gemeente wageningen

GEMEENTEBLAD

Officiële uitgave van gemeente Wageningen.

Nr. 76598

21 augustus 2015

Informatiebeveiligingsbeleid 2015

Het college van Burgemeester en Wethouders heeft in zijn vergadering van 4-8-2015 gesproken over informatiebeveiligingsbeleid en besloten:

1. Het informatiebeveiligingsbeleid 2015 vast te stellen

2. Het informatiebeveiligingsbeleid 2014 in te trekken

3. De stafadviseur bedrijfsvoering en ICT, Rob Haans, aan te wijzen als informatiebeveiligingscoördinator zoals beschreven in het informatiebeveiligingsbeleid

Inzage
Dit besluit wordt met deze elektronische publicatie volledig bekendgemaakt en niet meer fysiek ter inzage gelegd.

Bezwaar
Op dit besluit is geen bezwaar en beroep mogelijk.

Inleiding

In onze digitale samenleving zijn we zeer afhankelijk van (digitale) informatie. We delen zeer veel informatie met elkaar, met burgers en bedrijven en andere instanties. Hierdoor ontstaan ook risico's. De vraag is hoe we onze informatievoorziening willen en kunnen beschermen.
Dit document bevat algemene beleidsuitgangspunten over informatiebeveiliging. Die hebben een sterk normerend karakter en geven keuzes weer. Verder beschrijft dit document welke rollen betrokken zijn bij informatiebeveiliging en welke maatregelen genomen worden om informatie te beschermen. Dit zijn maatregelen op het vlak van huisvesting, ICT, maar houden ook werkafspraken en procedure-maatregelen in. Het beleid geldt dan ook niet alleen voor beheerders van informatie of voor gebouwbeheerders, maar ook voor medewerkers en managers. Iedereen in de organisatie gaat met informatie om.
Voor een groot deel is dit document een beschrijving van bestaande uitgangspunten, normen en maatregelen. De verschillende maatregelen en normen zijn wel eenduidig gemaakt en binnen één geheel geplaatst. De grootste vernieuwing is het 'open, tenzij'-principe. Dit uitgangspunt geeft richting aan onze interne informatievoorziening en is nodig om als organisatie flexibel met veranderingen om te kunnen gaan. Het gaat uit van vertrouwen in (het integer gedrag van) medewerkers, een van de kernwaarden van de gemeente Wageningen. Dit is geen blind vertrouwen en houdt in dat medewerkers elkaar kunnen aanspreken op gedrag. Het doorvoeren van het principe zorgt ervoor dat er bewuster wordt omgegaan met risico's.
Het informatiebeveiligingsbeleid is een onderdeel van het informatiebeleid van de gemeente Wageningen. Het is een zoveel mogelijk generiek plan. Buiten dit plan vallen specifieke procesbeschrijvingen (waarborgen voor betrouwbaarheid/integriteit van gegevens), het backup-, herstel- en uitwijkdraaiboek (waarborgen voor continuïteit van gegevens) en beleidsplannen en procedures die niet rechtstreeks met informatiebeveiliging te maken hebben, zoals het agressieprotocol. Buiten dit plan vallen ook specifieke handboeken, regelingen en verordeningen die vanuit wet- en regelgeving of audits opgesteld moeten worden. Al deze plannen hebben een relatie met dit plan.
Dit document is een geactualiseerde versie van het informatiebeveiligingsbeleid, dat vastgesteld is in 2014, en vervangt dat document dan ook. De aanpassingen hebben onder andere betrekking op de verschillende verantwoordelijkheden rond informatiebeveiliging, waarbij de rol van algemene informatiebeveiligingscoördinator is toegevoegd en functiescheidingen scherper zijn beschreven. Andere aanpassingen liggen op het gebied van privacybescherming en betere beschrijving van procedures rond beveiligingsincidenten en wijzigingen in taken van medewerkers.

H1 Bescherming van waardevolle informatie

Informatiebescherming draait om bescherming van de waardevolle informatie. Hoe meer waarde bepaalde informatie heeft voor de gemeente Wageningen, hoe meer beschermingsmaatregelen we nemen. De waarde van informatie wordt hieronder gesplitst in drie soorten: beschikbaarheid, integriteit en vertrouwelijkheid.

1.1 Beschikbaarheid van informatie
Informatie heeft waarde wanneer het continue beschikbaar moet zijn. Wanneer de informatie niet toegankelijk is en/of niet gebruikt kan worden, heeft dit een impact op de dienstverlening en op kosten. Dit is een verlies van efficiëntie. Het belang van beschikbaarheid is niet voor alle informatiebronnen

en systemen hetzelfde. Wanneer het belang van beschikbaarheid hiervan hoog is, wordt deze als *bedrijfskritisch* bestempeld en worden er aanvullende maatregelen genomen om bedreigingen op dit vlak tegen te gaan. De beoordeling van deze waarde moet worden gedaan door de eigenaar van de informatie.
Bedreigingen voor de beschikbaarheid van informatie zijn onder andere:
- Wijzigingen van software en netwerk die bewust, als aanval, of onbedoeld de beschikbaarheid van een informatiebronnen en systeem negatief beïnvloeden. Bij onvoldoende bescherming is de kans hierop vrij groot.
- Bedoeld, als aanval, of onbedoeld, door ondeskundig gebruik, verwijderen of vernietigen van informatie(bronnen). Bij onvoldoende bescherming is de kans hierop vrij groot.
- Te beperkte netwerkcapaciteit (snelheid, opslag) bij het gebruik van het netwerk of aanvallen gericht op het vastlopen van het netwerk. De kans op dit soort aanvallen is beperkt, maar netwerkcapaciteit moet continu in de gaten gehouden worden, want de kans op "bottlenecks" is vrij groot.
- Uitval van nutsvoorzieningen en elektriciteit (regionale of landelijke blackout). De waarschijnlijkheid hierop wordt door de VGGM ingeschat op 1x in de 50 jaar.
- brand (1x in de 100 jaar)

1.2 Integriteit van informatie
Informatie heeft waarde wanneer veranderingen ervan impact hebben op de organisatie. Dit betekent dat de "integriteit" van informatie beschermd moet worden. Integriteit van informatie betekent: "de mate waarin de gegevens in overeenstemming zijn met het afgebeelde deel van de realiteit, waarbij niets ten onrechte is toegevoegd, verdwenen of achtergehouden". Het belang van integriteit van informatie is niet voor alle informatie hetzelfde. Zo zal de boodschap van e-mail nog steeds overkomen als een komma verkeerd staat. Bij financiële gegevens kunnen de gevolgen van verlies van integriteit een stuk groter zijn. Bij archiefdocumenten (authenticiteit) en dossiers (volledigheid) speelt integriteit ook een grote rol. Informatiebronnen zijn *bedrijfskritisch* wanneer het belang van de integriteit van informatie hoog is. Aanvullende maatregelen zijn nodig om bedreigingen tegen te gaan.
Bedreigingen voor de integriteit van informatie zijn onder meer:
- Bedoeld (als fraude of diefstal) of onbedoeld (door ondeskundig gebruik) wijzigen van informatie(bronnen);
- Onbedoelde veranderingen aan informatie door vervanging en conversie van informatie, van bijvoorbeeld papier naar digitaal of van de ene applicatie naar de andere;

1.3 Vertrouwelijkheid van informatie
Informatie heeft ook waarde als ongeoorloofde toegang ertoe al impact heeft op de organisatie. Wanneer de toegang tot informatie impact kan hebben, wordt informatie als vertrouwelijk of gevoelig bestempeld. Vertrouwelijkheid betekent dat een gegeven alleen te benaderen is door iemand die daarvoor gemachtigd is. Vertrouwelijkheid speelt vooral bij de omgang met persoonsgegevens en naar communicatie buiten de gemeente. De gemeente kiest ervoor om geen beperkingen op vertrouwelijkheid van informatie toe te kennen, met uitzondering van persoonsgegevens waar rechten van burgers beschermd moeten worden. Buiten de organisatie kan de impact van een (te vroegtijdige) openbaarmaking van informatie groter zijn voor de gemeente, zoals speculatie van grond en vastgoed of (politieke) imagoschade. Informatie waarbij vertrouwelijkheid een rol speelt worden in dit document als *gevoelig* bestempeld.
Bedreigingen voor de vertrouwelijkheid van informatie zijn onder meer:
- Onjuiste autorisaties en machtigingen in informatiesystemen;
- Misbruik van andermans identiteit (identiteitsfraude) of doorbreken en omzeilen van autorisaties (hacking);
- Bedoeld of onbedoeld "lekken" van informatie.

