# Context informatiebeveiligingsplan GBA

# Inleiding

Informatiebeveiliging is voor de gemeente Laren van groot belang. De processen bij de gemeente worden in hoge mate ondersteund door informatiesystemen. De gegevens die binnen de gemeente en in informatiesystemen worden verwerkt zijn divers van aard en van gevoeligheid. De gegevens die worden geraadpleegd in en worden verwerkt ten behoeve van de GBA kenmerken zich door een hoge mate van gevoeligheid. Mede hierdoor is het noodzakelijk dat die verwerkingen tegen onjuistheid, onvolledigheid, kennisname door onbevoegden en/of uitval van het informatiesysteem worden beveiligd.

Onjuiste en/of onvolledige informatie, misbruik van informatie of een informatielek kan in het geval van de GBA grote negatieve consequenties hebben. Het kan leiden tot imagoverlies van de gemeente, tot een breuk in het vertrouwen dat burgers mogen stellen in een lagere overheid aan wie zij gegevens ter beschikking (moeten) stellen. Ook kan het een probleem opleveren indien de burgers foutieve informatie ontvangen, hetgeen zelfs kan leiden tot claims.

Voorts is de continuïteit van de gegevensverwerking van de GBA van belang. Op het moment dat de GBA-applicatie om wat voor reden dan ook niet beschikbaar is, mist de gemeente een belangrijke bron met basisgegevens, die noodzakelijk is voor de uitvoering van de dagelijkse processen binnen de gemeente. Een mogelijk gevolg is dat processen stagneren.

Bovenstaande overwegingen alsmede wettelijke bepalingen (waaronder Wet op de Gemeentelijke Basis Administratie, de Wet Bescherming Persoonsgegevens, de Paspoort Uitvoeringsregeling Nederland 2001) en uitvoeringsvoorschriften hebben ertoe geleid dat de gemeente Laren ter zake een beleid en procedures heeft opgesteld alsmede maatregelen treft met betrekking tot de beveiliging van informatie.

# Opbouw informatiebeveiligingsplan GBA

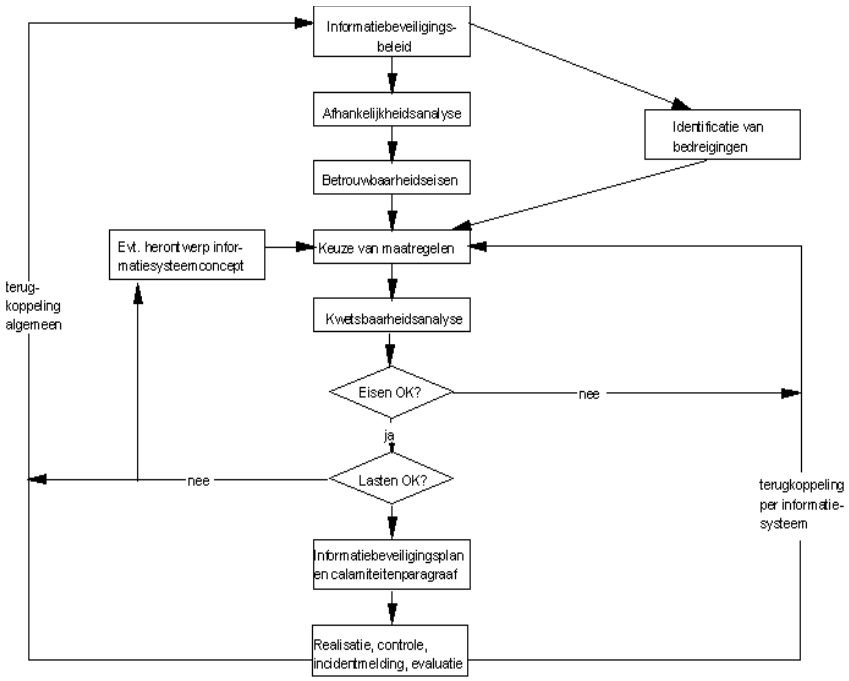
Het informatiebeveiligingsplan GBA kent de volgende opbouw:

- Aanleiding en vaststelling informatiebeveiligingsplan GBA
- Context
  - Toelichting gehanteerde methodiek
  - Totstandkoming en onderhoud beveiligingsplan
  - Voorlichting en verspreiding
- Informatiebeveiligingsplan GBA
  - Relevante processen en informatiesystemen

- Gestelde betrouwbaarheidseisen
- Componenten van het informatiesysteem
- Bedreigingen en gerelateerde betrouwbaarheidscriteria
- Gewenste maatregelen
  - Reeds getroffen
  - Nog te treffen
  - Implementatieplan en prioriteitenstelling.

# Toelichting gehanteerde methodiek

Voor het opstellen van het informatiebeveiligingsplan GBA is gebruik gemaakt van de Afhankelijkheids- en Kwetsbaarheidsanalyse (A&K-analyse). Het ACIB (Advies en Coördinatiepunt Informatiebeveiliging van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties) heeft een methode ontwikkeld om A&K-analyses uit te voeren. De hoofdlijn van de A&K-analyse wordt onderstaand schematisch afgebeeld:




Het informatiebeveiligingsbeleid voor de gemeente Laren is vastgesteld en geeft opdracht tot het opstellen van informatiebeveiligingsplannen, zo ook voor de GBA. Door de uitvoering van een afhankelijkheidsanalyse kan worden bepaald welke betrouwbaarheidseisen dienen te worden gesteld voor de informatiesystemen en verantwoordelijkheidsgebieden. Daarnaast wordt vastgesteld welke bedreigingen het

bereiken van de primaire doelstellingen van de processen in de weg staan. Aan de hand van de betrouwbaarheidseisen en de relevante bedreigingen wordt vervolgens de ideaalsituatie bepaald (waarin alle geïdentificeerde maatregelen zijn opgenomen). Vervolgens wordt met de mix van maatregelen beoordeeld of aan de eisen is voldaan. Ook het kostenaspect wordt hierbij in overweging genomen, daar de baten op moeten wegen tegen de lasten. Op basis van deze vergelijking kan het nodig blijken andere maatregelen te treffen waarmee het proces zich herhaalt. Tenslotte worden de maatregelen definitief gekozen, waarbij een deel reeds zal zijn getroffen en een ander deel nog dient te worden geïmplementeerd. Het overzicht met getroffen en nog te treffen maatregelen krijgt vervolgens de weerslag in een informatiebeveiligingsplan. Daarbij worden verantwoordelijkheden en prioriteiten duidelijk aangemerkt. Tenslotte dienen de nog niet getroffen maatregelen te worden geïmplementeerd en gecontroleerd.

***Belangrijk om daarbij te realiseren is dat het informatiebeveiligingsplan GBA geen statisch document is. Voortdurend wijzigende omstandigheden, door bijvoorbeeld ontwikkelingen in dienstverlening, in techniek of in bedreigingen nopen ertoe de actualiteit van het beveiligingsplan GBA te handhaven. Hiertoe dient periodieke bewaking en evaluatie plaats te vinden (zie ook volgende paragraaf).***

# Totstandkoming, periodieke evaluatie en onderhoud

Het informatiebeveiligingsplan GBA van de gemeente Laren is zoals gezegd geen statisch document. De werking van het beveiligingsbeleid en de maatregelen en procedures dienen periodiek te worden bewaakt en geëvalueerd. Ervaringen met de uitvoering van beveiligingsmaatregelen, gewijzigde omstandigheden of incidenten kunnen aanleiding vormen het informatiebeveiligingsplan bij te stellen. De actualiteit van het informatiebeveiligingsplan GBA valt onder de directe verantwoordelijkheid van de Afdelingsmanager Publiek, Vergunningverlening en Handhaving. Deze zal daartoe minimaal één keer per jaar (en voorts op elk moment dat daar aanleiding toe is) het informatiebeveiligingsplan GBA integraal met alle direct betrokkenen evalueren en alle noodzakelijke corrigerende en aanvullende acties treffen. De afdelingsmanager Publiek, Vergunningverlening en Handhaving legt hierover schriftelijk verantwoording af aan het College B&W.

