gemeente wageningen

Informatiebeveiligingsbeleid

Versie: besluit College 2014 9-9-2014
ID: 14INT01004

Inhoudsopgave

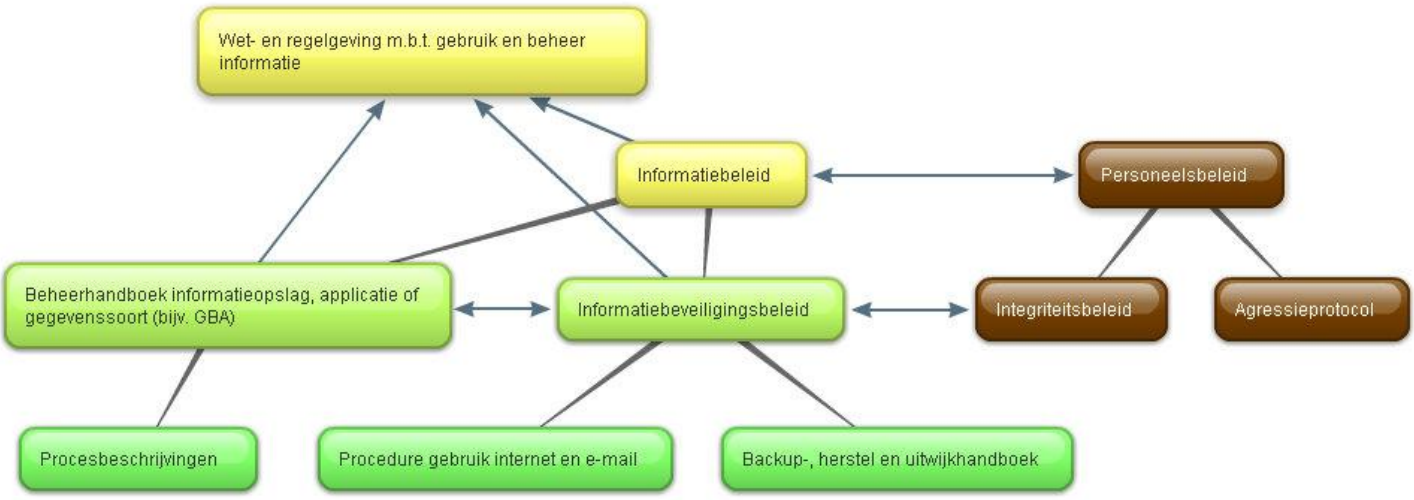
Inleiding

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 2013, en vervangt dat document dan ook. De aanpassingen hebben betrekking op maatregelen rond Suwinet (aangepaste kaders) en een verscherping/verduidelijking van maatregelen rond samenwerking met derden (risico-analyse). Daarnaast zijn de maatregelen uit de Baseline informatiebeveiliging gemeenten beoordeeld op wenselijkheid en uitvoerbaarheid. Hiermee is het beveiligingsplan voor Suwinet geïntegreerd in en vervangen door dit document.

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 is. 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 electriciteit (nutsvoorzieningen). De kans dat dit optreed is redelijk aanwezig (2% kans per jaar) [1].
- Natuurlijke verschijnselen als brand, oververhitting, rook en wateroverlast. De kans hierop is beperkt.

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 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;
- Fouten in programmatuur (applicaties, databases en koppelingen) die gegevens beïnvloeden.

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

[1] Veiligheids- en gezondheidsregio Gelderland-midden, Risicoprofiel Gelderland Midden, 2010.

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[2] 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 onderhevig zijn aan 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] Dit zijn onder meer (incl. onderliggende regelgeving):
- Grondwet (algemene eisen m.b.t. persoonlijke levenssfeer, briefgeheim)
- Wet Bescherming Persoonsgegevens (eisen m.b.t. bescherming persoonsgegevens)
- Auteurswet (eisen m.b.t. bescherming intellectueel eigendom)
- Telecommunicatiewet (eisen m.b.t. gebruik digitale media)
- Wet elektronische handtekeningen (eisen m.b.t. ondertekenen documenten)
- Archiefwet (eisen m.b.t. beschikbaarheid en integriteit documenten)
- Ambtenarenwet (art. 125a, lid 3: eis m.b.t. geheimhouding)
- Gemeentewet (art. 25, art. 55: eis m.b.t. geheimhouding)
- Wet Openbaarheid Bestuur (eisen m.b.t. vertrouwelijkheid informatie)
- Wet GBA (eisen m.b.t. kwaliteit gemeentelijke basisadministratie)
- Wet Suwi (eisen m.b.t. omgaan persoonsgegevens sociale keten)

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 telefoonlijn) 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 het netwerkverkeer van het eigen netwerk met andere netwerken, waaronder Internet, geldt het principe: alleen verkeer dat expliciet is toegestaan is mogelijk.