De kans dat de bovenstaande bedreigingen optreden is vrij groot, maar geldt maar voor een deel van de informatie van de gemeente Wageningen. Er is dus maar een deel van de informatie dat bescherming nodig heeft.

H2 Beleidsuitgangspunten
De gemeente Wageningen hanteert een aantal belangrijke uitgangspunten in haar informatiebeveiligingsbeleid. De principes in dit hoofdstuk dienen ook buiten de beschreven maatregelen toegepast te worden.

2.1 Doel en scope informatiebeveiligingsbeleid
1. Informatiebeveiliging is het geheel van maatregelen, procedures en processen die de waarde van informatie beschermen voor de gemeente Wageningen. Hierbij staat de mens steeds meer centraal.
2. De informatiebeveiliging dient de volgende waarden van informatie van en/of binnen de Gemeente Wageningen te waarborgen: beschikbaarheid, integriteit en vertrouwelijkheid.

3. In het informatiebeveiligingsbeleid van de gemeente Wageningen worden de uitgangspunten op dit terrein weergegeven, wat de verschillende verantwoordelijkheden zijn van betrokken personen en welke maatregelen de gemeente Wageningen neemt om waardevolle informatie te beschermen.
4. De maatregelen om informatie te beschermen moeten in verhouding zijn met de waarde die de gemeente Wageningen wil beschermen en moeten effectief en efficiënt zijn. De maatregelen dienen zo min mogelijk ten koste te gaan van andere sturingsprincipes van de gemeente Wageningen, zoals flexibiliteit en klantgerichtheid.
5. De ambitie van het informatiebeveiligingsbeleid ligt vooral op externe controles (audits), privacygevoelige gegevens en hoge risico's (bijv. informatiesystemen die geheel of deels buiten het netwerk liggen).
6. Specifieke procesbeschrijvingen en handboeken die voor een beperkt deel van de organisatie interessant zijn vormen geen onderdeel van het informatiebeveiligingsbeleid, maar dienen er wel mee samen te hangen.
7. Het informatiebeveiligingsbeleid wordt jaarlijks geëvalueerd en indien nodig geactualiseerd.

2.2 Wetgeving/compliancy

1. De beveiliging dient te voldoen aan de relevante wet- en regelgeving die eisen stelt aan de betrouwbaarheid (beschikbaarheid, integriteit, vertrouwelijkheid) van informatie.
2. Bij nieuwe wet- en regelgeving moet de impact op de organisatie onderzocht worden en eventueel verwerkt worden in dit document.
3. De gemeente Wageningen kiest voor een pragmatische invulling van de bovenstaande wetgeving, wat betekent dat de focus ligt op wettelijke bepalingen die de basis zijn van externe controles en audits. Als het nodig is pakt de gemeente ook andere zaken aan.

2.3 Open/gesloten

1. Toegang tot informatie is beschikbaar op basis van het principe 'open, tenzij'. Informatie is openbaar en bij uitzondering kan daarvan afgeweken worden. Applicaties en informatiesystemen en andere bronnen van informatie worden hierop ingericht. Alleen aspecten die hoge risico's veroorzaken worden beheerst. Wanneer het doorvoeren van dit uitgangspunt echter kostenstijgingen met zich meebrengt, zullen kosten en baten afgewogen worden.
2. Persoonsgegevens zijn een belangrijke uitzondering. Op dit type gegeven is het tegengestelde principe van toepassing: 'least privilege' of 'need to know'; toegang is er pas na het vaststellen van de juiste machtiging.
3. Bedrijfskritische en gevoelige informatiebronnen en -systemen hebben extra beschermingsmaatregelen nodig. Hoewel toegang vrij kan zijn, geldt hier het principe 'open, tenzij' niet voor het hebben van bewerkingsbevoegdheden. Daarnaast worden deze informatiebronnen en -systemen in principe niet via internet ontsloten als dat via andere manieren mogelijk is (bijvoorbeeld via een directe lijn) of tenzij deze met extra veiligheidsmaatregelen omkleed zijn (zoals bijv. via een VPN-verbinding). Dit geldt ook voor de verbinding tussen het Wageningse netwerk en het informatiesysteem dat zich buiten het netwerk bevindt.
4. Voor de communicatie tussen het eigen netwerk en andere netwerken geldt ook het tegengestelde principe "dicht, tenzij..."

2.4 Persoonsgegevens

1. Het verzamelen, opslaan, verwerken en gebruiken van persoonsgegevens is uitsluitend toegestaan op basis van een of meer in de Wet Bescherming Persoonsgegevens (Wbp) genoemde grondslagen;
2. Persoonsgegevens waarvoor de gemeente Wageningen verantwoordelijk is mogen in principe alleen verwerkt worden voor het doel waarvoor ze oorspronkelijk verzameld zijn;
3. Persoonsgegevens waarvoor de gemeente Wageningen verantwoordelijk is mogen in principe alleen opgeslagen en verwerkt worden binnen het domein/netwerk van de gemeente Wageningen, tenzij een bewerkersovereenkomst is afgesloten;
4. Informatiesystemen die persoonsgegevens bevatten zijn alleen toegankelijk voor personen of instanties die daartoe bevoegd zijn.
5. Bij de verwerking en het gebruik van persoonsgegevens worden maatregelen getroffen om de privacy van burgers en personeel te waarborgen;
6. De verwerking moet worden gemeld aan het College Bescherming Persoonsgegevens, tenzij de verwerking van melding is uitgezonderd in het Vrijstellingsbesluit;
7. De betrokkene (eigenaar van eigen gegevens) moet ten alle tijde inzicht kunnen krijgen in zijn/haar gegevens en mag gegevens aan laten vullen, corrigeren, verwijderen of afschermen.

H3 Taken en verantwoordelijkheden

Er moeten principes gehanteerd worden, maatregelen genomen worden en keuzes gemaakt worden om informatiebeveiliging gestalte te geven binnen de organisatie. Deze principes, keuzes en maatregelen raken de hele organisatie van de gemeente Wageningen. De verantwoordelijkheidsverdeling is daardoor erg belangrijk.