Bij de periodieke evaluatie wordt het beveiligingsplan GBA stapsgewijs doorlopen waarmee de actualiteit van de in het plan opgenomen A&K-analyse kan worden vastgesteld. Eventueel gewijzigde omstandigheden leiden tot een minder of meer ingrijpende aanpassing in de A&K-analyse. Door het (gedeeltelijk) opnieuw uitvoeren van de A&K-analyse (conform de bovenstaande figuur) kunnen oude maatregelen overbodig worden of nieuwe gewenst zijn, hetgeen zich dan dient te vertalen in een aangepast informatiebeveiligingsplan GBA en communicatie naar alle

betrokkenen met en verantwoordelijken voor de uitvoering. De periodieke evaluatie vindt plaats in een vergadervorm op initiatief van de Informatiebeheerder.
Bij de periodieke evaluatie zijn de navolgende personen betrokken:

1. Applicatiebeheerder GBA
2. Informatiebeheerder en Privacybeheerder
3. Systeembeheerder
4. Beveiligingsbeheerder
5. Medewerker beheer gebouwen
6. Eventueel een externe deskundige

# Verspreiding en voorlichting

Het informatiebeveiligingsplan GBA zal worden ondergebracht bij de beveiligingsbeheerder. Het informatiebeveiligingsplan valt onder permanente verantwoordelijkheid van de Afdelingsmanager Publiek, Vergunningverlening en Handhaving. Zorg dient te worden gedragen voor het onderhoud van het informatiebeveiligingsplan (zie vorige paragraaf). Daarnaast zal de meest recente versie van het Informatiebeveiligingsplan GBA na iedere wijziging aan de beveiligingsbeheerder worden verstrekt, zodat deze periodiek onafhankelijk de actualiteit van het informatiebeveiligingsplan kan toetsen.

Essentieel voor een adequaat functionerende informatiebeveiliging is het beveiligingsbewustzijn van medewerkers. Medewerkers zijn een, zo niet de, cruciale factor bij de realisatie en handhaving van het gewenste niveau van de informatiebeveiliging. Het is dan ook essentieel dat medewerkers zich bewust zijn van de risico's die het bezit en gebruik van bepaalde informatie met zich meebrengt en dat ze begrijpen dat het nodig is de in dit plan voorgestelde maatregelen en procedures te moeten volgen in het kader van de adequate beveiliging van de informatie waarmee ze dagelijks in aanraking komen.

Maar ook hier geldt, evenals voor het onderhoud van het Informatiebeveiligingsplan dat het beveiligingsbewustzijn van medewerkers "onderhouden" - dat wil zeggen blijvend – dient te worden bevorderd. Er wordt in voorzien dat tenminste jaarlijks op enig moment speciale aandacht wordt besteed aan informatiebeveiliging in het algemeen en specifiek voor de GBA of zoveel eerder of vaker als daar op grond van feiten aanleiding toe is.

Communicatie inzake informatiebeveiligingsbeleid, informatiebeveiligingsplan GBA en de daarin opgenomen maatregelen richting de medewerkers vindt plaats middels een gezamenlijke jaarlijkse sessie ‘beveiligingsbewustzijn’ waarbij aanwezigheid verplicht is. In deze sessie zal een toelichting worden gegeven op informatiebeveiliging in het algemeen, het informatiebeveiligingsplan GBA en de in dat kader getroffen en te treffen maatregelen en de consequenties die dat heeft voor de betrokken medewerkers. Deze sessie zal worden verzorgd door De afdelingsmanager Publiek, Vergunningverlening en Handhaving tezamen met de beveiligingsbeheerder en medewerkers van de team I&A, eventueel aangevuld met externe deskundigen. De coördinatie en verantwoordelijkheid hiervoor zijn in handen van de Afdelingsmanager Publiek, Vergunningverlening en Handhaving.

# Informatiebeveiligingsplan GBA

In de volgende paragrafen worden stapsgewijs de belangrijkste resultaten van de A&K-analyse weergegeven. De belangrijkste stappen uit het eerder gepresenteerde schema worden nader uitgewerkt. Hiermee resulteert het feitelijke beveiligingsplan GBA waarin door een logisch redeneerproces niet alleen de getroffen maar ook de nog te treffen maatregelen worden geïnventariseerd. Aan de nog te treffen beveiligingsmaatregelen wordt een verantwoordelijke, een prioriteit en een expliciet en taakstellend implementatietijdpad gekoppeld, opdat maatregelen ook daadwerkelijk worden geïmplementeerd.

## Beschrijving processen, informatiesystemen, verantwoordelijkheidsgebieden en relaties

Voor het informatiebeveiligingsplan GBA zijn de GBA-processen voor de gemeente Laren geïnventariseerd en is een clustering aangebracht in vergelijkbare processen vanuit het oogpunt van informatiebeveiliging. Daarbij zijn de volgende clusters geïdentificeerd:

- Processen met betrekking tot de burgerlijke stand;
- Processen met betrekking tot verstrekking officiële documenten;
- Frontoffice processen GBA;
- Backoffice processen GBA;
- Binnengemeentelijke on-line GBA gegevensverstrekking.

Deze worden hieronder kort toegelicht.

*Processen met betrekking tot de burgerlijke stand*
Het betreft hier processen waarbij de GBA-applicatie feitelijk onontbeerlijk is, enerzijds om gegevens te controleren en anderzijds om aktes op te kunnen stellen. Het betreft veelal directe klantcontacten waarbij GBA gegevens dienen te worden gecontroleerd en direct aktes worden opgemaakt. Het niet beschikbaar zijn van de GBA-applicatie bemoeilijkt een betrouwbare uitvoering van deze processen aanzienlijk. Voorbeelden zijn geboorte, erkenningen, huwelijk en geregistreerd partnerschap en ontbinden daarvan, adoptie en overlijden.

*Processen met betrekking tot de verstrekking van officiële documenten*
Het betreft hier processen waar burgers aan de balie komen om documenten aan te vragen. Hierbij kan worden gedacht aan rijbewijzen, reisdocumenten, gegevensverstrekkingen GBA en verklaringen omtrent gedrag. Het niet beschikbaar zijn van de GBA-applicatie maakt een directe uitvoering van deze processen onmogelijk. Het is echter wel zo dat klanten veelal kunnen worden gevraagd op een later tijdstip terug te komen om de officiële documenten af te komen halen zonder dat dit direct tot problemen hoeft te leiden. Vanuit imago-overwegingen (de betrouwbare overheid) is dat echter zeer onwenselijk.

*Processen met betrekking tot de frontoffice verwerking GBA*
Het betreft hier processen waarbij burgers aan de balie komen en waarbij direct een controle op de identiteit van de betrokkene wordt uitgevoerd. Daarnaast worden brondocumenten ingenomen van burgers en wordt beoordeeld in hoeverre deze volledig zijn in de informatie die ze verstrekken. De GBA-applicatie wordt hierbij met name benut voor het inzien en controleren van de gegevens van de betrokkene, mutaties vinden in zeer beperkte mate plaats. Voorbeelden zijn verzoeken om geheimhouding en naamsaanduiding en aangiften van verhuizing.

*Processen met betrekking tot de backoffice verwerking GBA*
Het betreft hier processen waarbij mutaties in de GBA in de backoffice worden verwerkt. Denk hierbij bijvoorbeeld aan adreswijzigingen. Het niet beschikbaar zijn van de GBA-applicatie maakt uitvoering van deze processen onmogelijk, maar gezien het feit dat er geen direct klantcontact is en de mogelijkheid bestaat de verwerking enige tijd op te schorten is het tijdelijk (maximaal 48 uur) niet beschikbaar zijn van de GBA-applicatie voor de uitvoering van deze processen acceptabel. Als onderdeel van de back-office processen bij de gemeente Laren is ook het samenstellen van gegevens voor verkiezingen (stemgerechtigden en oproepen) van groot belang, alsmede het berichtenverkeer.

*Processen met betrekking tot interne on-line verstrekkingen GBA*
Het betreft hier processen waarbij andere afdelingen / teams dan het team Burgerzaken gebruik maken van de GBA-applicatie om gegevens on-line te kunnen inzien. Voor de meest betrouwbare taakuitoefening is dat noodzakelijk. Het niet beschikbaar zijn van de GBA-applicatie leidt ertoe dat deze afdelingen hun taken (deels) niet kunnen uitvoeren of op moeten schorten. De GBA-applicatie vormt een belangrijke ondersteunende rol bij de processen van andere afdelingen.

