de flexwerkplek en buiten de kantooromgeving van de organisatie. Het is toegestaan om SUWInet ook buiten de kantooromgeving te gebruiken, bij bijvoorbeeld telewerken. Het is belangrijk dat het MT echter goed nadenkt over de andere risico's die hierbij komen kijken. Bij het werken in de kantooromgeving van de gemeente Haarlemmermeer worden veel beveiligingsvereisten gefaciliteerd vanuit de organisatie. Wanneer medewerkers hun werkzaamheden buiten de kantooromgeving gaan gebruiken is dit niet langer het geval. Hier dient rekening mee gehouden te worden en met adequate maatregelen om ingespeeld te worden.

Verantwoordelijkheid : cluster Sociale Dienstverlening en organisatie breed informatiebeveiliging beleid

3.2 Kostenplaatje

In het kostenplaatje wordt een vergelijking gemaakt tussen de éénmalige en terugkerende kosten en de opbrengsten. Om met deze laatste te beginnen: de opbrengsten worden zoveel mogelijk uitgedrukt in objectieve cijfers. Een deel van de opbrengsten is niet te objectiveren, bijvoorbeeld als het imago betreft. De kosten voor het nemen van de maatregelen zijn wel te objectiveren. Iedere maatregel vergt een investering en jaarlijks terugkerende kosten. Uiteindelijk ontstaat een kostenoverzicht die door de manager in de afweging kan worden meegenomen.

De kosten voor de hierboven genoemde maatregelen zijn vooral terug te brengen op interne kosten voor het beschrijven van procedures en het vastleggen daarvan. De inzet die daarmee gemoeid gaat, is veelal onderdeel van de kerntaken van betreffende medewerker. Van extra kosten is dan geen sprake.

Aanbevolen wordt om eventuele workshops/presentatie in de teamoverleggen plaats te laten vinden. Hieraan kan door de ISM/FG en de Coördinator Procescontrole invulling worden gegeven. Ook hier geldt dat de inzet die daarmee gemoeid gaat, onderdeel is van de kerntaken van betreffende medewerkers. De inzet van medewerkers en teammanagers geschiedt zoveel als mogelijk binnen de reeds ingeplande overleggen en brengt ook geen extra kosten met zich mee. Wanneer dit gewenst is kan hier in overleg met de ISM/FG ook gekozen worden voor verdere invulling m.b.v. een externe partij, om verdieping te geven aan de workshops.

3.3 Afwegingen

De gegeven adviezen in 3.1 zijn bedoeld om de organisatie van cluster Sociale Dienstverlening in lijn te brengen met de Verantwoordingsrichtlijn Gezamenlijk Elektronische Voorzieningen SUWI (GeVS). Vanuit deze richtlijn worden de eisen gesteld waarop de risicoanalyse en de adviezen gebaseerd zijn. Belangrijk is om te weten dat er momenteel gewerkt wordt aan een vernieuwde versie van deze verantwoordingsrichtlijn. In de nieuwe versie zal inhoudelijk niet veel veranderen. Belangrijke verandering is echter de komst van een verplichtte EDP-audit. Deze zal waarschijnlijk jaarlijks zijn en legt een aanzienlijk druk op de organisatie om aan de beveiligingseisen van de Verantwoordingsrichtlijn te voldoen. Het is daarom belangrijk te beseffen dat de nu genomen acties de organisatie alvast voorbereiden op het voldoen aan de verantwoordingsrichtlijn en dat daarmee de mogelijk toekomstige auditlasten alvast worden verlicht.

Voor de gegeven adviezen is het de keuze van het MT Sociale Dienstverlening, welke vervolgacties hierin te nemen. In de adviezen is veelal aangegeven wat een aanbevolen actie is. Maar het MT kan beslissen om niet alle voorgestelde acties ook daadwerkelijk uit te gaan voeren. Dit heeft te maken met de risicoafweging die altijd bij het verantwoordelijk lijnmanagement ligt. Er kunnen goede redenen zijn om bepaalde acties (nu) niet uit te gaan voeren. Eventuele risico's kunnen acceptabel worden geacht, of de maatregel kan worden beoordeeld als te kostbaar of met een te hoge impact. In dat geval accepteert het MT het eventuele restrisico als acceptabel en vindt er geen maatregel plaats.