3.1 Verantwoordelijkheden rond informatiebeveiliging

1. Informatiebeveiliging is ieders verantwoordelijkheid. Er wordt van alle medewerkers (ook ingehuurde) verwacht dat ze zich 'fatsoenlijk' gedragen en als de zaak er om vraagt geheimhouding betrachten. Dit staat beschreven in de gedragscode voor ambtenaren.
2. De gemeentesecretaris draagt de algemene eindverantwoordelijkheid voor informatiebeveiliging en deelaspecten ervan, zoals privacybescherming en de bedrijfscontinuïteit. De burgemeester draagt de bestuurlijke verantwoordelijkheid voor deze onderwerpen.
3. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Wageningen hebben een interne eigenaar die de waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid binnen de gemeente Wageningen voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie. Deze eigenaar is altijd een teammanager. Bij extern beheerde informatiebronnen en –systemen heeft de eigenaar de rol van opdrachtgever.
4. De eigenaar ziet er op toe dat het informatiebeveiligingsbeleid en de deelaspecten ervan, zoals het beleid op ICT-bedrijfscontinuïteit en privacybescherming, overeenkomstig wettelijke eisen en met inachtneming van bedrijfsvoeringsbelangen wordt uitgevoerd voor de informatiebronnen en –systemen waar deze eigenaar van is.
5. Elke teammanager is (mede-)verantwoordelijk voor de integrale informatiebeveiliging van en privacybescherming binnen zijn of haar organisatieonderdeel.
6. Applicatie-, systeem, facilitaire, gegevens- en archiefbeheerders zijn geen proceseigenaren maar zijn uitvoeringsverantwoordelijk voor een belangrijk deel van de informatiebeveiliging. Deze beheerders kunnen verstrekkende bevoegdheden hebben op basis van hun beheerrol. Deze bevoegdheden zijn in mandateringen en aanstellingen vastgelegd.
7. De eigenaar en beheerder bevorderen en adviseren over informatiebeveiliging en de deelaspecten ervan, verzorgen rapportages over de status ervan, controleren dat de maatregelen worden nageleefd, evalueren de uitkomsten en doen voorstellen tot implementatie c.q. aanpassing van het informatiebeveiligingsbeleid voor de aspecten die hun beheers- of eigenaarsrol raken.
8. Er is een algemene informatiebeveiligingscoördinator aangesteld door het College. Deze functionaris ziet er op toe dat het informatiebeveiligingsbeleid wordt opgesteld en geïmplementeerd. De informatiebeveiligingscoördinator bevordert en adviseert over informatiebeveiliging (en deelaspecten ervan) in samenspraak met eigenaren en beheerders, controleert dat de maatregelen worden nageleefd, evalueert de uitkomsten en doet voorstellen tot implementatie c.q. aanpassing van het informatiebeveiligingsbeleid. De functionaris rapporteert hierover eenmaal per jaar rechtstreeks aan het College (nadat de rapportage afgestemd is met de betrokkenen). Hierbij wordt ook aangegeven in welke mate de gewenste garanties en waarborgen voor de BRP en Suwinet zijn bereikt.
9. Taken, verantwoordelijkheden en bevoegdheden van medewerkers zijn zo geregeld dat medewerkers elkaars taken kunnen overnemen wanneer de continuïteit van informatievoorziening in gevaar komt.
10. Er zijn functiescheidingen en controle-mechanismes aangebracht in bedrijfskritische informatiesystemen. Beheerders hebben geen uitvoerende (gebruikers-)taken rond bedrijfskritische informatiesystemen waar ze beheerstaken voor uitvoeren. De informatiebeveiligingscoördinator heeft in deze informatiesystemen geen beheerdersrechten. Beslissingen worden in gezamenlijkheid genomen en in het uiterste geval door de eigenaar, de gemeentesecretaris of de burgemeester.
11. Er kunnen altijd uitzonderingen gemaakt worden op het informatiebeveiligingsbeleid. Dit moet in een wijzigingsoverleg besproken worden met de eigenaar, betrokken beheerder(s) en de algemene informatiebeveiligingscoördinator. Deze uitzonderingen worden vastgelegd in een formulier (zie bijlage) en ondertekend door de proceseigenaar.

3.2 Informatiebeveiliging en medewerkers

1. Al het personeel van de gemeente Wageningen moet een eed of belofte afleggen, waarmee ook de gedragscode voor ambtenaren ondertekend wordt. Ingehuurd personeel moet een integriteitverklaring ondertekenen.
2. Medewerkers zijn opgeleid in het gebruik van informatiesystemen en andere informatiebronnen en weten wat van hen verwacht wordt in het kader van informatiebeveiliging. Informatiebeveiliging is periodiek een onderwerp van gesprek in teamoverleggen wanneer binnen teams met bedrijfskritische of anderszins gevoelige informatie wordt gewerkt. Medewerkers kennen de waarde van informatie en handelen daarnaar. Van hen wordt verwacht dat ze actief bijdragen aan de veiligheid van informatiesystemen en de daarin opgeslagen informatie.
3. Wanneer medewerkers bedreigd worden of vinden dat ze onder druk gezet worden door andere personen om inbreuk te plegen op het informatiebeveiligingsbeleid wordt dit geuit bij de betrokken teammanager of een medewerker bij team POJ. Het team POJ hanteert hiervoor de leidraad "Agressie en geweld op het werk". De bovengenoemde personen zullen in onderling overleg actie ondernemen.

4. Wanneer beveiligingsincidenten (zoals onterechte gegevensverstrekkingen of schending van privacy) plaatsvinden wordt dit gemeld bij de betrokken teammanager en de ICT-servicedesk. Zij ondernemen naar aanleiding van dit incident actie:
   - bij externe meldingen wordt gehandeld conform de op de website gepubliceerde proclaimer en richtlijn responsible disclosure.
   - De teammanager neemt contact op met evt. gegevensbewerkers en andere betrokkenen.
   - Het beveiligingsincident wordt vastgelegd door de ICT-Servicedesk en de teammanager maakt in overleg met de betrokkenen een verbeterplan.
   - Indien nodig kan het Team POJ, in overleg met de manager van de betrokken medewerk(st)er, het College van B&W adviseren om disciplinaire maatregelen te nemen.
   - Indien nodig kan de teammanager van de betrokken medewerk(st)er het incident in een functioneringsgesprek bespreken.

5. Wanneer gevoelige gegevens in handen van derden gekomen zijn of wanneer er sterke aanwijzingen hiervoor zijn, wordt dit op een open manier gecommuniceerd met betrokken personen en instanties.

3.3 Vastleggen verantwoordelijkheden bij uitbesteding

1. Voorafgaand aan het afsluiten van een overeenkomst voor uitbesteding, samenwerking of externe inhuur is bepaald welke waarde en gevoeligheid de informatie heeft waarmee de derde partij in aanraking kan komen en een risicoanalyse gedaan.
2. Afspraken met externe partijen worden door de opdrachtgever (eigenaar) vastgelegd in een overeenkomst. Hierin is onder meer (indien van toepassing) opgenomen:
   a. De garantie van de leverancier dat de betrokken applicatie of gegevensverwerking aan relevante wet- en regelgeving voldoet, zal blijven voldoen en dat gebleken afwijkingen of tekortkomingen in dit opzicht door de leverancier op zo kort mogelijke termijn zullen worden hersteld. Verder dat de externe partij zelfstandig aansprakelijk is voor schade die door hem is veroorzaakt en kan worden toegerekend en dat de verantwoordelijke een regresrecht heeft (vrijwaringsbepaling).
   b. Dat gepaste beveiligingsmaatregelen worden genomen en dat beveiligingsincidenten worden gerapporteerd aan de opdrachtgever (eigenaar).
   c. Bij structurele (geautomatiseerde) gegevensuitwisseling tussen de gemeente Wageningen en andere organisaties, waarbij gebruik wordt gemaakt van intern opgeslagen gegevens, dient te worden vastgelegd onder wiens verantwoordelijkheid deze uitwisseling plaats vindt (bij het verwerken van persoonsgegevens krijgen de betrokken partijen die niet verantwoordelijk zijn de status van bewerker). Hier staat ook in aan welke kwaliteiten de uitwisseling moet voldoen en welke maatregelen vanuit het oogpunt van beveiliging door de partijen moeten worden getroffen.
   d. Welke verwerkingen de bewerker precies moet doen (bij een verwerking van persoonsgegevens) en evt. ook wat de bewerker (in ieder geval) niet mag doen. De bewerker mag de persoonsgegevens uitsluitend bewerken in opdracht van de opdrachtgever (eigenaar) en niet zelfstandig besluiten om de persoonsgegevens op een andere manier te verwerken.

a.Dat de opdrachtgever (eigenaar) de mogelijkheden heeft om te controleren dat de externe partij zich (geheel) aan de overeenkomst houdt.

2. Het naleven van de afspraken met externe partijen wordt gecontroleerd.

3.4 Specifieke verantwoordelijkheden rond Suwinet

1. Voor het informatiesysteem “Suwinet” is de eigenaar de teammanager Bedrijfsvoering Samenleving. De eigenaar is er verantwoordelijk voor dat Suwinet gebruikt wordt volgens de gestelde normen.
2. De informatiebeveiligingscoördinator is aangemeld als “Security Officer” bij de beheerder van Suwinet. De eerder genoemde taken van de informatiebeveiligingscoördinator zijn ook van toepassing op Suwinet.
3. De applicatiebeheerder van Suwinet is verantwoordelijk voor het verlenen van autorisaties, instructie aan medewerkers en controle op logging, en rapporteert hierover aan de eigenaar en de informatiebeveiligingscoördinator.