Alle hierboven genoemde processen hebben vanzelfsprekend een sterke relatie met de ter zake doende wetgeving en worden uitgevoerd door het team Burgerzaken onder directe verantwoordelijkheid van Afdelingshoofd Publiek, Vergunningverlening en Handhaving.

Binnen het team Burgerzaken bestaat een drietal functies, te weten Teamleider Publiekszaken, Vakspecialist A en Medewerker Publieke Dienstverlening.

De standaard kantoorautomatisering van de gemeente Laren draagt zorg voor de reguliere ondersteuning op gebied van tekstverwerking, rekenkundige verwerkingen, interne en externe communicatie. Het gaat hierbij om de volgende applicaties:
- MS-office (Word, Excel, Access, Powerpoint, Outlook);
- Internet-browser;
- Tijdregistratie.

Deze kantoorautomatisering is aanwezig op alle standaardwerkplekken bij het team Burgerzaken. Functionele ondersteuning op het gebied van de kantoorautomatisering op de werkplekken vindt plaats door de helpdesk.

De belangrijkste applicaties voor het team Burgerzaken ter ondersteuning van de GBA-activiteiten zijn meegenomen in de A&K-analyse en worden hieronder weergegeven:

| Afdeling | Deel processen GBA | Informatiesysteem | Verantwoordelijk-heidsgebied |
|---|---|---|---|
| Handhaving, Vergunningverlening en Publiek, team burgerzaken | Burgerlijke stand processen<br>Frontoffice processen | Cipers<br>(modules burgerlijke stand, reisdocumenten, rijbewijzen, BRS, Covog (VoG), datacommunicatie)<br>(kassiersfunctie door middel van losstaande kassa) | team I&A (gemeenschappelijke IT infrastructuur) |
| | Verstrekking officiële documenten | | |
| | Backoffice processen | | |
| | Biunengemeentelijke online verstrekkingen GBA | | |
| | | Fysieke toegang | Afdeling Staf en Ondersteuning |

Hierbij wordt onder een verantwoordelijkheidsgebied verstaan een geheel aan voorzieningen dat ter beschikking staat aan één of meerdere informatiesystemen en waarvoor de verantwoordelijkheid eenduidig is toe te kennen aan één organisatorische eenheid.

In het kader van de afhankelijkheidsanalyse dient te worden bepaald wat het belang is van de hierboven beschreven processclusters en informatiesystemen. Het belang van de processen en ondersteunende informatiesystemen is als volgt te typeren, waarbij voor een uitleg van de typeringen wordt verwezen naar de bijlage:

| **Processcluster GBA** | **Typering processcluster** | **Typering informatiesysteem** |
|---|---|---|
| Burgerlijke stand processen | ***Kritisch Strategisch*** | ***Vitaal*** |
| Verstrekkingen officiële documenten | ***Kritisch Strategisch*** | ***Vitaal*** |
| Frontoffice processen GBA | ***Kritisch Strategisch*** | ***Vitaal*** |
| Backoffice processen GBA | ***Kritisch Strategisch*** | ***Vitaal*** |
| Binnengemeentelijke GBA verstrekkingen | ***Strategisch*** | ***Vitaal*** |

# Beschrijving componentgroepen en componenten

Een informatiesysteem is op te delen in een aantal componentgroepen. Deze componentgroepen zullen later in de kwetsbaarheidsanalyse worden geconfronteerd met mogelijke dreigingen. Nadat is

vastgesteld welke dreigingen relevant zijn, kunnen mogelijke maatregelen worden geformuleerd. Deze maatregelen sluiten ook weer aan op de componentgroepen. Onderstaande tabel geeft een globaal overzicht van de componenten voor het informatiesysteem voor de GBA.

| **Gemeente Laren: Informatiebeveiligingsplan GBA** | | |
|---|---|---|
| | **Benoemde componenten** | **Beschrijving** |
| **1.** | **Mensen/Organisatie** | |
| | - Beveiligingsfunctionaris | Dhr. G. van Laar |
| | - Netwerkbeheerder,- Systeembeheerder | Dhr. R. van Midde |
| | - Helpdeskmedewerker | Mw. V. van der Zwaan |
| | - Applicatiebeheerder GBA | Mw. M. Rigter-Roodhart |
| | - Hoofd team Burgerzaken | Mw. I. Walet |
| | - Afdelingshoofd Publiek, Vergunningverlening en Handhaving | Ir. P. van Dijk |
| | | |
| **2.** | **Apparatuur** | |
| | - PC's | Wyse TC 010 (11x)<br>IBM Thinkpad mod 8183 (1x) |
| | - Servers | VMWARE ESX 3x |
| | - Printers | HP4250<br>HP 4551 (3x) |
| | - Data- en telecommunicatiecomponenten: routers, hubs, gateways etc*)* | HP Pro Curve<br>Cisco<br>Mitel |
| **3.** | **Programmatuur** | |
| | - Besturingssysteem | Windows 2003 |
| | - Applicaties | Cipers, kantoorautomatisering |
| | - Beheertools (bijvoorbeeld HP Openview, NT 4.0, Oracle Enterprise Manager, CA-AMO, Wininstall, Support Magic) | MS SCCM<br>PRTG<br>OP manager<br>Cisco View<br>Procurvemanager<br>RDP |
| **4.** | **Gegevens (dragers)** | |
| | - Database | DB2 |
| | - Dossiers | Bewaard op harde schijf en fysieke dossiers is kluis op afdeling burgerzaken |
| | - Tapes / diskettes / CD's | Tapes voor back up<br>CD Rom voor incidentele uitwisseling |
| **5.** | **Omgeving** | |
| | - Gebouw (wellicht meerdere) | Gegevensverwerking ten behoeve van de GBA vindt plaats in het BEL kantoor, Zuidersingel 5 te Eemnes |
| | - Werkplek | Frontoffice, Backoffice |
| | - Computerruimte | Afgesloten, beveiligde ruimte voorzien van relevante maatregelen |

| | | |
|---|---|---|
| | - Opslagruimte back-ups | De back up tapes worden bewaard in een inbraakwerende kluis op de gemeentewerf. |
| **6.** | **Diensten** | |
| | - Onderhoudscontract (Hard- en Software) | AS400 wordt uitbesteed aan Uphantis |
| | - Klimaatbeheersing | Airco / klimaatbeheersing aanwezig in computerruimte |
| | - Schoonmaak | Schoonmakers kunnen alleen op Burgerzaken komen indien er een medewerker aanwezig is. Het toegangspasje van de schoonmakers, geeft geen toegang tot burgerzaken |
| | - Bewaking | Anders dan de bewaking voor het gebouw zijn er geen extra maatregelen genomen |
| | - Papiervernietiging | Papiervernietiging vindt plaats door een gespecialiseerd bedrijf, op de afdeling staat een speciale papiercontainer, deze container is voorzien van een brievenbus met goot en is niet te openen. |
| | - Vervoer back up | De back up tapes worden vervoerd tussen serverruimte en gemeentewerf |

# Betrouwbaarheidseisen

De afdelingsmanager Publiek, Vergunningverlening en Handhaving heeft bepaald welke eisen dienen te worden gesteld aan de beschikbaarheid, exclusiviteit en integriteit voor de informatiesystemen en verantwoordelijkheidsgebieden welke onderdeel uitmaken van de GBA-processen. Onderstaande tabel geeft deze eisen weer. Voor een verklaring van de gehanteerde begrippen wordt verwezen naar de bijlage.

| Procescluster GBA | Beschikbaarheid | Exclusiviteit | Integriteit |
|---|---|---|---|
| Burgerlijke stand processen | ***Essentieel*** | ***Essentieel*** | ***Essentieel*** |
| Verstrekkingen officiële documenten | ***Essentieel*** | ***Essentieel*** | ***Essentieel*** |
| Frontoffice processen GBA | ***Essentieel*** | ***Essentieel*** | ***Essentieel*** |
| Backoffice processen GBA | ***Belangrijk*** | ***Essentieel*** | ***Essentieel*** |
| Binnengemeentelijke GBA verstrekkingen | ***Belangrijk*** | ***Essentieel*** | ***Essentieel*** |