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 van de gemeente Wageningen;
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

Informatiebeveiliging is belangrijk. Principes, maatregelen en keuzes moeten gemaakt worden. Daarmee raakt het beleid de hele organisatie van de gemeente Wageningen. De verantwoordelijkheidsverdeling is erg belangrijk.

3.1 Verantwoordelijkheden rond informatiebeveiliging

1. Informatiebeveiliging is ieders verantwoordelijkheid. Er wordt van alle medewerkers 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 de beveiliging en de bedrijfscontinuïteit. De burgemeester draagt de bestuurlijk verantwoordelijkheid.
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 voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie. Deze eigenaar is altijd een teammanager.
4. Elke teammanager is verantwoordelijk voor de integrale informatiebeveiliging van zijn of haar organisatieonderdeel.
5. Applicatie-, systeem, facilitaire en archiefbeheerders zijn geen proceseigenaren maar zijn uitvoeringsverantwoordelijk voor een belangrijk deel van de informatiebeveiliging.
6. Taken, verantwoordelijkheden en bevoegdheden van medewerkers zijn zo geregeld dat medewerkers elkaars taken kunnen overnemen wanneer de continuïteit van informatievoorziening in gevaar komt.
7. Er zijn functiescheidingen en controle-mechanismes aangebracht in bedrijfskritische informatiesystemen, zoals tussen de systeem-, applicatiebeheer- en gebruikersorganisatie.
8. Er kunnen altijd uitzonderingen gemaakt worden op het informatiebeveiligingsbeleid. Dit moet in een wijzigingsoverleg besproken worden. Deze uitzonderingen worden vastgelegd in een formulier (zie bijlage) en ondertekend door de proceseigenaar.
9. Periodiek wordt de informatiebeveiliging van de gemeente Wageningen door een externe partij gecontroleerd. Deze brengt advies uit aan de gemeentesecretaris en de burgemeester.

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 servicedesk automatisering. Zij ondernemen naar aanleiding van dit incident actie. Team POJ kan, in overleg met de manager van de betrokken medewerk(st)er, vanwege deze schending het College van B&W adviseren om disciplinaire maatregelen te nemen. De teammanager van de betrokken medewerk(st)er kan dit in een functioneringsgesprek bespreken. Alle beveiligingsincidenten worden vastgelegd in een meldingsysteem.
5. Wanneer gevoelige gegevens in handen van derden gekomen is 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, 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.
2. Afspraken met externe partijen worden vastgelegd in een overeenkomst. Hierin is onder meer (indien van toepassing) opgenomen:
    a. De garantie van de leverancier dat de betrokken applicatie aan relevante wet- en regelgeving voldoet en dat gebleken afwijkingen of tekortkomingen in dit opzicht door de leverancier op zo kort mogelijke termijn zullen worden hersteld.
    b. De garantie van de leverancier dat het systeem bij toekomstige wijzigingen en uitbreidingen van relevante wet- en regelgeving binnen de kaders van het onderhoudscontract zal worden aangepast.
    c. Een beschrijving van beveiligingsmaatregelen die vereist zijn, dat deze door de externe partij zijn getroffen en worden nageleefd en dat beveiligingsincidenten onmiddellijk worden gerapporteerd.
    d. Bij structurele (geautomatiseerde) gegevensuitwisseling tussen de gemeente Wageningen en andere instanties, waarbij gebruik wordt gemaakt van intern opgeslagen gegevens, dient te worden vastgelegd onder wiens verantwoordelijkheid deze uitwisseling plaats vindt. 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.
3. Het naleven van de afspraken met externe partijen wordt gecontroleerd.