H4 Maatregelen

Informatiebeveiliging wordt gevormd door beschermingsmaatregelen. Per onderdeel wordt hieronder beschreven wat de gemeente Wageningen doet om haar waardevolle informatie te beschermen.

4.1 Toegang tot en gebruik van informatie

1. Voordat toegang verleend wordt tot informatie en informatiesystemen wordt bepaald of en welke identificatie, authenticatie en autorisatie vereist is.
2. Alleen geautoriseerde medewerkers en bezoekers hebben toegang tot het netwerk van de gemeente. Zij hebben een beveiligd inlogaccount nodig dat ze krijgen van het team Automatisering. De wachtwoorden zijn beveiligd en bestaan uit minimaal 8 posities met een combinatie (3 van de 4 categorieën) van hoofd- en kleine letters, cijfers en/of speciale tekens. Het wachtwoord kan niet (onderdelen groter dan 3 tekens van) de eigen inlognaam bevatten en kan niet eerder gebruikt zijn. De wachtwoorden worden eens in de 60 dagen gewijzigd. De gebruiker wordt geblokkeerd na drie keer het verkeerde wachtwoord te hebben ingetypt. Het systeem maakt hier melding van. Daarnaast hebben servers, databases en bedrijfskritische en gevoelige informatiesystemen (incl. testomgevingen) een eigen vorm van toegangsbeveiliging. Bij deze informatiesystemen mogen geen groepsaccounts gebruikt worden. Standaard accountnamen en wachtwoorden moeten aangepast worden. Bedrijfskritische en gevoelige informatie wordt niet onbeheerd op werkplekken achtergelaten en/of zichtbaar gemaakt voor onbevoegden. Wachtwoorden zijn niet op te vragen. Toegang tot het netwerk via niet door de gemeente beheerde apparaten wordt alleen via 2-weg authenticatie verleend (token en wachtwoord) en aangevuld met extra veiligheidsmaatregelen.
3. De toegang tot gebouwen van de Gemeente Wageningen is voorbehouden aan geautoriseerde medewerkers en bezoekers. Hiervoor beschikken ze over een badge. Bezoekers worden altijd opgehaald en begeleid door eigen personeel. De toegang tot het gebouw buiten kantooruren is slechts voorbehouden aan medewerkers van het team Facilitair Management, Automatisering en een calamiteiten kernteam. Een gedeelte van het gebouw is daarnaast 's avonds tijdens raadsvergaderingen open voor raadsleden, college en bezoek. Bedrijfskritische onderdelen van het gebouw hebben een aparte toegangscontrole die alleen toegang geeft aan specifieke geautoriseerde (gebaseerd op functie van) medewerkers. Bij stroomuitval werken de buitendeuren slechts met behulp van een sleutel. Sleutelafgifte voor toegang van buitenaf is zeer beperkt. Er is een toegangscontrolesysteem voor alle locaties waarmee toegang gereguleerd wordt. De actualiteit ervan wordt periodiek bewaakt. Onbevoegd gebruik van kopieerapparaten en scanners is niet mogelijk.
4. Toegangsrechten en autorisaties voor alle informatiesystemen en gebouwen worden actief onderhouden en eens per maand opgeschoond of inactief gezet. Bij tijdelijke medewerkers worden toegangsrechten zoveel mogelijk met een einddatum toegekend. Bij ontslag en vertrek van een medewerker of wijziging van functie of team meldt de betrokken teammanager dit via een formulier en worden zijn/haar account en autorisaties direct gewijzigd of geblokkeerd. Als een maand geen gebruik wordt gemaakt van autorisaties of de toegangspas, doet de betrokken beheerder een melding aan de betrokken teammanager met de vraag of toegangsrechten en autorisaties ingetrokken kunnen worden of dat ze verlengd moeten worden. Naast accountgegevens worden ook gegevens in bijvoorbeeld mailboxen, verkenner-omgeving en inrichting van applicaties (bijv. workflows) opgeschoond.
5. De gemeente Wageningen analyseert periodiek (afhankelijk van het risiconiveau) het gebruik van informatiesystemen die gevoelige informatie zoals persoonsgegevens bevatten. Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen worden hiertoe vastgelegd in logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole. Er vindt controle plaats op de opslag van logbestanden.
6. Informatie, (delen van) applicaties, computers en gegevensdragers van de Gemeente Wageningen die geen gebruikswaarde meer hebben worden zoveel mogelijk verwijderd, vernietigd of uitgeschakeld. Dit geldt bijvoorbeeld voor gegevens op mobiele gegevensdragers, voor informatie op de website en voor vernietiging vatbaar archiefmateriaal. Verwijdering en vernietiging van informatie en gegevensdragers gebeurt volgens daarvoor geldende wet- en regelgeving.
7. Bij het opzetten van een verbinding voor interne datacommunicatie is de identiteit van de betrokken zend- en ontvangstpunten verzekerd door identificatie van de terminal en het aansluitpunt.
8. Bij het opzetten van een verbinding voor externe datacommunicatie is de identiteit van de betrokken zend- en ontvangstpunten verzekerd door terminal identificatie. Dit gaat via drie gescheiden loginprocedures voor VPN, terminal servers, bedrijfskritische en gevoelige applicaties en via de firewalls en routers. De controle op authenticiteit is niet door onbevoegden te onderscheppen. Bij het extern verzenden van bedrijfskritische of gevoelige gegevens worden de gegevens via cryptografische methoden versleuteld. Handelingen van derden die van buiten het netwerk op het netwerk van de gemeente Wageningen worden verricht (inbellen) worden alleen op verzoek toegestaan. Dit is afhankelijk van de bevoegdheden en mogelijkheden van de inbeller (raadplegen/wijzigen) door applicatiebeheer en/of systeembeheer. Wanneer inbellers bevoegdheden of mogelijkheden hebben om gegevens te veranderen kijkt een betrokken beheerder mee.
9. Het buiten de gemeente versturen van bedrijfskritische, vertrouwelijke of anderszins gevoelige informatie vindt uitsluitend plaats indien dit voor de uitoefening van de functie noodzakelijk is en dient altijd omkleed te zijn met gepaste beschermingsmaatregelen. Onder "buiten de gemeente versturen" wordt verstaan: "buiten de gemeente meenemen, het fysiek of per mail versturen of het plaatsen op internettoepassingen". Wanneer dit soort gegevens extern verstuurd worden,

moet de verstuurder controleren dat de gegevens in goede staat aangekomen zijn bij de afnemer. Bij versturing via fysieke post kan dit door deze aangetekend te versturen, bij digitale verzending door een vorm van ontvangstbevestiging.

10. Wanneer informatie omgezet wordt van medium (papier naar digitaal), bestandsformaat (bijv. van tiff naar jpeg) of van applicatie (bijv. via een koppeling) worden maatregelen genomen om de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie te verzekeren.

