Concept
Versie 0.87
21-05-2014
Beleid CIO

Gemeente Amsterdam

Classificatie van Informatie

CONCEPT

Datum : 21 mei 2014
Auteur : CIO-office

Overzicht Beleidsregels

De gemeente Amsterdam heeft zich als lid van de Vereniging der Nederlandse Gemeenten (VNG) verbonden aan de resolutie Informatieveiligheid (29-11-2013). In deze resolutie wordt de Baseline Informatiebeveiliging Gemeenten (BIG) de standaard waarmee de informatiebeveiliging bij gemeenten moet worden ingericht. Gemeente Amsterdam is daarmee nu aan zet om de uitvoering van de BIG in te vullen. Eén van de vereisten is het beschrijven en toepassen van een classificatie van gemeentelijke informatie (artikel 7.2 van de Tactische BIG). Daarnaast zijn er technologische ontwikkelingen die de gemeente dwingen om de classificatie van informatie scherper te beschrijven. Hierbij moet gedacht worden aan het gebruik van Wi-Fi, mobiele apparaten en opslag van informatie in cloudoplossingen. Tot slot wordt er in de ambtseed gesproken over het zorgvuldig omgaan met informatie. Hierover is echter onduidelijkheid.

Er wordt voorgesteld om de volgende normen voor beschikbaarheid, integriteit en vertrouwelijkheid te implementeren op basis van de ontbrekende onderdelen in de huidige classificatie:

De onderscheiden niveaus van beschikbaarheid zijn:

1. **Niet nodig**: de informatie kan zonder gevolgen langere tijd niet beschikbaar zijn. Schending van beschikbaarheid heeft geen gevolgschade.
2. **Noodzakelijk**: de informatie of service mag incidenteel uitvallen, het bedrijfsproces staat incidentele uitval toe. De continuïteit zal op redelijke termijn moeten worden hervat. Schending van deze classificatie kan enige (in)directe schade toebrengen.
3. **Belangrijk**: de informatie of service mag nauwelijks uitvallen. De continuïteit zal snel moeten worden hervat. Schending van deze classificatie kan serieuze (in)directe scharde toebrengen.
4. **Essentieel**: de informatie of service mag alleen in zeer uitzonderlijke situaties uitvallen, bijvoorbeeld als gevolg van een calamiteit. Het bedrijfskritische proces staat eigenlijk geen uitval toe. De continuïteit zal zeer snel moeten worden hervat. Schending van deze classificatie kan (zeer) grote schade toebrengen.

De onderscheiden niveaus van integriteit zijn:

1. **Geen impact**: deze informatie mag worden veranderd. Er is geen extra bescherming van integriteit noodzakelijk. Een schending van integriteit heeft geen gevolgschade.
2. **Beschermd**: het bedrijfsproces dat gebruik maakt van deze informatie staat enkele (integriteits-)fouten toe. Een basisniveau van beveiliging is noodzakelijk.. Schending van deze classificatie kan enige (in)directe schade toebrengen.
3. **Hoog**: het bedrijfsproces dat gebruik maakt van deze informatie staat zeer weinig (integriteits-)fouten toe. Bescherming van integriteit is absoluut noodzakelijk. Schending van deze classificatie kan serieuze (in)directe schade toebrengen.
4. **Absoluut**: het bedrijfsproces dat gebruik maakt van deze informatie staat geen (integriteits-)fouten toe. Schending van integriteit kan (zeer) grote schade toebrengen.

De onderscheiden niveaus van vertrouwelijkheid zijn:

1. **Openbaar:** Alle informatie die algemeen toegankelijk is voor een ieder en ook geschikt is om te publiceren. Er is geen schending van deze classificatie mogelijk.

CONCEPT

2. **Intern:** Informatie die toegankelijk mag zijn voor alle medewerkers van de gemeente. Vertrouwelijkheid is gering. Schending van deze classificatie kan enige (in)directe schade toebrengen.
3. **Vertrouwelijk:** bestemd voor beperkte groep medewerkers die deze informatie nodig hebben voor hun werk ("need to know"). De informatie wordt op basis van vertrouwen beschikbaar gesteld. Schending van deze classificatie kan serieuze (in)directe schade toebrengen.
4. **Geheim:** bestemd voor een enkele persoon of een zeer beperkte groep personen, het belang van de gemeente wordt ernstig geschaad als ongeautoriseerden inzage krijgen.

Bovenstaande classificatie is een gebaseerd op de bestaande classificatie van informatie zoals deze is opgesteld door Rotterdam en KING[1]. Hierdoor is de classificatie ook toepasbaar op de bestuurlijke informatie. Door het vaststellen van deze rubricering zal het onderscheid tussen geheim en strikt geheim vervallen. De beperkte verzending van strikt geheime stukken kan echter nog wel door de griffie worden uitgevoerd zoals nu gebeurd.