# Bedreigingen

Per componentgroep zijn de bedreigingen geïnventariseerd, waarbij eveneens wordt aangegeven of het een bedreiging vormt voor de beschikbaarheid, exclusiviteit of integriteit. Daarnaast wordt de ernst/schade van de gevolgen aangegeven (hoog, midden, laag). De laatste kolom geeft aan of de dreiging zonder verdere maatregelen wordt geaccepteerd, dus feitelijk acceptabel is. Is dat het geval, dan is er sprake van een niet-relevante dreiging en deze zal in het vervolg dan ook niet verder worden meegenomen.

| **Bedreigingen (Per componentgroep)** | | **BEI-eisen** | | | **Ernst/ Schade** | | | **Nr.** | **Accep-tabel** |
|---|---|---|---|---|---|---|---|---|---|
| Mensen | Incident | B | E | I | H | M | L | Nr. | Ja/ Nee |
| Wegvallen | Voorzienbaar (ontslag, vakantie) | X | | | | | X | 1 | Nee |
| | Onvoorzienbaar (ziekte, ongeval, staking) | X | | | | X | | 2 | Nee |
| Onopzettelijk foutieve handelingen | Onkunde, slordigheid, stress | X | X | X | X | | | 3 | Nee |
| | Foutieve procedures | | | X | X | | | 4 | Nee |
| | Complexe foutgevoelige bediening | X | | | | | X | 5 | Nee |
| | Onzorgvuldige omgang met passwords | | X | X | X | | | 6 | Nee |
| Opzettelijke foutieve handelingen | Niet in acht nemen van voorschriften/procedures | | X | X | X | | | 7 | Nee |
| | Fraude/diefstal | | X | X | X | | | 8 | Nee |
| | Ongeautoriseerde toegang | | X | X | X | | | 9 | Nee |
| Apparatuur | Incident | B | E | I | H | M | L | - | Ja/ Nee |
| Spontaan technisch falen | Veroudering/slijtage | X | | X | X | | | 10 | Nee |
| | Storing | X | | X | X | | | 11 | Nee |
| | Ontwerp-, fabricage-, installatie-, onderhoudsfouten | X | | | X | | | 12 | Nee |
| Technisch falen door externe invloeden | Spanningsschommelingen | X | | X | X | | | 13 | Nee |
| | Te hoge/lage temperatuur/vochtigheid | X | | X | X | | | 14 | Nee |
| | Vuil/stof | X | | X | X | | | 15 | Nee |
| | Elektromagnetische straling | X | | X | X | | | 16 | Nee |
| | Elektrostatische lading | X | | X | X | | | 17 | Nee |
| | Diefstal | X | | | X | | | 18 | Nee |
| Menselijk handelen | Bedieningsfouten | X | | X | X | | | 19 | Nee |
| | Opzettelijke functionele aanpassing/sabotage | X | X | X | X | | | 20 | Nee |
| | Beschadiging/vernieling | X | | X | X | | | 21 | Nee |
| | Diefstal | X | X | | X | | | 22 | Nee |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Ontbrekende toebehoren | X | | | | X | | 23 | Nee |
| Programmatuur | Incident | B | E | I | H | M | L | - | Ja/ Nee |
| Nalatig menselijk handelen | Ontwerp-, programmeer-, implementatie-, onderhoudsfouten | X | | X | X | | | 24 | Nee |
| | Introductie van virus e.d. door gebruik van ongescreende programma's | X | | X | X | | | 25 | Nee |
| | Gebruik van de verkeerde versie van programmatuur | | | X | X | | | 26 | Nee |
| | Slechte documentatie | X | | X | X | | | 27 | Nee |
| Opzettelijk menselijk handelen | Manipulatie voor of na ingebruikname | X | X | X | X | | | 28 | Nee |
| | (ongeautoriseerde) functieverandering en/of toevoeging | | | X | | X | | 29 | Nee |
| | Introductie van virussen, Trojaanse paarden e.d. | X | | X | X | | | 30 | Nee |
| | Illegaal kopiëren van programmatuur | | | X | | X | | 31 | Nee |
| | Diefstal of privé-gebruik van programmatuur | X | | | | X | | 32 | Nee |
| Technische fouten/mankementen | Fouten in programmatuur | X | | X | X | | | 33 | Nee |
| | Malicious code / Trojaanse paarden in programmatuur | X | | X | X | | | 34 | Nee |
| Gegevens (verzamelingen) | Incident | B | E | I | H | M | L | - | Ja/ Nee |
| Via gegevensdragers | Diefstal/zoekraken | X | X | | X | | | 35 | Nee |
| | Beschadiging door vuur, water, vochtigheid, ontmagnetisering, verkeerde behandeling | X | | X | X | | | 36 | Nee |
| | Incompatible formats | | | X | X | | | 37 | Nee |
| | Foutieve ver- of ontsleuteling | | | X | X | | | 38 | Nee |
| | Foutieve of vervalste identificatie | | X | | X | | | 39 | Nee |
| Via apparatuur | Fysieke schrijf- of leesfouten | | | X | X | | | 40 | Nee |
| | Fouten in interne geheugens | | | X | X | | | 41 | Nee |
| Via programmatuur | Foutieve of gemanipuleerde programmatuur | X | X | X | X | | | 42 | Nee |
| | Doorwerking van virussen | X | X | X | X | | | 43 | Nee |
| | Afbreken van verwerking | X | | X | X | | | 44 | Nee |
| Via personen | Foutieve gegevensinvoer, -verandering of –verwijdering (wel/niet opzettelijk, wel/niet bevoegde medewerkers) | | | X | X | | | 45 | Nee |
| | Illegaal kopiëren van gegevens | | X | | X | | | 46 | Nee |
| | Meelezen zichtbare invoer en uitvoer (printer, beeldscherm) | | X | | X | | | 47 | Nee |
| | Uitlezen elektromagnetische straling | | X | | X | | | 48 | Nee |
| | Onzorgvuldige vernietiging | | X | | X | | | 49 | Nee |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Foutieve bediening | X | | X | X | | | 50 | Nee |
| Organisatie | Incident | B | E | I | H | M | L | - | Ja/ Nee |
| Gebruikersorganisatie | Mismanagement | X | | X | X | | | 51 | Nee |
| | Gebrekkige toedeling taken, bevoegdheden, verantwoordelijkheden | X | | X | X | | | 52 | Nee |
| | Geen gedragscodes | | X | X | | X | | 53 | Nee |
| | Geen handboeken / systeemdocumentatie / werkprocedures/ gebruiksinstructies | X | | X | X | | | 54 | Nee |
| | Geen interne controle | | | X | | X | | 55 | Nee |
| | Geen toetsing op naleving richtlijnen | | X | X | | X | | 56 | Nee |
| | Geen contractbeheer, SLA's | X | | X | X | | | 57 | Nee |
| | Gebrekkige doel/middelen beheersing | X | | | | X | | 58 | Nee |
| Beheersorganisatie | Gebrekkig beleid betreffende systeembeheer | X | X | X | | X | | 59 | Nee |
| | Gebrekkige capaciteitsverwerving en/of -benutting | X | | | X | | | 60 | Nee |
| | Geen kwaliteitsborging | | | X | | X | | 61 | Nee |
| | Geen (periodieke) inspecties | X | X | X | | | X | 62 | Nee |
| Systeemontwikkelingsorganisatie | Geen projectmanagement | X | | X | | X | | 63 | Nee |
| | Geen ontwikkelrichtlijnen en/of – procedures | X | | X | | X | | 64 | Nee |
| | Geen methoden/technieken | X | | X | | X | | 65 | Nee |
| Omgeving | Incident | B | E | I | H | M | L | - | Ja/ Nee |
| Buitengebeuren | Natuurgeweld (overstroming, blikseminslag, storm, aardbeving etc) | X | | | X | | | 66 | Nee |
| | Overig geweld (oorlog, terrorisme, brandstichting, inbraak, neerstortend vliegtuig) | X | X | | X | | | 67 | Nee |
| | Blokkade/staking | X | | | | X | | 68 | Nee |
| Nutsvoorzieningen | Uitval van elektriciteit, water, telefoon | X | | | X | | | 69 | Nee |
| | Wateroverlast door lekkage, bluswater | X | | | X | | | 70 | Nee |
| | Uitval van licht-, klimaat-, sprinklerinstallatie | X | | | X | | | 71 | Nee |
| Huisvesting | Brand, trilling, ontploffingen | X | | | X | | | 72 | Nee |
| | Gebreken in ruimtes, inbraakgevoeligheid | X | X | | X | | | 73 | Nee |
| Diensten | Incident | B | E | I | H | M | L | - | Ja/ Nee |
| Diensten definitief niet meer te leveren | Faillissement, fusie, leegloop | X | | | X | | | 74 | Nee |
| | Staakt dienstverlening | X | | | X | | | 75 | Nee |
| | Beroept zich langdurig op overmacht in verband met een calamiteit of staking subcontractor | X | | | X | | | 76 | Nee |
| | Wordt overgenomen | X | | | X | | | 77 | Nee |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Stoot taken af | X | | | X | | | 78 | Nee |
| | Verlening serviceovereenkomst wordt geweigerd | X | | | X | | | 79 | Nee |
| Diensten tijdelijk niet te leveren | Komt verplichtingen niet na | X | | | X | | | 80 | Nee |
| | Moet uitwijken | X | | | X | | | 81 | Nee |
| | Beroept zich tijdelijk op overmacht | X | | | X | | | 82 | Nee |
| | Legt prioriteiten bij andere klanten | X | | | X | | | 83 | Nee |
| | Voert geen goed capaciteitsbeheer, overbelasting | X | | | X | | | 84 | Nee |
| Diensten worden niet conform afspraak geleverd | Geen goed opgeleid personeel (kwaliteit) | X | | X | X | | | 85 | Nee |
| | Geen loyaliteit bij personeel, personeelsverloop, verlies kennis/ervaring | X | | | X | | | 86 | Nee |
| | Onvoldoende capaciteit | X | | | X | | | 87 | Nee |
| | Valse verklaringen TPM, ISO-9000, antecedentenonderzoek | X | | X | | X | | 88 | Nee |
| | Onvoldoende of geen kwaliteitsborging | | | X | | X | | 89 | Nee |
| | Komt afspraken vertrouwelijkheid niet na | | X | | X | | | 90 | Nee |
| | Komt afspraken integriteit niet na | | | X | X | | | 91 | Nee |
| | Voert wanbeheer, slordigheden in beheersactiviteiten, releasemanagement, configuratiemanagement, changemanagement, problem-/incidentmanagement, en onderhoudsmanagement | X | X | X | X | | | 92 | Nee |
| | Maakt misbruik van toevertrouwde gegevens | | X | | X | | | 93 | Nee |
| | Maakt misbruik van toevertrouwde applicaties | | X | | X | | | 94 | Nee |
| | Maakt misbruik van toevertrouwde documentatie | | X | | X | | | 95 | Nee |
| | Houdt zich niet aan functiescheiding | | X | X | | X | | 96 | Nee |