De gegeven adviezen lijden tot maatregelen voor het implementatievoorstel in het volgende hoofdstuk. Aan het MT de keuze om hierin prioritering aan te brengen en eventuele maatregelen toe te voegen of eventueel met onderbouwing niet tot uitvoering te brengen.

Implementatieplan

Implementatieplan

De maatregelen die op basis van de afwegingen en het gekozen beveiligingsniveau zijn genomen, moeten worden geïmplementeerd, onderhouden en gecontroleerd. Beschreven wordt welk organisatieonderdeel verantwoordelijk is voor het nemen en controleren van betreffende maatregelen en wanneer deze zullen plaats hebben.

1. Advies: Verhoging beveiligingsbewustzijn

Maatregel:

- Uitrol gemeentebrede Bewustwordingscampagne Informatiebeveiliging (ISM, 2e halfjaar 2013).
- Bespreking Beveiligingsplan, Beveiligingsprocedures en specifieke maatregelen SDV in het MT SDV (Coördinator AO/IC en ISM, 16 mei 2013)
- Bespreking Beveiligingsprocedures SDV in de diverse teamoverleggen van Cluster SDV (Coördinator AO/IC en ISM en betreffende teammanagers, 3e kwartaal 2013 en daarna minimaal 1 maal per jaar).

2. Advies: Borging kennis en kunde cruciaal personeel

Maatregel:

- Met de reorganisatie die de cluster Sociale Dienstverlening doorvoert per september 2013, is deze kennis en kunde van personeel geborgd.

3. Advies: Vaststellen en borging continuïteitsplan

Maatregel:

- Brainstormsessie over continuïteitbehoefte SDV (Coördinator Procescontrole en inhoudsdeskundigen SDV o.l.v. ISM, 4e kwartaal 2013)
- Opstellen continuïteitsplan SDV in overleg met ondersteunende clusters (Coördinator Procescontrole i.o.m. ISM en clusters HRM en FM, 4e kwartaal 2013)
- Vaststellen continuïteitsplan SDV (MT SDV, 4e kwartaal 2013)
- Afspraken maken met ondersteunende clusters o.b.v. continuïteitsplan SDV (Coördinator Procescontrole, 4e kwartaal 2013)

4. Advies: Vaststellen en borging test- en acceptatieproces softwarewijzigingen

Maatregel:

- Opstellen MT-acceptatievoorstel n.a.v. testfase project Werkprocessen , of eventueel andere van toepassing zijnde softwarewijzigingen tot september 2013 (Projectleider(s) Werkprocessen en AO/IC i.o.m. projectmedewerkers, in juni 2013).
- Acceptatie n.a.v. testfase project Werkprocessen (MT, juni/juli 2013)
- Opstellen MT-acceptatievoorstel n.a.v. eventueel andere van toepassing zijnde softwarewijzigingen als versiewisselingen GWS4all tot september 2013 (Onder verantwoordelijkheid van Teammanager Kwaliteit / Informatievoorziening en Procescontrole)
- Opstellen procedure voor impactanalyse, testen en accepteren softwarewijzigingen, waarbij sprake is van een vast testteam van superusers (Senior Functioneel Applicatiebeheer / Financiële Kwaliteitsbewaking , na plaatsing, uiterlijk 4e kwartaal 2013).
- Vaststellen test- en acceptatieprocedure (MT SDV, 4e kwartaal 2013).

5. Advies: Borging autorisatiebeheer

Maatregel:

- Aanhaking SDV bij project in-, door- en uitstroom voor opstellen autorisatieprocedure (Coördinator Procescontrole, Applicatiebeheerder en HRM-adviseur SDV i.o.m. Innovatiefabiek, derde kwartaal 2013).
- Implementatie project in-, door- en uitstroom (Innovatiefabriek en HRM-adviseurs, derde of vierde kwartaal 2013).

6. Advies: Borging eisen verantwoordingsrichtlijn bij dienstverleningsontwikkelingen

Maatregel:

- Tweede check SDV-meldingsformulier bij Innovatiefabriek aan de eisen uit de verantwoordingsrichtlijn (Coördinator AO/IC, mei 2013)
- Borging eisen verantwoordingsrichtlijn bij andere dienstverleningsontwikkelingen als bijvoorbeeld proeftuinen Programma Sociaal Domein (Coördinator Procescontrole en Applicatiebeheerders SDV i.o.m. Informatiemanager Info+ M. van Lith en projectleiders PSD, afstemming gestart per 2e kwartaal 2013).