Streven is om de informatie in de rubriek Open zoveel mogelijk middels Open Data beschikbaar te stellen. Hierbij moet de informatie wel voldoen aan de wettelijke eisen.

De classificatie dient te worden opgenomen op elke pagina van een document of in de Service Level Agreement die van toepassing is op een database. De classificatie wordt toegepast op alle informatie die door de gemeente wordt gegenereerd/ ontvangen. Conform de Baseline Informatiebeveiliging Gemeenten (BIG) wordt bij het niet opgeven van een classificatie het niveau *Vertrouwelijk* toegepast.

De CIO is verantwoordelijk dat de business bovenstaande classificatie implementeert. Hiervoor kan de CISO de classificatie onderdeel maken van zijn plan van aanpak met betrekking tot de Baseline Informatiebeveiliging Gemeente (BIG). De praktische uitvoering kan per cluster worden belegd.

CONCEPT

[1] Handreiking Data Classificatie Gemeente Rotterdam, 11 januari 2011, Handreiking Dataclassificatie, KING, januari 2014

Versiebeheer

Versies

Versie	Datum	Auteur	Samenvatting van de wijzigingen
0.1	16-5-2013	R.Ulrich	
0.2	22-5-2013	R.Ulrich	Aanpassingen nav input CIO-beleidsteam
0.3	25-7-2013	M. Haubrich	Aanpassingen ism beleidsteam nav feedback CPIB, CISO
0.4	12-9-2013	L. van der Dussen	Aanpassingen op basis van externe documenten
0.81	11-10-2013	R. Ulrich en L. van der Dussen	Kleine tekstuele aanpassingen en verwerking input P. van Leeuwen en klankbordgroep Informatiebeleid
0.82	22-11-2013	R.Ulrich en L. van der Dussen	Kleine aanpassing na overleg met Directie Communicatie/BDA
0.83	2-12-2013	L. van der Dussen	Aanpassingen nav collegiale review
0.85	13-2-2014	L. van der Dussen	Aanpassingen obv brede review CIO-office en stad
0.86	18-3-2014	L. van der Dussen	Aanpassingen nav bespreking in CPIB en klankbordgroep Informatiebeleid
0.87	2-4-2014	L. van der Dussen	Aanpassingen obv bespreking klankbordgroep Informatiebeleid en CIO-adviesteam

Goedkeuring

Versie	Datum	Naam
0.87	18-3-2014	Klankbordgroep Informatiebeleid
0.87	18-3-2014	Cluster Privacy en Informatiebeveiligersoverleg
0.87	27-5-2014	Cluster Informatiemanagersoverleg
0.87		Ambtelijk Team

CONCEPT

Inhoud

CONCEPT

1 Het Onderwerp

1.1 Aanleiding

Op 29 november 2013 is in de Bijzondere Algemene Ledenvergadering van de Vereniging der Nederlandse Gemeenten (VNG) de resolutie Informatieveiligheid aangenomen. Deze resolutie houdt in dat de leden van de VNG, waaronder gemeente Amsterdam, zich committeren aan de Baseline Informatiebeveiliging Gemeenten (BIG). Deze baseline bestaat uit een strategisch en tactisch deel. In het strategische deel wordt op hoofdlijnen de informatieveiligheid benoemd. Eén van de randvoorwaarden die door de gemeenten moet worden ingevuld is:

"4. Methoden voor rubricering en continue evaluatie hiervan zijn hanteerbaar om onder- en overrubricering te voorkomen. De Strategische Baseline geeft geen aanpak voor rubriceren van informatie."[2]

In de tactische Baseline wordt deze randvoorwaarde vertaald naar de classificatie van informatie (artikel 7.2). Het doel van de classificatie is zorgdragen voor een geschikt niveau van bescherming voor de informatie. Hiervoor moet er door de gemeente een classificatie worden opgesteld.[3] Onderliggende beleidsstuk is een uitwerking van artikel 7.2 van de Tactische Baseline. Het geeft een classificatie voor zowel bestuurlijke als ambtelijke documenten binnen de gemeente Amsterdam. Het voorgestelde kader is gebaseerd op de *Handreiking Dataclassificatie* van KING/ VNG en de gemeente Rotterdam.[4]

Daarnaast wil Amsterdam zich transparant profileren naar burgers en bedrijven. Om na te gaan hoe de gewenste transparantie van de gemeente in de praktijk vertaald kan worden is het noodzakelijk dat eerst bepaald wordt welke informatie zonder problemen kan worden ingezien door burgers en bedrijven. Hiervoor moet de informatie geclassificeerd worden. Het classificeren van informatie is van belang omdat je met de classificatie aangeeft of en hoe die informatie beschermd moet worden.