# Maatregelen

Onderstaande tabel geeft een overzicht van de hoofdmaatregelen die kunnen worden getroffen om de dreigingen die zijn geïnventariseerd het hoofd te kunnen bieden. De relatie met de tabel met dreigingen is af te leiden uit de derde kolom. Voorts wordt hier aangegeven of een gewenste maatregel reeds getroffen is, en zo ja, of deze actueel is. Indien een maatregel nog niet bestaat, kan worden aangegeven dat deze in de toekomst wordt getroffen. Overal waar in deze tabel BZ staat wordt het team Burgerzaken, overal waar IT staat wordt het team I&A bedoeld.

| CODE | HOOFDMAATREGELEN | Relatie met nr. | Aanwezig | Actueel | Te treffen? | Motivatie en vastlegging |
|---|---|---|---|---|---|---|
| **M** | **Componentgroep Mens** | | | | | |
| M100 | Arbeidscontract/aanstellingsbrief (met (verwijzing naar) rechten, plichten, sancties) | 2,6,7,8,46, 68 | BZ:Ja IT: | | Nee | BZ: Alle medewerkers hebben een aanstellingsbrief. VOG wordt standaard gevraagd. Controle op referenties vindt niet plaats (ook niet wenselijk) Diploma's worden wel gecontroleerd. |
| M101 | Passende arbeidsvoorwaarden (salaris, functiewaardering) | 2,68 | BZ:Ja IT: Ja | | | |
| M102 | Goede arbeidsverhoudingen (OR, vakbond, beoordelingssysteem) | 2,8,68 | BZ:Ja IT: Ja | | | |
| M103 | Werk- en vakantieplanning | 3 | BZ:Ja IT: Deels | | Ja | IT: wordt uitbesteed, opnemen in SLA |
| M104 | Reservecapaciteit | 3 | BZ:Nee IT: Ja | | Nee | BZ: Wordt op dit moment aan gewerkt. |
| M105 | Voldoen aan ARBO-wetgeving | 2 | BZ:Ja IT:Ja | | | |
| M106 | Bedrijfshulpverlening (BHV) | 2 | BZ:Ja IT:Ja | | | |
| M107 | Beveiligingsbewustzijn | 6,7,46,47,4 8 | BZ: Deels IT:Varieert | | Ja | BZ: Beveiligingsbewustzijn op de afdeling goed aanwezig, kamer wordt nooit verlaten zonder deze af te sluiten, documenten slingeren niet rond. Binnenkort wordt een sessie beveiligingsbewustzijn verzorgd. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | IT: Het beveiligingsbewustzijn varieert, afhankelijk van de afdeling. In het algemeen toch vrij laag te noemen, getuige bijvoorbeeld de uitwisseling van login-accounts |
| M108 | Regels t.a.v. aan- en afwezigheid | 3 | BZ:Ja<br>IT:Ja | | | |
| M200 | Voldoen aan eisen brandweer, bouwverordening | 2 | BZ:Ja<br>IT:Ja | | | |
| M201 | Calamiteitenprogramma, evacuatieplan | 2 | BZ:Ja<br>IT:Ja | | | |
| M202 | Regels (m.b.t. brand(preventie)) | 2,7,8 | BZ:Ja<br>IT:Ja | | | |
| M300 | Passende opleidingen | 3,5,45,50 | BZ:Ja<br>IT:Ja | | Nee | |
| M301 | Functiescheiding | 8 | BZ:Ja | | | |
| M302 | Beschreven AO, procedures en werkinstructies | 4,5,7,45, 50 | BZ:Deels<br>IT:Nee | | Nee | BZ: Belangrijkste aanwezig, de rest niet<br>IT: Niet wenselijk |
| M303 | Interne controle, naleven richtlijnen | 5,7,45,55,5 6 | BZ:Ja<br>IT: Ja | | | BZ: middels beveiligingsoverleg |
| M304 | Externe controle | 7,45 | BZ:Ja | | | Accountant, GBA-audit |
| M305 | Clean Desk/clear screen Policy | 7 | BZ:Deels<br>IT:Deels | | Deels | BZ: Clear Desk niet formeel, wel in de praktijk, formalisering wenselijk.<br>Schermbeveiliging met wachtwoord aanwezig, echter zelf uit te schakelen, hetgeen niet wenselijk is. |
| **A** | **Apparatuur** | | | | | |
| A100 | Inkoopbeleid alleen kwaliteitsproducten (apparatuur en programmatuur) | 11,40,41 | IT:Nee | | Nee | IT: op basis van inschatting systeembeheerder |
| A101 | Registratie apparatuur (Configuration Manager, Change Management, Problem Management) | 10,11,12 | IT:Nee | | Ja | |
| A103 | Onderhoudscontracten (incl. Storings- en calamiteitenvoorzieningen) | 10,11,12,6 6,67 | IT:Deels | | Nee | IT: Onderhoud voor de AS/400 geregeld. Een keer per jaar systeem check. Daarnaast service director op AS/400 die een probleem direct meldt aan IBM.<br>Voor de servers contract |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | met IBM met garanties over termijn waarbinnen wordt gereageerd en ten aanzien van vervanging. Voor de werkplekken is bewust geen contract afgesloten. Daarnaast wordt onderhoud AS/400 uitbesteed aan Uphantis met SLA |
| A104 | Schoonmaakcontracten (incl. Calamiteitenclausules) | 11,15 | Ja | | | |
| A105 | Toegangscontrole/procedures tot apparatuurlokaties | 9,16,17, 18,20,21,2 2,67,73 | Ja | | Ja | Afdeling Burgerzaken afgeschermd. Alarm aanwezig, ingeschakeld tussen 20.45 en 06.45. Buiten dat tijdbestek toegankelijk voor medewerkers met sleutel. Daarbuiten kunnen geautoriseerden alarm uitschakelen, met differentiatie in bevoegdheden. Alle werkplekken niet toegankelijk voor publiek, afgesloten met sloten. Serverruimte en patchruimte verder niet toegankelijk voor onbevoegden. De serverruimte heeft brandwerende deuren welke zijn afgesloten middels sleutel, serverruimte uitgerust met brandmelder, bewegingsmelder, blusapparaat, airco. Slechts beperkt aantal personen heeft sleutel. Schoonmakers komen niet in serverruimte. Toegangspasje voor medewerkers BZ zijn zo afgesteld dat zij in serverruimte kunnen komen, niet wenselijk. |
| A106 | Tegengaan van stroomfluctuaties | 11,13,66,6 9,70 | IT: Ja | | | IT:UPS |
| A107 | Noodvoorzieningen (gas, water, | 11,66,69,7 | Nee | | Nee | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | elektriciteit) | 0,71 | | | | |