4.2 Technische maatregelen

1. Er wordt alleen gewerkt met geautoriseerde versies van (legale) programmatuur. Voor alle applicaties die (voor een deel) buiten het netwerk van de gemeente Wageningen staan zijn servicepacks en (beveiligings)patches geïnstalleerd en deze worden volgens een beheerst proces doorgevoerd. Dit ligt vast in een overeenkomst. Bedrijfskritische applicaties (deels) buiten het netwerk van de gemeente Wageningen periodiek onderworpen aan een penetratietest en een scan op kwetsbaarheden.
2. Apparatuur en andere hulpmiddelen die van belang zijn voor informatiesystemen (bijv. kabels) worden zo geplaatst en beschermd dat risico's van schade, storing en ongeoorloofde toegang beperkt zijn.
3. Mobiele/verwijderbare gegevensdragers, zoals mobiele telefoons, usb-opslag, tapes en Cd-rom's, dienen goed beheerd worden indien deze gevoelige gegevens bevatten. Gevoelige gegevens hierop dienen beveiligd te zijn.
4. De netwerkbeveiliging gaat uit van beveiliging in lagen ("layered defense, defense-in-depth"). De lagen zijn zo ontworpen dat het falen van één laag niet leidt tot het falen van het geheel. Hierbij wordt gebruik gemaakt van een Demilitarised Zone (DMZ), waarbij compartimentering wordt toegepast en de verkeersstromen tussen deze compartimenten wordt beperkt tot alleen de hoogst noodzakelijke.
5. Er zijn, indien mogelijk, maatregelen getroffen voor detectie en preventie van virussen, spyware, spam en phishing-programmatuur, ook op mobiele apparatuur. Er wordt stelselmatig gecontroleerd op de aanwezigheid van dit soort programmatuur. Dit geldt voor zowel het netwerk van de gemeente Wageningen als verkeer met informatiesystemen en apparatuur die in verbinding staat met het netwerk van de gemeente Wageningen, zoals usb-sticks.
6. Er zijn firewalls op het netwerk van de gemeente Wageningen. Deze zijn zo geconfigureerd dat alle poorten die (in productie) niet noodzakelijk zijn worden gesloten. Er wordt gebruik gemaakt van Intrusion Detection. Bij inloggen van buitenaf wordt de verbinding en toegang tot het netwerk afgeschermd tegen indringen van buitenaf. Wijzigingen in de firewall die beperkend werken moeten van te voren aangekondigd, besproken en getest worden met betrokken functioneel applicatiebeheerders. Het netwerk wordt periodiek onderworpen aan een penetratietest en gescand op kwetsbaarheden.
7. Het beheer en de opslag van gegevens zijn zodanig, dat het risico op verlies van informatie beperkt is. De ICT-omgeving is dubbel (gespiegeld) uitgevoerd. Minimaal iedere werkdag worden alle gemuteerde gegevens (via back-up) veiliggesteld. Daarnaast wordt ieder weekend alle gegevens veiliggesteld. Iedere maand, kwartaal en jaar worden deze backup-gegevens extern opgeslagen. Een nader aan te wijzen deel van de gebouwen is voorzien van een noodstroomvoorziening, in ieder geval de serverruimtes van de afdeling automatisering. De gemeente Wageningen gebruikt een NAS-systeem. Dit systeem bevat meerdere schijven. Als een schijf crasht neemt de "reserveschijf" de taken van de uitgevallen schijf over (RAID). Het NAS-systeem beschikt over vijf reserveschijven. Een kapotte schijf wordt volgens contract binnen 24 uur vervangen. Ook databasegegevens worden op een RAID 5 systeem opgeslagen met vergelijkbare veiligheidsmaatregelen.
8. Voor bedrijfskritische onderdelen van de ICT-omgeving zijn er voorzieningen om interne uitwijk mogelijk te maken bij calamiteiten. Er zijn onderhoudscontracten afgesloten bij leveranciers die een snelle en goede ondersteuning bij calamiteiten garanderen. De backup-, herstel- en uitwijkconfiguratie wordt tenminste eenmaal per twaalf maanden getest op actualiteit en juiste werking. Van deze test wordt een verslag opgesteld.
9. Gebouwen zijn beveiligd tegen inbraak. Er zijn op verschillende plekken overval alarmknoppen geplaatst. Wanneer de gebouwen niet in bedrijf zijn, is het inbraakmeldsysteem ingeschakeld. Het gebouw is opgesplitst in meerdere zones. Het uitschakelen van dit systeem is voorbehouden aan medewerkers van het team Facilitair Management, Automatisering en raadsleden (deze laatste groep alleen voor een beperkt deel van het gebouw). Inbraak- en storingsmeldingen komen binnen bij een particuliere alarmcentrale. In het geval van calamiteiten wordt de dienstdoende bode/huismeester gewaarschuwd, alsmede de surveillant van een particuliere beveiligingsdienst. In de publiekshal van het gebouw is (zichtbaar en aangekondigd) cameratoezicht. De beelden worden na 5 dagen overschreven en zijn slechts in te zien door de gebouwbeheerders. Er worden geen andere gegevens vastgelegd dat datum en tijdstip.
10. Gebouwen zijn beveiligd tegen brand. De gebouwen van de gemeente zijn voorzien van een NEN-gecertificeerd branddetectiesysteem. Afhankelijk van de te beveiligen objecten signaleert dit systeem op basis van rook of warmte. Buiten kantooruren worden brand- en storingsmeldingen

rechtstreeks gemeld aan de meldkamer van de regionale brandweer en de servicecentrale van de leverancier van het detectiesysteem. In geval van calamiteiten wordt daarnaast de bode/huismeester gewaarschuwd. Het systeem wordt maandelijks getest. Verder is het gehele gemeentehuis voorzien van kleine blusmiddelen. Deze staan aangegeven op het ontruimingsplan en worden één maal per jaar getest en onderhouden door het bedrijf dat de middelen geplaatst heeft. Op een aantal plaatsen hangen brandslangen (haspels). De ruimte waar de computerhardware (servers/patchpanel) staat is voorzien van een airco om hoge temperaturen terug te dringen. De ruimte is voorzien van een temperatuurmelder die de bode/huismeester alarmeert via een telefoonkiezer wanneer de temperatuur te hoog wordt. Eenmaal per jaar wordt een ontruiming geoefend.

11. Fysieke documenten die gevoelige gegevens bevatten of van bedrijfskritisch belang zijn worden in beveiligde ruimtes bewaard. Dit is de archiefruimte of archiefbewaarplaats/kluis, afhankelijk van niveau van gevoeligheid of bedrijfskritisch belang. De archiefbewaarplaats voldoet aan daarvoor geldende wettelijke eisen. In geval van wateroverlast of brand bieden de deuren van de archiefbewaarplaats voldoende bescherming door een afdichtende strip die geactiveerd wordt bij oververhitting of contact met water. In geval van brand sluiten de deuren automatisch via kleefmagneten. De archiefbewaarplaats wordt ook gebruikt voor interne opslag van back-up media.

4.3 Nieuwe systemen en wijzigingen

1. Bij wijzigingen van de informatievoorziening wordt vanaf de start rekening gehouden met informatiebeveiliging en privacybescherming. Voor de procedure van het wijzigingenproces wordt verwezen naar het Informatiebeleid van de Gemeente Wageningen.
2. Installatie van systemen verloopt volgens de instructies van de leverancier.
3. Aanschaf, installatie en onderhoud van informatiesystemen mag geen afbreuk doen aan het niveau van veiligheid van de totale informatievoorziening.
4. Alle wijzigingen worden altijd eerst getest voordat deze in productie worden genomen. Een acceptatietest geldt als ingangscontrole op de eisen, die aan de ontwikkeling en het onderhoud gesteld zijn.
5. Bij de geautomatiseerde informatievoorziening zijn scheidingen aangebracht tussen de testomgeving en de productieomgeving.
6. Updates/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de potentiële schade hoog is worden zo spoedig mogelijk doorgevoerd, echter minimaal binnen één week. Minder kritische beveiligings-updates/patches worden ingepland bij de eerst volgende onderhoudsronde.

4.4 Specifieke maatregelen basisregistraties

1. De technische en organisatorische inrichting van de door de gemeente beheerde basisregistraties is zodanig van aard en opzet dat de gegevens daarin volledig zijn opgenomen, juist en actueel zijn en voldoen aan hiervoor geldende richtlijnen. Hiervoor zijn instructies en procesbeschrijvingen met betrekking tot het invoeren van gegevens, het controleren van gegevens en het wijzigen van de ingevoerde gegevens opgesteld. Betrokken teammanagers (eigenaren) zien minimaal één keer per jaar toe op de naleving van de instructies. Minimaal één keer per jaar worden producties c.q. controleprogramma's gedraaid voor het beheersen van de integriteit van de gegevens. De door de gemeente gebruikte applicatie voor het beheren van de basisregistraties voldoet aan hiervoor geldende richtlijnen.
2. Registratie van gegevens voor de basisregistraties Personen (BRP) en Adressen en Gebouwen (BAG) gebeurt op basis van originele brondocumenten.
3. De verantwoordelijke personen en teams treffen maatregelen dat op ieder gewenst moment en periodiek de gegevens in de basisregistraties kunnen worden gecontroleerd. Brondocumenten voor de BAG kunnen binnen 3 uur getoond worden.
4. Kritische onderdelen van informatiesystemen voor basisregistraties worden binnen 48 uur hersteld en overige delen binnen 72 uur. De voorzieningen zijn zodanig dan maximaal één werkdag aan geautomatiseerde gegevensverwerking verloren kan gaan.
5. In het geval van een calamiteit zijn er voorzieningen getroffen voor het BAG. Binnen vier weken kunnen de meest noodzakelijke activiteiten plaatsvinden op een andere locatie.
6. Bronnen die sinds de laatste back-up gebruikt zijn voor de mutaties in de basisregistraties worden bewaard. Door het opnieuw invoeren of inlezen van de mutaties wordt aansluiting gevonden met de datum en het tijdstip van de laatste back-up.