Om invulling te geven aan de transparantie leggen ambtenaren de ambtseed af. In artikel 7 van *"De gerechtigheid dienen - de nieuwe Amsterdamse Ambtseed"* wordt hieraan gerefereerd:

> 7. Ik zal zorgvuldig omgaan met informatie.
> De toenemende concentratie van informatie over burgers bij de overheid vraagt van de ambtenaar uiterste zorgvuldigheid in de omgang hiermee. Dergelijke informatie mag alleen gebruikt worden voor het doel waarvoor ze door de burger ter beschikking is gesteld. Het uitlekken van dergelijke informatie dient dan ook te worden verhinderd. Gaat het niet om informatie met betrekking tot individuele burgers, maar om informatie met betrekking tot de overheid, de wetten en het beleid dan dient zoveel mogelijk openheid te worden betracht. De gemeentelijke organisatie dient naar de geest van de Wet Openbaarheid Bestuur te handelen. Dat sluit natuurlijk niet uit dat bepaalde informatie tijdelijk een vertrouwelijk karakter krijgt en door de ambtenaar als zodanig moet worden behandeld.[5]

[2] Strategische Baseline Informatiebeveiliging Gemeenten, versie 1.0 mei 2013, IDB

[3] Tactische Baseline Informatiebeveiliging Gemeenten, versie 1.0 mei 2013, IDB, p. 25

[4] Handreiking Dataclassificatie KING/ VNG, oktober 2013

[5] *De gerechtigheid dienen De nieuwe Amsterdamse Ambtseed, maart 2006, Bureau Integriteit*

CONCEPT

In dit artikel klinkt duidelijk een tweedeling door: enerzijds is de gemeente (en dus de individuele ambtenaar) verplicht vertrouwelijk en dus uiterst zorgvuldig om te gaan met privacygevoelige informatie, anderzijds dient de gemeente (en dus de individuele ambtenaar) transparantie na te streven in al haar doen en laten. Er zijn uiteraard duidelijke voorbeelden van beide categorieën: enerzijds persoonsinformatie zoals geboortedatum en inkomen, anderzijds genomen besluiten zoals bestemmingsplannen en vergunningen. Maar er is een grijs gebied waarin informatie een (zoals de ambtseed dit noemt) “vertrouwelijk karakter” krijgt.

Ook sluit de ambtseed af met de opmerking dat door de ambtenaar vertrouwelijke informatie “als zodanig moet worden behandeld”; er wordt in het midden gelaten wat dat zoal inhoudt. Dit beleidskader poogt daarin een handreiking te doen en gaat daarom vooral over de classificatie op basis van vertrouwelijkheid.

De scope van dit beleidsstuk is de toegankelijkheid (“inzien van”) de informatie. Hierbij wordt geen onderscheid gemaakt tussen de ambtelijke informatie of de bestuurlijke informatie.

1.2 De beleidsvraag/vragen

Op welke wijze kan Amsterdam invulling geven aan de BIG en de vertrouwelijkheid van informatie classificeren, met inachtneming van risico’s (schade) van openbaar inzien en/of verspreiding van die informatie?

Wat betekent een bepaalde classificatie voor de “zorgvuldige behandeling” van deze informatie voor een ambtenaar of ketenpartner?

1.3 Stakeholders en hun belangen en overwegingen

In principe is elke organisatie van de gemeente Amsterdam belanghebbend, maar er zijn enkele partijen die een bijzondere rol hebben en daarom betrokken zijn bij het opstellen van dit beleidsstuk:

BDA-DMC, verantwoordelijk voor NRGA/gedragscode
BDA-Directie Communicatie, verantwoordelijk voor gemeentebrede communicatie via Intranet
SHP, verantwoordelijk voor communicatie met en screening van medewerkers
CISO, verantwoordelijk voor toezicht op naleving beleid namens de CIO
DICT, als leverancier van gemeentebrede IT
CIO, verantwoordelijk voor informatiebeleid
DFM, met betrekking tot de communicatie met burgers en bedrijven en de fysieke maatregelen om classificatie te implementeren.
Stadsarchief, verantwoordelijk voor het toezicht op informatiebeheer, inclusief de toepassing van de wettelijke openbaarheidsregimes.
SAA: verantwoordelijk voor het archiveren en ontsluiten van informatie. Daarnaast ontwikkelt zij kaders voor het digitaal ondertekenen van documenten.
Clusters: verantwoordelijk voor de implementatie van de voorgestelde classificatie.