7. Advies: Vaststellen risico's en beheersmaatregelen flexwerken / het "Nieuwe Werken"

Maatregel:

- Uitrol gemeentebrede Bewustwordingscampagne Informatiebeveiliging met aandacht voor Flexwerken en "Het Nieuwe Werken" (ISM, 2e halfjaar 2013).
- Opstellen richtlijnen SDV m.b.t. flexwerken en 'Het Nieuwe Werken' bij SDV voor Projectleider Flexwerken SDV (ISM en Coördinator AO/IC, mei 2013)
- Vaststelling van deze richtlijnen SDV als onderdeel van de Beveiligingsprocedures SDV (MT SDV, juni 2013).

8. Advies: N.a.v. kwetsbaarheidsanalyse beheersing technisch risico DKD-server

Maatregel:

- Actie ondernemen richting leverancier Centric voor maatregelen DKD-server (ISM i.s.m. overige medewerkers Info+, 2e halfjaar 2013).

9. Advies: N.a.v. kwetsbaarheidsanalyse borging capaciteitsbeheer van de omgeving

Maatregel:

- Structurele afspraken borgen binnen Cluster Info+ m.b.t. capaciteitsbeheer van de omgeving t.b.v. borging van goede functionering van de systemen die voor SDV van belang zijn (ISM met MT van Info+, 2e halfjaar 2013).
- Indien nodig: Afstemming van deze afspraken tussen MT SDV en MT Info+ (Teammanager Bedrijfsbureau en betreffende Teammanager binnen Info+, indien nodig 2e halfjaar 2013)

Control

Instrumenten voor controle

De toegepaste methode van control is om via workshops een risicoanalyse uit te voeren waarmee op alle inhoudelijke onderdelen en afweging wordt maakt voor het beveiligingsplan. Een stuk zelfevaluatie, om inzicht te krijgen in de huidige beveiligingsstatus, welke maatregelen zijn er al of juist niet en in hoeverre zijn maatregelen effectief, etc. wordt meegenomen in de workshop. Jaarlijks zal de stand van zaken van het beveiligingsplan moeten worden gecontroleerd, om een nulmeting te verkrijgen als startpunt voor verbeteringen, om ingezette verbeteringen te kunnen monitoren en om risicoanalyses uit te kunnen voeren. De risicoanalyse workshop zal dan ook ieder jaar worden uitgevoerd en functioneert daarmee als evaluatie-instrument en gelijktijdig als risicoanalyse als input voor het nieuwe beveiligingsplan. Zodoende wordt het proces van beveiligingsmanagement cyclisch ingeregeld. Het proces zal ook een jaarlijkse beveiligingsrapportage opleveren die inzicht geeft in hoeverre de gestelde doelen ook zijn gehaald en hoe effectief de genomen maatregelen zijn.

5.1 Workshopmethodiek

Om het beveiligingsplan gebaseerd op de risicoanalyses op te stellen, is een workshopmethodiek de meest aangewezen weg. In de hierna beschreven workshop komen in drie sessies alle tien stappen van de afhankelijkheid- en kwetsbaarheidanalyse aan bod (zie Bijlage 2: Afhankelijksheids- en kwetsbaarheidsanalyse). De workshopmethodiek zal door de Information Security Manager bij de gemeente worden begeleid. Het is de bedoeling dat bij deze workshop zowel de verantwoordelijke managers (proceseigenaar en informatie-eigenaar) als de uitvoerende organisaties aanwezig zijn. Op die manier draagt het bij aan zaken als bewustwording, onderling begrip, gevoel voor elkaars belangen en het nemen van afgewogen beslissing over te accepteren en op te lossen risico's. In de workshopmethodiek worden drie sessies gevolgd. Bij iedere sessie is het belangrijk dat steeds dezelfde groep deelnemers aanwezig is. Verloop in de deelnemers betekent telkens herhalen van de conclusies en de onderbouwing en zal eindigen in een minder (gedragen) resultaat.