| A110 | Regels/voorschriften t.a.v. aankoop, afschrijving, installatie en verandering van apparatuur/componenten) | 10,11,12,19 | IT: Ja | | | IT: afschrijving server 4 jaar, pc's 3 jaar |
| A111 | Verzekeringen/reserve budget | 21,67 | | | | |
| A112 | Brandmaatregelen (preventie, detectie, bestrijding) | 21,67 | Ja | | | Rookmelders, brandblussers |
| A113 | Reserve apparatuur | 10,11,21 | IT:Ja | | | IT: desktops, servers contract |
| A200 | Passende omgevingscondities | 11,14 | IT:Ja<br>BZ: deels | | | IT: Airco in serverruimte en klimaatcontrole<br>Locatie BEL: alles accoord, balie wordt afgescheiden van back-office, slot van kluis wordt vervangen en er komt een sleutelkluis<br>Locatie Laren: kluisdeur is standaardsleutel en reserve sleutel is kwijt, hang en sluitwerk is oud, geen brandwerende kasten. Volgend jaar wordt locatie verbouwd, deze zaken meenemen in plannen. |
| A201 | Helpdesk | 11 | IT:Ja | | Ja | IT: Helpdesk aanwezig, |
| A202 | Escalatie-procedures | 11 | IT: ja<br>BZ: Ja | | Ja | Er is een uitwijkcontract, echter deze is marginaal. Daarnaast is er een uitwijkhandboek met noodplan |
| A203 | Aanhouden voorraden reserve-onderdelen | 10,11,23 | | | | |
| A204 | Dubbele uitvoering | 10,11 | Nee | | Nee | |
| A300 | Installatievoorschriften | 11,12,19 | ?? | | ?? | |
| A302 | Documentatie en handleidingen | 11,12,19 | IT: ja | | | |
| **P** | **Programmatuur** | | | | | |
| P100 | Registratie programmatuur (Change management, Problem management) | 29 | IT:Ja | | | |
| P101 | Gescheiden ontwikkel-, test- en productieomgevingen | 24,28,42 | BZ: Ja<br>IT: Ja | | Nee | Geen tests nieuwe versies GBA-applicatie, is niet nodig, wel een testomgeving voor AS/400 aanwezig |
| P102 | Versiebeheer | 26,29 | BZ: Ja | | Nee | Onlangs zijn alle updates vanaf december |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | 2008 geplaatst. Applicatiebeheerder houd dit nu goed in de gaten |
| P103 | Autorisaties en matrices | 28,29 | BZ: kan beter | | Ja | BZ: Er zijn accounts voor externen, deze zijn niet op naam gesteld. Daarnaast is het ww van gebruiker service gelijk aan de inlog |
| P104 | Autorisatie-procedures | 28,29 | BZ:ja IT:Ja | | Nee | BZ: Toewijzing rechten geschiedt door systeembeheer voor de AS/400 welke via BZ een formulier ontvangt na ondertekening leidinggevende. Na autorisatie AS/400 kan BZ zelf zorgdragen voor rechtentoekenning binnen GBA-applicatie Procedure uit-dienst bestaat niet. Procedure autorisaties onlangs vastgesteld en wordt in praktijk ook uitgevoerd |
| P105 | Toegangscontrole/procedures | 28,29 | IT: Deels | | Ja | IT: Op het moment bestaan zowel voor Novell als de AS/400 geen verplichte wijzigingstermijn voor wachtwoorden. Voor de GBA-applicatie staat een termijn van 60 dagen. Het minimaal aantal karakters is 6. Herhaling van laatste wachtwoord(en) niet toegestaan. Blokkering na een aantal pogingen, blokkering is altijd hard. Zie ook gedoogpunt bij audit. |
| P106 | Back-up restore voorzieningen | 25,30 | BZ:ja IT:ja | | Nee | BZ: geregeld verder geen bemoeienis mee IT: 9 november wordt back up en restore getest. Medewerkers van BZ worden hierbij betrokken. Back up tapes worden |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | op gemeentewerf bewaard en dagelijks weggebracht. Vanaf heden wordt er een administratie bijgehouden van het maken van de back up |
| P107 | Virusprotectie | 25,30,43 | IT: Ja | | | Controle op werkplek, server en e-mail middels specialistische software. Deze leest alle mail. |
| P108 | Programmadocumentatie | 27 | | | | |
| P200 | Test- en acceptatieprocedures | 24 | IT:Ja | | | |
| P203 | Installatieprocedures | 24 | | | | |
| P400 | Regels t.a.v. privé gebruik programmatuur | 31,32 | BZ: niet bekend IT: geen regels | | Ja | |
| P401 | Regels t.a.v. gebruik privé-programmatuur | 31,32 | BZ: niet bekend IT: geen regels | | Ja | IT: zal gaan verdwijnen |
| **G** | **Gegevensdragers** | | | | | |
| G100 | IT stuurgroep c.q. -planningsgroep | 51 | N.v.t. | | | |
| G101 | Registratie gegevens(dragers) | 35 | Ja | | Ja | BZ: Applicatiebeheerder houdt administratie bij |
| G102 | Procedure omgang met en vertrouwelijke afvoer van gegevens(dragers) (papier, (harde) schijven etc) | 35,36 | BZ: Ja | | Nee | BZ: Procedure is vernieuwd en bevindt zich in beveiligingshandboek |
| G104 | Backup/restore faciliteiten | 44 | IT:Ja | | | IT: 9 november volgt een test |
| G105 | Controle op integriteit | 37,38 | BZ: Ja | | Nee | Zie procedure |
| G106 | Controle op geautoriseerd gebruik | 39 | BZ: Ja | | Nee | Zie procedure |
| **O** | **Organisatie** | | | | | |
| O100 | Verdeling taken, bevoegdheden en verantwoordelijkheden | 51,52 | Ja | | Ja | Formeel is er niets geregeld, hiervoor wordt een document opgesteld |
| O101 | Gedragscodes gebruikersorganisatie | 53 | BZ:deels IT: heel beperkt | | Ja | BZ: Afspraken of procedures. Een internet/e-mail protocol bestaat niet. Thuiswerken nu nog niet, in de toekomst wel, maar niet voor de GBA-applicatie |
| O102 | Handboeken, systeemdocumentatie,procedures, werkinstructies | 54 | BZ: Ja | | Nee | Handboeken IZRM aanwezig |