3.4 Specifieke verantwoordelijkheden rond Suwinet

1. Voor de informatiebron “Suwinet” is de eigenaar de teammanager Ondersteuning Samenleving. Deze eigenaar wordt “Security Officer” genoemd. Deze persoon is aangemeld bij BKWI.
2. De Security Officer voor Suwinet heeft de volgende taken: bevorderen en adviseren over de beveiliging van Suwinet, verzorgen van rapportages over de status van het gebruik van Suwinet, controleren dat m.b.t. de beveiliging van Suwinet de maatregelen worden nageleefd, evalueren van de uitkomsten en het doen van voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging van Suwinet. De Security Officer voor Suwinet rapporteert rechtstreeks aan het College, waarmee zowel naar de inhoudelijk verantwoordelijke voor het domein van werk en inkomen als naar de bestuurlijk verantwoordelijke voor informatiebeveiliging gerapporteerd wordt.

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 gebruikersnaam en een wachtwoord nodig die ze krijgen van het team Automatisering. De wachtwoorden zijn beveiligd en bestaan uit minimaal 8 posities met een combinatie van cijfers en letters. De wachtwoorden worden eens in de 60 dagen gewijzigd. Er is een controle dat het nieuw ingevoerde wachtwoord vergelijkt met het voorgaande wachtwoord. 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. 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).
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 stadhuis 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.
4. Toegangsrechten en autorisaties worden actief onderhouden en periodiek opgeschoond of inactief gezet. Bij ontslag en vertrek van een medewerker worden zijn/haar account en autorisaties direct geblokkeerd. Als twee maanden geen gebruik wordt gemaakt van autorisaties, doet de betrokken beheerder een melding aan de betrokken manager met de vraag of autorisaties ingetrokken kunnen worden. Naast accountgegevens worden ook gegevens in bijvoorbeeld mailboxen, verkenner-omgeving en inrichting van applicaties (bijv. workflows) opgeschoond.
5. De gemeente Wageningen analyseert periodiek het gebruik van informatiesystemen die gevoelige informatie zoals persoonsgegevens bevatten. Alle mutaties in persoonsgegevens worden gelogd. Het is mogelijk om verwerkte mutaties nogmaals te verwerken in geval van calamiteiten. Ook is het mogelijk om per periode de mutaties op te vragen voor reconstructie bij herstel.
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. 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 stadhuis 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.
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. Voor richtlijnen over 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 test-/ontwikkelomgeving 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. Het management ziet 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 (BPR) 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. Tenminste eenmaal per jaar wordt aan burgemeester en wethouders een managementrapport uitgebracht. Hierin wordt aangegeven in welke mate de gewenste garanties en waarborgen voor de BPR zijn bereikt.
6. 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.
7. 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.
2. Toegangsrechten voor Suwinet worden vastgelegd in een autorisatiematrix. Hierin wordt een relatie gelegd tussen gebruikersgroepen en specifieke functies in Suwinet.
3. Het aantal accounts waarbij gebruikers kunnen zoeken met meerdere zoeksleutels dan het BSN (zware autorisaties) is zeer beperkt (minder dan 20% van het totaal).

4. Nieuwe functionaliteiten binnen Suwinet worden na het beschikbaar komen actief uitgezet bij gebruikers van Suwinet en verwerkt in de autorisatiematrix.
5. Toegangsrechten worden maandelijks gecontroleerd. Deze controle wordt schriftelijk vastgelegd en gedeeld met de Security Officer voor Suwinet.
6. 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.
7. 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.
8. Het gebruik van Suwinet vindt slechts plaats via beveiligde verbindingen
9. Alleen verkeer uit het eigen netwerk van de Suwi-partij wordt via firewalls aangeboden aan het Suwi-Koppelpunt.
10. Bij koppelingen van de Suwi-partij aan de Suwinet-infrastructuur 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[3] 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, rapportages, 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.

[3] In document wordt gesproken van een nieuwe versie van een applicatie wanneer er voor de invoering ervan installatiewerkzaamheden nodig 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.
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.
GBA	Gemeentelijke Basisadministratie, nu ook wel Basisregistratie Personen genoemd (BRP)
Gebruiker	Iedere persoon of applicatie die op een of andere manier gebruik maakt van een informatiesysteem.
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.

Begrip	Uitleg/definitie
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.
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.