De deelnemers van de workshop zijn het verantwoordelijke management en de uitvoerende afdelingen van het werkproces enerzijds en anderzijds de facilitaire afdelingen. Deze zijn aangevuld met de beveiligingsspecialisten en verantwoordelijke(n). Dit komt neer op de volgende deelnemers:

1. proceseigenaar of diens plaatsvervanger,
2. teamleiders/coördinatoren van het proces,
3. verantwoordelijke facilitaire afdeling(en) zoals ICT en gebouwen,
4. Information Security Manager / procesbegeleider

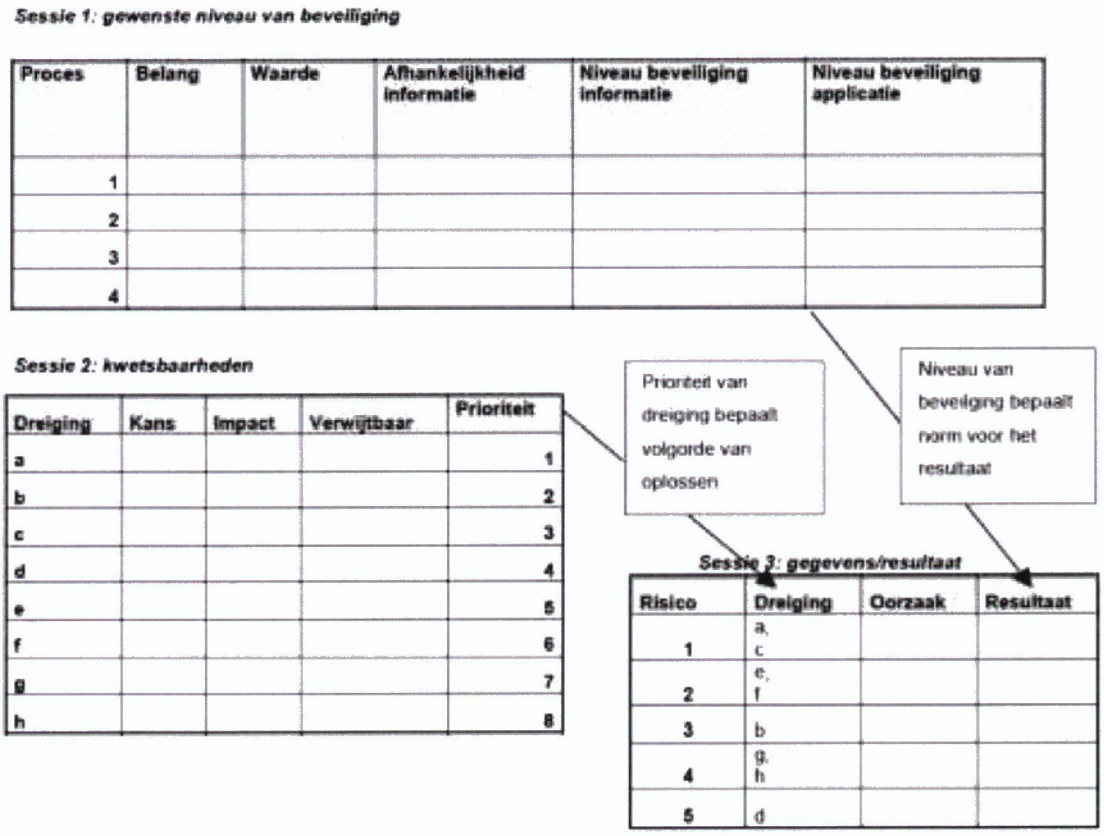
5. Functioneel applicatiebeheerders

Sessie 1: Hierin wordt het gewenste niveau van beveiliging bepaald. Dit gebeurt op basis van het belang van het proces, de waarde van de informatie en de afhankelijkheid van de informatie en de (geautomatiseerde) ondersteuning. Hierbij kan gebruik gemaakt worden van Bijlage 1: Handvat voor indelen van processen en informatie.

Sessie 2: Hierin wordt de kwetsbaarheid en de specifieke bedreigingen (zie Hoofdstuk 3: Bedreigingen) geïnventariseerd voor de behandelde processen uit sessie 1. Generieke dreigingen die uit standaardlijsten zijn af te leiden hebben geen prioriteit in de workshop. Deze worden vanuit deskundigheid aangevuld.

Sessie 3: Deze sessie is gebaseerd op de uitkomsten uit sessie 1 en 2. Het resultaat van sessie 3 is een overzicht van dreigingen gekoppeld aan het gewenste niveau van beveiliging en de afweging tussen oplossen of accepteren van risico's inclusief een oplossingsrichting.

In de volgende afbeelding zijn de sessies symbolisch weergegeven, inclusief hun samenhang.