| | | | | | | |
|---|---|---|---|---|---|---|
| O200 | Geformaliseerd systeembeheerbeleid | 59 | IT: Ja | | Nee | IT: uitbesteed aan Uphantis |
| O201 | Procedures beheersorganisatie | 60,61 | BZ: Ja | | Nee | |
| O202 | (Periodieke) controle/inspecties | 62 | BZ: Ja | | Nee | |
| O203 | Projectmanagement systeemontwikkeling | 63 | | | | |
| O204 | Richtlijnen ontwikkeling en gebruik tools/methodieken systeemontwikkeling | 64,65 | N.v.t. | | | Systeemontwikkeling vindt niet in-house plaats. |
| **D** | **Diensten** | | | | | |
| D100 | Ballotage nieuwe leveranciers (continuïteit, betrouwbaarheid etc) | 74,75,84,85,86,87 | IT: Niet echt | | Ja | IT: is zelf verantwoordelijk voor het afsluiten van contracten. IT geeft aan met een aantal leveranciers om de tafel te gaan zitten. Uit de offertes wordt een selectie gemaakt en wordt een leverancier aangewezen |
| D101 | Bankgaranties | 74 | | | | Hangt samen met D100 |
| D102 | Leveringsvoorwaarden | 74,75,76,77,78,87 | | | | Hangt samen met D100 |
| D103 | Contractuele afspraken (o.a. schadeclaims) | 74,76,77,78,79,80,83,90,91 | | | | Hangt samen met D100 |
| D104 | Regelen eigendomsverhoudingen | 75,77,78 | | | | Hangt samen met D100 |
| D105 | Uitwijkcontracten, -procedures | 80,81,82 | Deels | | Nee | Jaarlijkse test bij IBM te Almere en daarnaast uitwijkcontract voor AS/400. Uitwijkplan bestaat. Uitwijk is niet volledig geregeld, alleen voor GBA. |
| D106 | Escrow-overeenkomsten | 94 | | | | Hangt samen met D100 |
| D108 | Contractmanagement | 57,74,75,76 | | | | Hangt samen met D100 |
| D200 | Service Level Agreement, met concrete afspraken over procedures en handelwijzen | 57 | | | | IT: SLA's worden ingevoerd. |
| D201 | Service Level rapportage | 57 | | | | Middels vragenlijst (interne audit) |
| D202 | Dossier afspraken en procedures | 88,89 | | | | Hangt samen met D100 |
| D204 | Gecertificeerde leveranciers | 85,86,88,89 | | | | Hangt samen met D100 |
| D205 | Boeteclausules, schadeclaims | 76,79,81,8 | | | | Hangt samen met D100 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | 3,87,90,91, 92,93,94,9 5 | | | | |
| D206 | Aansprakelijkheid | 76,79,81,8 3,87,90,91, 92,93,94,9 5 | | | | Hangt samen met D100 |

# Prioriteitenstelling nog te treffen maatregelen

Uit de bovenstaande tabel is af te leiden welke maatregelen nog getroffen dienen te worden. Aangezien niet alle maatregelen tegelijkertijd kunnen worden geïmplementeerd dient een keuze te worden gemaakt. Daartoe wordt in de volgende tabel een prioritering aangegeven

| Maatregelen | Prioriteit | | |
|---|---|---|---|
| | H | M | L |
| **Formaliseren Clean Desk Policy** | X | | |
| **Opstellen documentatie en handleidingen apparatuur** | | X | |
| **Autorisaties externen aanpassen** | X | | |
| **Procedure autorisaties uit dienst formaliseren** | | X | |
| **Wachtwoord Service aanpassen** | X | | |
| **Opstellen regels ten aanzien van privé gebruik zakelijke programmatuur en gebruik privé programmatuur in zakelijke omgeving** | | | X |
| **Schermbeveiliging instellen bij verlaten werkplek** | X | | |
| **Opstellen gedragscodes gebruikersorganisatie** | X | | |
| **Realisatie geformaliseerd systeembeheerbeleid** | | X | |
| **Formaliseren procedures inhuur diensten** | | X | |
| **Beveilingsbewustzijn vergroten (vast punt op agenda werkoverleg, onderdeel van functioneringsgesprek** | X | | |
| **Toegangspasjes voor serverruimte aanpassen** | X | | |
| **Uitwijk beter regelen (uitgebreider)** | X | | |
| **Verdeling Taken, verantwoordelijkheden en bevoegdheden** | X | | |
| **Locatie BEL, balie, slot kluis, sleutelkluis en ramen** | | | |
| **Locatie Laren, zie A200 kluissleutel, lage balie, geen brandwerende kasten** | X | | |

Opgemerkt moet worden dat de maatregelen getroffen moeten worden in samenhang met elkaar en de reeds getroffen maatregelen.

Onderstaande tabel geeft aan wat de verwachte doorlooptijd en het verwachte capaciteitsbeslag van het implementeren van de gewenste maatregelen zal zijn. Daarnaast wordt aangegeven wie verantwoordelijk is voor de implementatie.

| Maatregel | Doorlooptijd | Capaciteitsbeslag | Verantwoordelijk |
|---|---|---|---|
| **Formaliseren Clean Desk Policy** | 6 maanden | 2 uur per week | Team I&A |
| **Opstellen documentatie en handleidingen apparatuur** | 2 maanden | 2 uur per week | Team I&A |
| **Autorisaties externen aanpassen** | 1 week | 4 uur | Applicatiebeheerder GBA |
| **Procedure autorisaties uit dienst formaliseren** | 2 maanden | 16 uur | Team I&A, team P&O, alle overige afdelingen |
| **Wachtwoord Service aanpassen** | 1 week | 2 uur | Team I&A |
| **Opstellen regels ten aanzien van privé gebruik zakelijke programmatuur en gebruik privé programmatuur in zakelijke omgeving** | 2 maanden | 16 uur | Team I&A i.s.m. overige afdelingen |
| **Schermbeveiliging instellen bij verlaten werkplek** | 1 week | 4 uur | Team I&A en overige afdelingen |
| **Opstellen gedragscodes gebruikersorganisatie** | 6 maanden | 2 uur per week | Team I&A en overige afdelingen |
| **Realisatie geformaliseerd systeembeheerbeleid** | 6 maanden | 2 uur per week | Team I&A |
| **Formaliseren procedures inhuur diensten** | 4 maanden | 60 uur | Juridische zaken, inkoop en I&A |
| **Beveilingsbewustzijn vergroten (vast punt op agenda werkoverleg, onderdeel van functioneringsgesprek** | 1 maand | 2 uur | Beveiligingsfunctionaris |
| **Toegangspasje voor serverruimte aanpassen** | 1 maand | 2 uur | Afdelingmanager Publiek, Vergunningverlening en Handhaving |
| **Uitwijk beter regelen** | 6 maanden | Onbekend | Team I&A, Team BZ |
| **Verdeling Taken, verantwoordelijkheden en bevoegdheden** | 1 maand | 4 uur | Beveiligingsfunctionaris |
| **Locatie Laren, zie A 200, bij verbouwing kritisch op alle zaken letten, kluissleutel, lage balie, geen brandwerende kasten** | 6 maanden | Onbekend | Team, I&A, gebouwenbeheer, Team BZ en Beveiligingsfunctionaris |
| | | | |

Gezien het beslag dat het hierboven beschreven stelsel op de afdeling I&A legt, is besloten eerst de maatregelen met prioriteit Hoog te implementeren. Deze maatregelen kunnen gelijktijdig worden geïmplementeerd.

Bij een startdatum van 1 november 2009 zijn deze maatregelen dus gerealiseerd op 1 mei 2010, waarna de overige maatregelen kunnen worden getroffen in de periode daarna. Ook hier geldt dat maatregelen simultaan kunnen worden geïmplementeerd, hetgeen impliceert dat op 1 mei 2010 alle maatregelen zijn getroffen.