Bijlage 2 Overzicht bedrijfskritische en gevoelige informatiesystemen

Informatiesysteem	Afdeling	Belang/impact beschikbaarheid	Belang/impact integriteit	Belang/impact vertrouwelijkheid
Smartdocuments / Xential	Middelen	Zeer hoog	Zeer hoog	Zeer hoog
Corsa DMS	Middelen	Zeer hoog	Zeer hoog	Zeer hoog
Key2 Burgerzaken GBA	Samenleving	Zeer hoog	Zeer hoog	Zeer hoog
Basis netwerkinfrastructuur (VM-ware, oracle, platforms, filer)	Middelen	Zeer hoog	Zeer hoog	Zeer hoog
GBA extract Website	Middelen	Gemiddeld	Zeer hoog	Zeer hoog
PION/ADP	Middelen	Hoog	Zeer hoog	Zeer hoog
Key2Financiën	Middelen	Gemiddeld	Zeer hoog	Zeer hoog
HIS4all WOZ	Middelen	Hoog	Zeer hoog	Zeer hoog
GWS4all	Samenleving	Zeer hoog	Hoog	Zeer hoog
Verkeerssystemen	Ruimte	Hoog	Hoog	Zeer hoog
Key2 GBA-V	Samenleving	Gemiddeld	Hoog	Zeer hoog
Suwinet	Samenleving	Hoog	Hoog	Zeer hoog
DKD	Samenleving	Gemiddeld	Hoog	Zeer hoog
Key2 Datadistributie	Ruimte	Hoog	Laag	Zeer hoog
Key2 Parkeren	Middelen	Gemiddeld	Hoog	Zeer hoog
Key2 Begraven	Samenleving	Gemiddeld	Gemiddeld	Zeer hoog
Key2 Onderwijs	Samenleving	Hoog	Gemiddeld	Zeer hoog
Giskit BAG	Ruimte	Zeer hoog	Zeer hoog	Gemiddeld
Kas4all Betalingen	Samenleving	Hoog	Zeer hoog	Laag
Green Valley CMS/website	Middelen	Zeer hoog	Gemiddeld	Laag
Internet Explorer	Middelen	Zeer hoog	Laag	Laag

Bijlage 3 Risicoklassering persoonsgegevens

Risicoklasse 0: Publiek niveau

Het gaat hier om openbare persoonsgegevens. In deze klasse zijn persoonsgegevens opgenomen waarvan algemeen aanvaard is dat deze, bij het beoogde gebruik, geen risico opleveren voor de betrokkene. Voorbeelden hiervan zijn telefoonboeken, brochures, publieke internet sites etc. De persoonsgegevens behoeven ten aanzien van de exclusiviteit van de persoonsgegevens niet beter beveiligd te worden dan gebruikelijk is om een toereikende kwaliteit van de informatievoorziening tot stand te brengen en in stand te houden. Als gevolg van de Wet bescherming persoonsgegevens worden voor deze risicoklasse geen extra eisen ten aanzien van de beveiliging gesteld dan welke al noodzakelijk zijn voor een zorgvuldige bedrijfsvoering.

Risicoklasse I: Basis niveau

De risico's voor de betrokkene bij verlies of onbevoegd of onzorgvuldig gebruik van de persoonsgegevens zijn zodanig dat standaard (informatie)beveiligingsmaatregelen toereikend zijn. Bij verwerkingen van persoonsgegevens in deze klasse gaat het meestal om een beperkt aantal persoonsgegevens 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 dient de beveiliging van persoonsgegevens tenminste te worden ondergebracht in risicoklasse II.

Risicoklasse II: Verhoogd risico

De uitkomst van de analyse toont aan dat er extra negatieve gevolgen bestaan voor de betrokkene bij verlies, onbehoorlijke of onzorgvuldige verwerking van de persoonsgegevens. De te nemen (informatie)beveiligingsmaatregelen moeten voldoen aan hogere normen dan die gelden voor het basis niveau. In deze klasse passen bijvoorbeeld verwerkingen van persoonsgegevens die voldoen aan een van de hieronder gegeven beschrijvingen:

1. de verwerkingen van bijzondere persoonsgegevens zoals bedoeld in artikel 16 WBP;
2. de verwerking in het bank- en verzekeringswezen van gegevens over de persoonlijke of economische situatie van een betrokkene;
3. de gegevens die bij handelsinformatiebureaus worden verwerkt ten behoeve van kredietinformatie of schuldsanering;
4. de gegevens die worden verwerkt hebben betrekking op de gehele of grote delen van de bevolking (de impact van op zich onschuldige gegevens over een groot aantal betrokkene);

Soms moet de verwerking van bijzondere gegevens vanwege een hoge gevoeligheidsgraad in het maatschappelijk verkeer, bijvoorbeeld wanneer het gegevens over levensbedreigende ziektes betreft, ondergebracht worden in risicoklasse III.