5.2 Aanpak

U geeft een voorzet voor de wijze waarop de beveiligingsorganisatie haar werk aanpakt en controleerbaar maakt. Hierin specificeert u onder andere de wijze van verantwoording, planning en het vaststellen van beleidsprioriteiten. U borgt hiermee dat de beveiligingsorganisatie onder bestuurlijke controle blijft, maar toch een stuk vrijheid krijgt in haar onafhankelijke advisering.

Speerpunten

Ieder jaar zal in overleg met de Information Security Manager een set speerpunten voor informatiebeveiliging worden bepaald, waaraan extra aandacht wordt geschonken. Hiermee wordt beoogd de inzet van de beperkte capaciteit zo goed als mogelijk in te zetten. De speerpunten zijn enerzijds gebaseerd op de actualiteit en anderzijds op de doorgaande lijn van informatiebeveiliging. Bij het vaststellen van speerpunten moeten keuzes gemaakt worden.

Uitvoeringsplannen
Ieder jaar stelt de cluster Sociale Dienstverlening i.s.m. de Information Security Manager een uitvoeringsplan op waarin onder andere de speerpunten voor volgend jaar staan beschreven.

Communicatie
Bewustwording is een continue activiteit van informatiebeveiliging. Om de maatregelen voor beveiliging effectief te laten zijn, moeten deze door de organisatie geaccepteerd worden. Meer bewustwording zal ook resulteren in het melden van mogelijke problemen. Bewustwording is een belangrijk aspect binnen informatiebeveiliging. Alleen als de medewerkers weten hoe ze met informatie om moeten gaan en waar hun verantwoordelijkheid ligt, hebben maatregelen blijvend effect. Om dit te bereiken, moeten de medewerkers weten wat van hun verwacht wordt, hoe dat gecontroleerd wordt en welke sancties er bestaan.

Iedere medewerker (intern en extern) tekent een integriteits- of geheimhoudingsverklaring waar in staat wat er verstaan wordt onder zorgvuldig omgaan met informatie. Voor het bieden van het handvat aan de medewerkers gelden de 'Tien geboden' voor het omgaan met informatie:

1. Gebruik informatie niet om anderen te hinderen of te schaden.
2. Weet of de informatie die je bezit van belang is voor derden (en geef deze informatie niet
3. ongeautoriseerd uit handen).
4. Gebruik informatie als hulpmiddel bij het uitvoeren van je taak.
5. Vraag alleen informatie op voor zover die nodig is voor je taak.
6. Verzamel en gebruik informatie op een rechtmatige manier.
7. Wees je bewust van de risico's van het uitlekken van informatie.
8. Accepteer de verantwoordelijkheid voor de manier waarop je met informatie omgaat.
9. Leef de reglementen voor de omgang met informatie na.
10. Neem kennis van het gemeentelijke informatiebeveiligingsbeleid.
11. Gebruik informatie in overleg en met respect.

Voortgang en verantwoording
Het cluster rapporteert de voortgang en legt verantwoording af. Zo wordt snel inzichtelijk wat de voortgang is en waar eventuele problemen ontstaan. In de rapportages worden deze problemen toegelicht.

Bijlagen

Bijlage: Afhankelijkheids- en Kwetsbaarheidanalyse

In deze bijlage gaan wij in op de uitvoering van een afhankelijkheids- en kwetsbaarheidanalyse. Stap voor stap geven wij aan hoe u een dergelijke analyse moet aanpakken. De kwetsbaarheidanalyse kunt u pas doen als u de afhankelijkheidsanalyse hebt voltooid.

Afhankelijkheidsanalyse

Het resultaat van de Afhankelijkheidsanalyse is inzicht in de mate waarin de bedrijfsprocessen afhankelijk zijn van het adequaat functioneren van het informatiesysteem. Ook vloeit uit deze analyse een set betrouwbaarheidseisen voort die aan het informatiesysteem worden gesteld. Het uitvoeren van de Afhankelijkheidsanalyse vindt plaats met behulp van verschillende stappen die hier worden toegelicht.

Stap 1: Organisatiecheck
De organisatiecheck is een goed middel om gevoel voor de organisatie te krijgen. Voor het uitvoeren van deze stap wordt gebruik gemaakt van de organisatiedocumenten.