# Bijlage

**Typering en waardering proces**

| Typering | Waardering |
|---|---|
| Kritisch<br>Strategisch | In relatie tot de doelstellingen van de gemeente speelt het proces een primaire rol. Het hoort bij de primaire taken waarop de gemeente direct wordt aangesproken. De gemeente ontleent haar bestaansrecht aan het uitvoeren van deze taken.<br>*Dit is een proces wat essentieel is voor de gemeente, bijvoorbeeld een proces waar de gemeente voor opgericht is of een proces dat een essentiële bijdrage levert aan het bereiken van de strategische doelen van de gemeente.* |
| Strategisch | Het proces kan als strategisch worden getypeerd als het een directe relatie heeft naar het tot stand brengen van de noodzakelijke voorwaarden om de diensten/producten te kunnen voortbrengen. Een aanzienlijk deel van het te besteden budget komt ten goede van dit proces.<br>*Het proces is geen onderdeel van de missie, maar wel een extern zichtbaar product. De buitenwereld zal de gemeente mede afrekenen op de kwaliteit van dit proces* |
| Ondersteunend | Er is slechts sprake van een indirecte relatie met de hoofdactiviteiten van de gemeente. Het ontbreken echter van het bijdragende proces heeft binnen het primaire proces effectiviteits- en efficiency verliezen tot gevolg.<br>*Het proces staat niet in de missie van de gemeente, maar is wel een belangrijke voorwaarde om de missie te kunnen uitvoeren.*<br>*Voorbeeld: de gemeente is er niet voor de urenadministratie of het post archief, maar zonder deze twee processen wordt het wel moeilijker de strategische processen uit te voeren, zelfs al ziet de buitenwereld er niets van.* |
| Overhead | Er is geen relatie met primaire proces. Voorbeeld: activiteiten die moeten worden uitgevoerd zonder direct een wezenlijke bijdrage te leveren aan producten/diensten. |

**Typering en waardering informatiesysteem**

| Typering | Waardering |
|---|---|
| Vitaal | Het uitvoeren van de bedrijfsprocessen en/of het tot stand brengen van producten/diensten is nagenoeg onmogelijk zonder de inzet van informatiesystemen. De inzet van informatiesystemen in van essentieel belang voor een goede uitvoering van het bedrijfsproces.<br>*Voorbeeld: de balans opmaken zonder boekhoudpakket kan echt niet, omdat noodzakelijke informatie in het pakket is opgeslagen. Het is volstrekt onmogelijk de activiteiten uit te voeren zonder het informatiesysteem.* |
| Nuttig | Het informatiesysteem levert een belangrijke bijdrage aan de activiteiten binnen het proces en/of de voortbrenging van producten/diensten. Slechts met grote, onevenredige inspanning is voortzetting van het proces mogelijk. Inzet van het informatiesysteem heeft een positief effect op de doelmatigheid en doeltreffendheid van de gemeente.<br>*Zonder het informatiesysteem zouden de activiteiten alleen met veel extra werk uitgevoerd kunnen worden.* |
| Ondersteunend | Het informatiesysteem biedt ondersteuning bij de activiteiten binnen het bedrijfsproces en is handig om te hebben.<br>*Voorbeeld: PowerPoint is handig om een presentatie te maken, maar als dat er niet is kan je zonder veel extra moeite met Word een aantal sheets maken.* |
| Geen relatie | Het informatiesysteem wordt niet gebruikt binnen het betreffende proces of de inzet van het informatiesysteem is vruchteloos, onbruikbaar of zinloos. |

Beschikbaarheid: Met beschikbaarheid wordt bedoeld, de ongestoorde voortgang van de informatievoorziening evenals het treffen van maatregelen waardoor de kansen op en/of de gevolgen van calamiteiten worden verminderd.

**Classificatie beschikbaarheideisen**

| Classificatie | Omschrijving |
|---|---|
| Maatregelen | Zie bewerkersovereenkomst BEL en Uphantis;<br>Er is een back up en restore procedure vastgesteld en wordt jaarlijks beproefd;<br>Er is een uitwijkcontract en uitwijkprocedure + noodplan;<br>Er is een incidentenregistratie en incidentenprocedure vastgesteld en wordt nageleefd;<br>Er is een SLA opgesteld tussen BEL Combinatie en Uphantis met daarin eisen ten aanzien beschikbaarheid, deze worden ook geëvalueerd. Is op dit moment nog niet gedaan aangezien Uphantis sinds 1 november 2009 bewerker is) |
| Wenselijk | Een enkele keer uitval is aanvaardbaar.<br>*Na een uitval van een week kan de achterstand worden ingehaald naast het gewone werk, zonder dat dit een zware extra belasting voor de medewerkers betekent.* |
| Belangrijk | Nauwelijks uitval gedurende de operationele tijd;<br>*Na een uitval van een dag kan de achterstand met de nodige extra inspanningen worden ingehaald, zonder dat dit onoverkomelijke overlast voor externe partijen oplevert.* |
| Essentieel | Slechts in zeldzame, uitzonderlijke gevallen niet operationeel |

Exclusiviteit: Met exclusiviteit wordt bedoeld, dat de informatie vertrouwelijk is en uitsluitend beschikbaar is voor een gedefinieerde gebruiker / groep van gebruikers in verband met het verrichten van tevoren vastgelegde en goedgekeurde handelingen met de informatie.

**Classificatie exclusiviteiteisen**

| Classificatie | Omschrijving |
|---|---|
| Maatregelen | Er wordt gewerkt met bevoegdheidsprofielen;<br>Autorisatieprocedure is onlangs aangescherpt en wordt gecontroleerd;<br>Er worden alleen vakbekwame medewerkers aangenomen;<br>Er is jaarlijks een presentatie omtrent het beveiligingsbeleid;<br>Beveiliging is standaard onderdeel van werkoverleg en functioneringsgesprekken;<br>Er is een logische toegangsbeveiliging;<br>Er is een procedure onrechtmatige kennisname vastgesteld en wordt nageleefd;<br>Bewerkers worden intern geaudit;<br>Alle medewerkers hebben een geheimhoudingsverklaring getekend;<br>Het GBA systeem beschikt over een adequate toegangsbeveiliging middels wachtwoorden; |
| Wenselijk | Afgeschermd, gegevens zijn alleen ter inzage voor een bepaalde groep.<br>Beperkte schade als gegevens ter beschikking komen van ongeautoriseerden. |

| | |
|---|---|
| | Norm: er mag nooit informatie ter beschikking komen van gebruikers waarvoor deze niet bevoegd zijn! |
| Belangrijk | Cruciaal, gegevens alleen toegankelijk voor direct betrokkenen. Aanzienlijke mate van schade als gegevens uitlekken. |
| Essentieel | Dwingend, belangen van de gemeente of externe partijen worden ernstig geschaad als iemand toegang krijgt zonder dat daar toestemming voor is. Zowel financiële schade als imagoschade. |

Integriteit: Met integriteit wordt bedoeld dat de informatie in overeenstemming is met het afgebeelde deel van de realiteit en dat niets ten onrechte is achtergehouden of verdwenen, kortom de juistheid, volledigheid en tijdigheid van gegevens.

**Classificatie Integriteiteisen**

| Criterium | Omschrijving |
|---|---|
| Maatregelen | Er is een procedure integriteit opgesteld met daarin waarborgen voor de integriteit;<br>Er is een kwaliteitsmodule, welke real-time meedraait, alle mutaties worden direct gecontroleerd;<br>Er vindt handmatige controle plaats van alle mutaties;<br>Zie verder procedure 24 (Integriteit) |
| Wenselijk | Actief, proces tolereert enkele fouten.<br>*Voorbeeld: Urenadministratie. De grote lijnen moeten juist zijn, maar een enkel uur gemaakt in week 46 en geboekt in week 47 heeft geen consequenties voor het bedrijfsproces.* |
| Belangrijk | Detecteerbaar, een zeer beperkt aantal fouten is toegestaan.<br>Fouten zullen worden herkend en hersteld, maar wel ten koste van verloren tijd en wellicht beperkte kosten.<br>*Voorbeeld: een foute verwijzing in het interne telefoonboek betekent verloren tijd, maar is eenvoudig te herkennen en te corrigeren. Of een verkeerde postcode bij contactpersoon of het boeken van uren op een verkeerde projectcode.* |
| Essentieel | Onontbeerlijk, proces vereist foutloze informatie.<br>*Niet-integere informatie veroorzaakt grote schade: kans op grote fraude, kans op onjuiste beslissingen met financiële consequenties en/of imagoschade.* |