Risicoklasse III: Hoog risico

Bij verwerking van meerdere verzamelingen van bijzondere persoonsgegevens kan het resultaat van deze verwerking een dermate vergroot risico voor de betrokkene opleveren dat het gerechtvaardigd is deze verwerking van persoonsgegevens in risicoklasse III te plaatsen. De maatregelen die voor de beveiliging van dergelijke persoonsgegevens moeten worden genomen, moeten voldoen aan de hoogste normen. De verwerking van persoonsgegevens die in deze klasse passen zijn onder andere de verwerkingen die betrekking hebben op opsporingsdiensten met bijzondere bevoegdheden of verwerkingen waarbij de belangen van de betrokkene ernstig kunnen worden geschaad indien dit onzorgvuldig of onbevoegd geschiedt. Bijzondere verwerkingen van persoonsgegevens, bijvoorbeeld een DNA-databank, vallen in deze klasse. Daarnaast valt de verwerking van persoonsgegevens waarop een bijzondere geheimhoudingsplicht van toepassing is binnen deze klasse.

Bijlage 4 Geïnterviewde personen

Compleet nieuwe versie 2013

- Marijke Verstappen (gemeentesecretaris)
- Jan Verwoert (teammanager Publiekszaken)
- Thomas Beke (teammanager Ondersteuning Samenleving)
- Rob de Vries (teammanager Vergunningverlening en Handhaving)
- Karin Jeuken (teammanager Automatisering)
- Wim Aartse (teammanager Informatiemanagement)
- Richard van Vliet (teammanager Ingenieursbureau)
- Hans Rothuis (teammanager Facilitair Management)
- Harry Post (lid ondernemingsraad)
- Lindsay Hooyer (lid ondernemingsraad)
- Mira Faber (lid ondernemingsraad)
- Maartje Gewin (integriteitscoördinator)
- Lily Mujica (systeembeheerder)
- Michel Voorderhake (systeembeheerder)
- Peter van der Laan (applicatie- en gegevensbeheerder GBA)
- Paulisca van Telgen-Vreeke (BAG-beheerder, applicatiebeheerder datadistributie)
- Henri Berends (applicatiebeheerder Sociale Zaken)
- Theo ter Maat (applicatiebeheerder Sociale Zaken)
- Michiel van Velp (proces- en applicatiebeheerder Midoffice)
- Arie van der Klift (proces- en applicatiebeheerder Midoffice)
- Woutera Susebeek (coördinator WOZ)
- Fred van Wijk (proces- en applicatiebeheerder financiële applicaties)
- Jörgen Willemsen (applicatiebeheerder CMS/website)
- Bob Kernkamp (gemeentearchivaris)
- Khalid Sultani (applicatiebeheerder team Ingenieursbureau)
- André Kok (applicatiebeheerder verkeerssystemen)
- Paul Quint (facilitair beheerder/bode)
- Rudolf van Geffen (facilitair beheerder/bode)

Actualisatie 2014

- Michel Voorderhake (systeembeheerder)
- Lily Mujica (systeembeheerder)
- Henri Berends (applicatiebeheerder sociaal domein)
- Theo ter Maat (applicatiebeheerder sociaal domein)
- Peter van der Laan (applicatie- en gegevensbeheerder GBA)
- Maartje Gewin (integriteitscoördinator)
- Cynthia van der Roest (inkoopadviseur)

Bijlage 5 Geraadpleegde bronnen

Agentschap BPR, *Vragenlijst procesdeel audit GBA (Bijlage 2)*, 2007.

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.

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 (GBA) 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.

Landelijk overleg van provinciale archiefinspecteurs, Werkverband gemeentelijke archiefinspectie, *Referentiekader Opbouw Digitaal Informatiebeheer (RODIN)*, 2010.

Logius, *Norm ICT-beveiligingsassessments DigiD*, 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.

Veiligheids- en gezondheidsregio Gelderland-midden, *risicoprofiel Gelderland-midden*, 2010.

Bijlage 6 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 handtekening

Teammanager (eigenaar)

……

Betrokken beheerder(s) (huisvesting, applicatie, systeem)

……