4. 5 Specifieke maatregelen bedrijfskritische webapplicaties

1. Voor webapplicaties met DigiD wordt al het bezoek via logging actief gecontroleerd.
2. Beheer- en productieverkeer van bedrijfskritische webapplicaties zijn van elkaar gescheiden.
3. Bedrijfskritische webapplicaties valideren alle invoer, inclusief HTTP-verzoeken, aan de serverzijde. De applicaties controleren voor elke invoer en http-verzoek of de initiator geauthenticeerd is en de juiste autorisaties heeft. Invoerdata wordt voor validatie genormaliseerd. Webapplicaties met DigiD staan geen dynamische file includes toe of beperken de keuze mogelijkheid bij invoer.

4. Voor het raadplegen en/of wijzigen van gegevens in de database gebruiken bedrijfskritische webapplicaties alleen voorgedefinieerde zoekvragen.
5. Bedrijfskritische webapplicaties coderen dynamische onderdelen in de uitvoer en maken gebruik van versleutelde (HTTPS) verbindingen. Cookies worden versleuteld. Cookie attributen van webapplicaties met DigiD staan op 'HttpOnly' en 'Secure'. Gevoelige gegevens op webapplicaties met DigiD worden versleuteld opgeslaan. Sleutels hiervan zijn niet onversleuteld op de servers te vinden.
6. Voor bedrijfskritische webapplicaties worden periodiek (geautomatiseerde) blackbox scans uitgevoerd.
7. Beheermogelijkheden voor bedrijfskritische webapplicaties worden zoveel mogelijk beperkt. Beheer van bedrijfskritische webapplicaties buiten het netwerk van de gemeente Wageningen is alleen toegestaan vanaf vooraf gedefinieerde IP-adressen. Hierbij worden complexe wachtwoorden en/of sterke authenticatiemechanismen gebruikt.

4.6 Specifieke maatregelen Suwinet

1. Toegang tot Suwinet is beperkt tot een aantal functies die vanuit een publiekrechtelijke taak gegevens nodig hebben uit de suwi-keten. Toegangsrechten voor Suwinet worden vastgelegd in een autorisatiematrix. Hierin wordt een relatie gelegd tussen gebruikersgroepen en specifieke functies in Suwinet. Het aantal accounts waarbij gebruikers kunnen zoeken met meerdere zoeksleutels dan het BSN (zware autorisaties) is zeer beperkt (minder dan 20% van het totaal).
2. Nieuwe functionaliteiten binnen Suwinet worden na het beschikbaar komen actief uitgezet bij gebruikers van Suwinet en verwerkt in de autorisatiematrix.
3. Toegangsrechten worden maandelijks gecontroleerd. Deze controle wordt schriftelijk vastgelegd en gedeeld met de Security Officer voor Suwinet.
4. Het gebruik van Suwinet wordt gelogd en periodiek gecontroleerd. De logginggegevens worden door de applicatiebeheerder beoordeeld. Bij twijfel of vermoedens van ongeoorloofd gebruik wordt direct overleg gevoerd door de betrokken teammanager met de betreffende medewerker. Worden twijfels of vermoedens in het gesprek onvoldoende weggenomen, dan wordt het ongeoorloofd gebruik als beveiligingsincident bestempeld en vastgelegd.
5. Als overheidsorganisaties (via Suwinet) of burgers (via internet) daar om vragen levert de gemeente Wageningen via DKD binnen 15 seconden de gevraagde gegevens. Gegevensoverdracht wordt actief gelogd en gecontroleerd.
6. Het gebruik van Suwinet vindt slechts plaats via beveiligde verbindingen. Alleen verkeer uit het eigen netwerk van de Suwi-partij wordt via firewalls aangeboden aan het Suwi-Koppelpunt. Bij koppelingen van de Suwi-partij aan de Suwinetinfrastructuur wordt filtering toegepast, waarmee alleen geautoriseerd netwerkverkeer tussen de Suwi-partijen wordt doorgelaten. De inrichting van de externe koppeling is voorzien van afzonderlijke beveiligingzones.

4.7 Vastleggen maatregelen

1. Er wordt een inventaris bijgehouden van alle informatiesystemen en andere middelen die informatie bevatten. Deze informatie wordt beschermd tegen ongeoorloofde toegang. Hierin moet in ieder geval vastgelegd zijn:
   a. Eigenaar
   b. Beheerder
   c. Type computer(s)
   d. Besturingssysteem van de gebruikte computers
   e. Locatie van opslag en type database(s)
   f. Niveau waarop toegangsbeveiliging voor toegang is geregeld: applicatie, besturingssysteem, database en/of internet
   g. Bestandsinformatie
   h. Licenties
   i. Informatie over backup en evt. uitwijk
   j. Belang voor de organisatie

2. Voor iedere nieuwe versie van de applicatie worden de volgende zaken bijgehouden:
   a. datum van binnenkomst nieuwe versie
   b. versie
   c. begin datum van de test
   d. akkoord van de applicatiebeheerder
   e. installatie datum op de productieserver
   f. paraaf installateur

3. Voor specifieke bedrijfskritische of anderszins risicovolle systemen wordt schriftelijk vastgelegd welke beveiligingsmaatregelen van kracht zijn en worden instructies, procesbeschrijvingen, rap-

portages, verslagen van tests en controles in een dossier verzameld. Dit geldt vooral voor systemen die onderhevig zijn aan externe controles en gemeentelijke systemen buiten het netwerk van de gemeente Wageningen.

4. Bij gebruik door medewerkers van draagbare computers en telefoons van de gemeente Wageningen, zoals laptops, tablets en mobiele telefoons en bij gebruik van specifieke ICT-diensten op afstand (zoals webmail) wordt een gebruiksovereenkomst getekend. Hierin wordt ook ingegaan op informatiebeveiliging.
5. Maatregelen die genomen moeten worden om beschikbaarheid en integriteit van informatie te waarborgen bij calamiteiten worden vastgelegd in een integraal uitwijkdraaiboek, waarin alle taken, verantwoordelijkheden en acties zijn vastgelegd. Dit draaiboek is altijd beschikbaar, ook wanneer de reguliere locaties niet bereikbaar zijn.