Stap 2: Benoemen van de processen
Voor het realiseren van de doelstellingen van de organisatie moeten de bedrijfsprocessen goed functioneren. Ieder proces wordt geclassificeerd naar prioriteit. De volgende classificaties worden gebruikt: maatschappelijk vitaal, bedrijfsvitaal en ondersteunend. Deze stap vindt plaats aan de hand van procesmodellen.

Stap 3: Stellen van eisen aan de processen
Per bedrijfsproces wordt aangegeven welk betrouwbaarheidscriterium (beschikbaarheid, exclusiviteit en integriteit) belangrijk is. Aan het betrouwbaarheidscriterium wordt een classificatie gegeven en zowel het criterium als de classificatie worden beargumenteerd.

Stap 4: Benoemen van de informatiesystemen en relateren aan processen
Er wordt een opsomming gegeven van de informatie(deel)systemen die de processen ondersteunen. Het al dan niet geautomatiseerd zijn van een informatiesysteem is hier niet aan de orde. Het maakt ook niet uit of een informatiesysteem operationeel of nog in ontwikkeling is. De informatie(deel)systemen worden gekoppeld aan de bedrijfsprocessen. De koppeling en de mate van belang worden via een codering (Vitaal, Nuttig, Ondersteunend, Geen belang) aangegeven.

Stap 5: Relateren informatiesystemen aan (IT-)diensten
In deze stap van de Afhankelijkheidsanalyse wordt per informatiesysteem(functie) aangegeven welke (IT-)dienst of verantwoordelijkheidsgebied belangrijk is voor het functioneren van het systeem.

Stap 6: Stellen van betrouwbaarheidseisen
Per informatiesysteem en betrouwbaarheidscriterium wordt het belang aangegeven. Deze classificatie kent vier mogelijkheden: Essentieel, Belangrijk, Wenselijk en Geen criterium. Bij classificatievermeldingen kan de uitkomst triviaal zijn, bij discussiepunten kan een argumentatie worden gegeven.

Het uitvoeren van de stappen 3 t/m 6 vindt plaats door het afnemen van interviews bij management en medewerkers of workshops.

Kwetsbaarheidsanalyse

Het resultaat van de Afhankelijkheidsanalyse en de vastgestelde kaders in de beleidsuitgangspunten informatiebeveiliging vormen de basis voor het uitvoeren van de Kwetsbaarheidsanalyse. Het resultaat van de Kwetsbaarheidanalyse is een pakket van te nemen maatregelen. Dit pakket voorkomt en/of reduceert de gevolgen van het manifest worden van de bedreigingen waar de informatiesystemen en de verantwoordelijkheidsgebieden die de processen van de organisatie ondersteunen, aan bloot kunnen staan. Ook kan het resultaat van de Kwetsbaarheidanalyse worden gebruikt voor het opstellen van een (informatie)beveiligings- en implementatieplan. Het opstellen van een kwetsbaarheidanalyse gebeurd aan de hand van de volgende stappen:

Stap 7: Inventariseren bestaande maatregelen
Inventariseer welke maatregelen er binnen de organisatie al bestaan.

Stap 8: Verdeling in (IT-)diensten en componenten
Bij de informatiesystemen die de processen ondersteunen, wordt gebruik gemaakt van diensten van anderen, waarbij al of niet informatietechnologie (IT) betrokken is. Aan de leveranciers van deze diensten en de daarin betrokken componenten worden ook informatiebeveiligingseisen gesteld, die voortvloeien uit de eisen gericht op de 'eigen' bedrijfsvoering. De leveranciers van deze diensten zullen de opzet en werking van die informatiebeveiligingseisen naar tevredenheid van de organisatie moeten aantonen.

Stap 9: Bepalen incidenten, gevolgen en ernst
Geef aan met welke incidenten rekening gehouden moet worden, wat de gevolgen voor de bedrijfsvoering van de organisatie zouden kunnen zijn en wat de ernst is van de gevolgen van het manifest worden van een incident.

Stap 10: Bepalen stelsel van maatregelen
Stel een stelsel van informatiebeveiligingsmaatregelen vast ter waarborging van een betrouwbaar functioneren van de informatiesystemen die de processen van de organisatie ondersteunen.

Het uitvoeren van stap 9 en 10 vindt plaats door het houden van een interview of workshop met management en medewerkers.

Bijlage: Beveiligingseisen verantwoordingsrichtlijn GeVS