Bijlage 1 Uitleg begrippen

Begrip	Uitleg/definitie
'need to know' of 'least privilege'	Principe bij toekennen van autorisaties, waarbij alleen toegang gegeven wordt tot wat een gebruiker voor de rol/taak/proces/vraag nodig heeft. Tegengesteld aan het principe 'open, tenzij', waarbij alleen toegang beperkt wordt op die gebieden waar risico's kunnen optreden.
Applicatie	Een computerprogramma dat bedoeld is om toegepast te worden voor een bepaalde taak of functie (letterlijk: toepassing). Dit programma kan een complex van samenhangende programmatuur zijn (soms ook wel een "suite" genoemd) of uitgebreid worden met extra toepassingen (ook wel "modules" genoemd).
Audit	Een onafhankelijke beoordeling om de activiteiten en de resultaten van een organisatie te onderzoeken en te evalueren.
Authenticeren	Het nagaan of een gebruiker de persoon of applicatie is voor wie hij zich uitgeeft.
Autoriseren	Het er voor zorgdragen een geïdentificeerde en geauthenticeerde persoon of applicatie enkel toegang krijgt tot voor hem ter beschikking gestelde diensten en informatie.
Archiefbewaarplaats	Bewaarplaats die is aangewezen en ingericht voor de blijvende bewaring van informatie. In wet- en regelgeving (archiefbesluit e.d.) zijn de eisen aangegeven waaraan een archiefbewaarplaats dient te voldoen.
Archiefruimte	Een ruimte bestemd voor tijdelijke bewaring van informatie.
Back-up	Veiligheidskopie van gegevens, die gebruikt kan worden als de originele gegevens verloren gegaan of onleesbaar zijn geworden.
Bedrijfskritisch	Kenmerk van een proces, informatie(bron), programma of ieder ander bedrijfsobject dat aangeeft dat de continuïteit van de bedrijfsvoering afhankelijk is van de beschikbaarheid ervan of dat de organisatie in hoge mate afhankelijk is van de integriteit of authenciteit van informatie er in.
Beschikbaarheid	De mate waarin informatie, informatiebronnen, ICT-voorzieningen op normale wijze gebruikt kan worden op het moment dat de organisatie het nodig heeft.
Beveiligingsincident	Een activiteit die het (informatie)beveiligingsbeleid schendt. Hieronder worden onder meer verstaan: pogingen (succesvol en niet-succesvol) ongeautoriseerd toegang te krijgen tot een netwerk, applicatie of de gegevens daarvan, niet-gewenste verstoring of dienstontzegging, ongeautoriseerd gebruik van een applicatie of de gegevens daarvan, wijzigingen van hardware-, firmware- of softwarekarakteristieken zonder kennis van de eigenaar, diens instructie of toestemming.
Bewerker	Bij de verwerking van persoonsgegevens kan de verantwoordelijke een bewerker inschakelen. De bewerker is een buiten de organisatie van de verantwoordelijke staande persoon of instelling. De bewerker neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegevens enz.
Blackbox testen	Een wijze van testen die applicaties alleen test op de mate waarin het aan toepassingseisen voldoet (functionele wensen en eisen) zonder kennis van de interne werking van de programmatuur. Testen waarbij wel kennis over de interne werking bestaat en evt. meegetest wordt wordt ook wel "white box" testen genoemd.
Compliancy	Een begrip waarmee wordt aangeduid dat een persoon of organisatie werkt in overeenstemming met de geldende wet- en regelgeving.
Computer	Elektronische gegevensverwerkende machine die een groot aantal rekenkundige en logische handelingen kan verrichten en daarbij door een intern programma wordt bestuurd.
Cookies	Kleine tekst bestandjes waarin informatie over een bezoeker lokaal op het systeem opgeslagen worden. Hierin kunnen voorkeuren, maar ook gebruikersnaam en wachtwoord in worden opgeslagen.
Demilitarised Zone (DMZ)	Dit is een een gedeelte van het netwerk dat zich tussen het interne netwerk en het internet bevindt en volledig toegankelijk is. Op de DMZ zijn servers aangesloten die nodig zijn voor externe communicatie, zoals voor de website. De DMZ wordt door een firewall beschermd, maar deze is zodanig ingesteld zijn dat de diensten toegankelijk blijven.
DigiD	Een systeem waarmee Nederlandse overheden op internet iemands identiteit kunnen verifiëren (identificeren en authenticeren), een soort digitaal paspoort voor overheidinstanties. Letterlijk: Digitale identiteit.
Firewall	Een informatiesysteemwaarmee de middelen van een netwerk of computer beschermd kunnen worden tegen misbruik van buitenaf. Aan de hand van een aantal regels bepaalt de firewall of verstuurde gegevens wordt doorgelaten of tegengehouden.
Functiescheiding	Het uit controle-overwegingen aanbrengen van een splitsing in taken en bevoegdheden die samenhangen met administratief handelen, over verschillende daartoe aangewezen medewerkers.
Gebruiker	Iedere persoon of applicatie die op een of andere manier gebruik maakt van een informatiesysteem.
Gegevensverwerking	Een verwerking van gegevens is elke handeling of elk geheel van handelingen met betrekking tot gegevens. Verwerkingen zijn in ieder geval het verzamelen,

	vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.
Gevoelig	Kenmerk van informatie dat aangeeft dat vertrouwelijkheid een rol speelt. Informatie wordt als gevoelig bestempeld wanneer deze maar voor een beperkt aantal personen openbaar mag zijn.
Identificeren	Het vaststellen van de identiteit van een gebruiker die zich aanmeldt voor gebruik van het netwerk of applicatie.
Informatiesysteem	Geheel van gegevens, structurele informatie, applicatie(s), apparaten en daarbij benodigde hulpmiddelen, opgezet voor de uitvoering van zijn of haar taken. Het informatiesysteem transformeert gegevens tot informatie.
Integriteit	De mate waarin gegevens in overeenstemming zijn met de realiteit, waarbij niets ten onrechte is toegevoegd, verdwenen of achtergehouden. Het is een kwaliteitsattribuut dat de authenticiteit en daarmee betrouwbaarheid waarborgt.
Intrusion Detection Systeem	Een informatiesysteem dat al het inkomend en uitgaand netwerkverkeer volgt en dat verdachte patronen daarin kan identificeren om een inbraak van het netwerk te herkennen.
Layered defense, defense-in-depth	Een begrip waarmee een in lagen opgebouwde reeks aan beveiligingsmaatregelen wordt aangeduid.
Logische toegangscontrole	Een vorm van toegangscontrole waarbij gebruik wordt gemaakt van informatie om toegang te verlenen. Dit in tegenstelling tot fysieke toegangscontrole, waarbij voorwerpen als sleutels worden gebruikt om toegang te verlenen. Combinaties van fysieke en logische toegangscontrole zijn ook mogelijk.
NAS-systeem	Een opslagmedium dat op het netwerk aangesloten is. NAS-systemen kunnen gebruikmaken van meerdere harde schijven.
Netwerk	Een netwerk is een verzameling van onderling verbonden computers. Binnen het netwerk kunnen computers gegevens met elkaar uitwisselen. Netwerken kunnen ook informatie uitwisselen met andere netwerken en zelf verdeeld zijn in sub-netwerken.
Patch	Kleine wijziging in een programma. Vaak verhelpt een patch een fout uit een programma, maar het kan ook een toevoeging zijn aan een bestaand programma. Een patch bestaat uit een (verzameling) bestand(en), die naar de directory van het programma gekopieerd dienen te worden.
Persoonsgegevens	Persoonsgegevens zijn alle gegevens over een geïdentificeerde of identificeerbare natuurlijke persoon. Een persoon is identificeerbaar indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden.
Penetratietest	Een test die tot doel heeft te testen hoe moeilijk het is om een netwerk ongeautoriseerd binnen te dringen. Bij een penetratietest wordt gebruik gemaakt van applicaties om gaten in de beveiliging (kwetsbaarheden) van netwerken en informatiesystemen te ontdekken.
Phishing	Het vissen (hengelen) naar gegevens gericht op personen, waarbij wordt verleid en verzocht om vertrouwelijke gegevens ergens in te vullen. Hiervoor worden communicatie-uitingen gebruikt die zoveel mogelijk lijken op die van legale instanties en bedrijven.
Programma	Een reeks opdrachten die een computer moet uitvoeren.
RAID	Een afkorting van Redundant Array of Independent Disks, een methode voor fysieke data-opslag op harde schijven waarbij de gegevens over meer schijven verdeeld worden en/of op meer dan één schijf worden opgeslagen ten behoeve van snelheidswinst en/of beveiliging tegen gegevensverlies.
Router	Apparaat dat informatiesystemen of netwerken met elkaar verbindt en/of met het internet. Omdat dit apparaat bepaalt langs welke route de gegevens worden verstuurd/ontvangen, wordt dit apparaat een router genoemd.
Server	Informatiesysteem dat aan iedere gebruiker van een netwerk diensten verleent, zoals het beschikbaar stellen van opslagcapaciteit voor gegevens. Een server staat centraal in een netwerk.
Servicepack	Een update voor een programma, die meerdere fouten opheft en eventueel nieuwe functies oplevert, danwel het programma aanpast aan nieuwe technieken. In tegenstelling tot een patch, die aan een bepaald probleem is gewijd, bevat een service pack een reeks aan patches.
Spam	Ongewenste berichten (vaak reclame), doorgaans in grote aantallen tegelijk verstuurd of geplaatst op communicatieplatforms. Letterlijk: Stupid Person's AdvertiseMent.
Spyware	Applicatie die ongevraagd of ongewild op een computer of netwerk wordt geïnstalleerd om handelingen van gebruikers te registreren (internetgedrag, toetsaanslagen) en extern door te sluizen.
Suwinet	Elektronische infrastructuur gebruikt door onder andere het UWV, Belastingdienst, RDW en gemeenten bij de uitvoering van de wettelijke taken die voor gemeenten met name op het terrein van werk en inkomen liggen. Via Suwinet worden gegevens over burgers uitgewisseld die te maken hebben met vermogen, loon, uitkeringen, etc.
Verantwoordelijke	De verantwoordelijke in de zin van de Wbp is degene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. De verantwoordelijke bepaalt welke persoonsgegevens, voor welk doel, op welke manier en met welke middelen worden verwerkt.

Bijlage 2 Risicoklassering persoonsgegevens

Niet alle verwerking van persoonsgegevens is risicovol. Er wordt onderscheid gemaakt in twee risiconiveaus, laag en hoog.

Laag risico

Openbare persoonsgegevens vallen in ieder geval onder deze categorie. Hiervan is algemeen aanvaard is dat deze, bij het beoogde gebruik, geen risico opleveren voor de betrokkene. Voorbeelden hiervan zijn telefoonboeken, brochures, publieke internet sites etc. Daarnaast bestaat een categorie persoonsgegevens waarvan de risico's voor de betrokkene bij verlies of onbevoegd of onzorgvuldig gebruik van de persoonsgegevens zodanig laag zijn dat standaard (informatie)beveiligingsmaatregelen toereikend zijn. Bij verwerkingen van persoonsgegevens gaat dan het meestal om een beperkt aantal persoonsge-

gevens dat betrekking heeft op bijvoorbeeld lidmaatschappen, arbeidsrelaties, klantrelaties en overeenkomstige relaties tussen een betrokkene en een organisatie. Voorbeelden van relaties waarover veelal persoonsgegevens worden verwerkt die vallen in deze klasse zijn: school - leerling, verhuurder - huurder, hotel - gast, vereniging - lid, organisatie - deelnemer. Opgemerkt wordt dat het lidmaatschap van een instelling op zich al informatie kan bevatten betreffende een persoon. Indien dit gegevens zijn die vallen onder de categorie bijzondere gegevens, bijvoorbeeld over politieke voorkeur, seksuele leven, kerkelijk genootschappen etc., dan moet het risico als hoog worden opgevat.

Hoog risico

De stand van de techniek, ontwikkelingen in de maatschappij en andere factoren kunnen van invloed zijn op de gevolgen die verlies of onrechtmatige verwerking van persoonsgegevens met zich mee kunnen brengen voor de betrokkenen. Onderstaande opsomming van categorieën van persoonsgegevens waar deze gevolgen ernstig kunnen zijn, is daarom niet uitputtend:

- Bijzondere persoonsgegevens zoals bedoeld in artikel 16 Wbp. Het gaat daarbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.
- Gegevens over de financiële of economische situatie van de betrokkene. Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden.
- (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene. Hieronder vallen bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen.
- Gegevens die betrekking hebben op mensen uit kwetsbare groepen. Het gaat hier bijvoorbeeld om mensen die te maken hebben met stalking of die in een blijf-vanmijn-lijfhuis verblijven, om klokkenluiders of om informanten van de politie of het Openbaar Ministerie.
- Gebruikersnamen, wachtwoorden en andere inloggegevens. De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens toegang toe geven.
- Gegevens die kunnen worden misbruikt voor (identiteits)fraude. Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het burgerservicenummer (bsn).

Behalve de aard van de verwerkte gegevens, kan ook de verwerking zelf risico's met zich meebrengen voor de betrokkenen. Factoren die een rol spelen zijn onder meer:

- Hoeveelheid verwerkte persoonsgegevens per persoon. Naarmate er per persoon meer persoonsgegevens worden verwerkt, kan verlies of onrechtmatige verwerking leiden tot een grotere inbreuk op de persoonlijke levenssfeer.
- Doel of doelen waarvoor de persoonsgegevens worden verwerkt. Naarmate de beslissingen die op basis van de verwerkte persoonsgegevens worden genomen ingrijpender zijn, is ook de impact van verlies of onrechtmatige verwerking groter.

Bijlage 3 Geraadpleegde bronnen

Rijksdienst voor Identiteitsgegevens, *Vragenlijst BRP 2015*, 2015.
Bureau Keteninformatisering Werk en Inkomen (e.a.), *Verantwoordingsrichtlijn GeVS / Normenkader GeVS*, 2011.
Bureau Keteninformatisering Werk en Inkomen, *De 7 Suwi-normen in relatie tot de normen uit de BIG*, 2014.
College Bescherming Persoonsgegevens, *CBP Richtsnoeren beveiliging van persoonsgegevens*, 2013.
Ernst & Young, *vragenlijst IT audit jaarrekening*, 2011.
Gemeente Bloemendaal, *Statuut informatiebeveiliging gemeente Bloemendaal*, 2008.
Gemeente Bussum, *Informatiebeveiligingsbeleid*, 2011
Gemeente Nijkerk, *Continuïteitsbeleid*, 2010.
Gemeente Wageningen, *Beveiligingsplan suwinet*, 2006.
Gemeente Wageningen, *Handboek Proces-audit Gemeentelijke basisadministratie persoonsgegevens (BRP) van de gemeente Wageningen*, 2010.
Gemeente Wageningen, *Integraal beveiligingsplan*, 2007.
Gemeente Wageningen, *Informatiebeleid*, 2012.
Gemeente Zeist, *Informatiebeveiligingsbeleid 2009-2011*, 2009.
Informatie Beveiligings Dienst, *Tactische baseline Nederlandse gemeenten*, 2014.
Informatie Beveiligings Dienst, *BEWERKERSOVEREENKOMST. Een van de producten van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)*, 2014.
Landelijk overleg van provinciale archiefinspecteurs, Werkverband gemeentelijke archiefinspectie, *Referentiekader Opbouw Digitaal Informatiebeheer (RODIN)*, 2010.
Logius, *Norm ICT-beveiligingsassessmentsDigiD*, 2012.
Ministerie van Justitie, *Handleiding voor verwerkers van persoonsgegevens*, 2002.
Ministerie van VROM, *Zelfcontrole kwaliteit. Kwaliteit van de BAG*, 2008.

Ministerie van VROM, *Kwaliteit van de basisregistraties adressen en gebouwen. Verdiepingsinformatie kwaliteit en de meting daarvan tijdens de toelatingsaudit*, 2010.
Nationaal Cyber Security Centrum, *ICT-beveiligingsrichtlijnen voor webapplicaties* (deel 1 en 2), 2012.
Nederlands Normalisatie-instituut, *Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging - Eisen (NEN-ISO/IEC 27001:2005 nl),* 2005.
Nederlands Normalisatie-instituut, *Informatietechnologie - Beveiligingstechnieken - Code voor informatiebeveiliging (NEN-ISO/IEC 27002:2007 nl)*, 2007.
Registratiekamer, *Beveiliging van persoonsgegevens*, 2001.
Rijksdienst voor Identiteitsgegevens, *Vragenlijst BRP 2015*, 2015.
Veiligheids- en gezondheidsregio Gelderland-midden, *risicoprofiel Gelderland-midden*, 2010.

Bijlage 4 Formulier uitzondering informatiebeveiligingsbeleid
Welke maatregel wordt niet of in beperkte vorm toegepast? (vermeld ook artikel nr.)
.....
Omschrijving uitzondering:
.....
Welke applicatie of informatiebron staat centraal?
.....
Wie is eigenaar van deze applicatie of informatiebron? (teammanager)
.....
Wat is het risico dat extra ontstaat door de uitzondering?
.....
Welke extra beveiligingsmaatregelen worden genomen om deze risico-toename te beperken?
.....
Naam en hand tekening
Teammanager (eigenaar)
.....
Betrokken beheerder(s) (huisvesting, applicatie, systeem)
.....