1.4 Beleidskoppelingen

Dit beleid valt binnen het volgende beleidsthema: *Vertrouwen en beveiliging van informatie*

Het beleid omtrent classificatie heeft door deze thematisering de volgende raakvlakken met andere beleidsonderwerpen:

CONCEPT

Authenticatie, Autorisatie, Accounting, met betrekking tot het toekennen van rechten aan medewerkers.
Open Data, een mogelijke manier om openbare informatie te ontsluiten.
Het Nieuwe Werken, de (on)mogelijkheden van het Nieuwe Werken worden in grote mate bepaald door de toegang tot informatie. De classificatie moet tijd-, plaats- en apparaat onafhankelijk kunnen functioneren.
Bring Your Own device, een manier om de classificatie apparaat onafhankelijk te laten functioneren.
Cloudcomputing, de opslag van gemeentelijke informatie in een cloud omgeving, zowel buiten de gemeente (bijvoorbeeld Dropbox, Evernote, iCloud oid) als binnen het eigen netwerk (de Amsterdamse Cloud), wordt beperkt door de classificatie die de informatie krijgt.
Informatiebeheer, dit loopt vanaf het ontstaan van informatie tot en met de vernietiging of langdurige bewaring. Hierbij moet worden opgetrokken met het Stadsarchief.

CONCEPT

2 Beleidskader

2.1 Uitgangspunten

Het belangrijkste uitgangspunt is dat in beginsel informatie van de gemeente Amsterdam openbaar is. Dit in het kader van transparantie en op basis van de Wet openbaarheid van bestuur:

"Overheidsinformatie is altijd openbaar, tenzij de Wet openbaarheid van bestuur (Wob) of andere wetgeving bepaalt dat de gevraagde informatie niet geschikt is om openbaar te maken."[6]

Kortom, informatie is in beginsel openbaar, tenzij:

- Wetgeving het niet toestaat (zoals in het geval van persoonsgegevens of bedrijfs- en fabricagegegevens),
- Openbaring het imago van (en dus vertrouwen in) de gemeente ernstig schaadt,
- De gemeente bij openbaring financiële schade oploopt (aanbestedingen, concurrentiegevoeligheid bij contracten enz.)

Het tweede uitgangspunt is dat informatie niet kan worden gedeclassificeerd. Dit betekent dat de gemeente de classificatie van medeoverheden en ketenpartners zal toepassen. Informatie wordt op hetzelfde niveau in Amsterdam geclassificeerd als door medeoverheden en ketenpartners. Dit betekent dat een selecte groep medewerkers deze informatie moet kunnen inzien en gebruiken. Hieraan zitten wel enkele verplichtingen en vereisten, die worden behandeld in de paragrafen over personeel..

De gemeente Amsterdam kent tot op heden de volgende niveaus van openbaarheid:

- *Actief Openbaar*: de informatie is openbaar en (uiteindelijk) voor een ieder toegankelijk.
- *Geheim (voorheen Kabinet):* aanduiding voor geheime informatie. De verspreidingskring is beperkt tot leden van het college van Burgemeester en Wethouders, de leden van de screeningscommissie, de wethouder assistenten, de loco gemeentesecretaris, de directeur directie Communicatie, de afdeling Voorlichting, de bestuursadviseur chef Kabinet burgemeester en twee annotatieschrijvers van het college B en W. Indien het stuk bestemd is voor (duo)raadsleden wordt de verspreidingskring uitgebreid met (duo)raadsleden en medewerkers van de griffie.
- *Strikt Geheim (voorheen Beperkt Kabinet):* aanduiding voor extreem gevoelige informatie. Deze stukken worden alleen verspreid onder de collegeleden, de gemeentesecretaris, de uitvoerende secretaris (notulist) en de directeur Communicatie.[7]

Het verschil tussen Geheim en Strikt geheim is enkel ingegeven door het aantal geadresseerden. De behandeling van de informatie geschiedt op dezelfde wijze. Deze informatie wordt per definitie niet elektronisch uitgewisseld.[8] Weliswaar worden deze

[6] Vrij naar artikel 10 en 11 van de Wet Openbaarheid van Bestuur, BWBR0005252

[7] *Handreiking geheimhouding, Nadere informatie over het opleggen, bekrachtigen en opheffen van geheimhouding,* februari 2012 Rekenkamer Amsterdam; Collegebesluit juli 2011

[8] Gesprek Griffie 11 september 2013

CONCEPT

stukken ingevoerd in Andreas. Binnen Andreas is er een rechtenstructuur ingericht die de ongeautoriseerde digitale toegang tot deze informatie niet mogelijk maakt.

In Andreas bestaat er ook een functionaliteit om de classificatie van informatie op een gewenst tijdstip te veranderen. Dit wordt *Onder Embargo* genoemd. Hierbij wordt geautomatiseerd de classificatie omgezet van geheim naar openbaar. De functionaliteit dient bij de implementatie van de nieuwe classificatie ook opgenomen te worden.

Tot slot zijn er nog twee principes die samenhangen met de classificatie van data:

1) De eigenaar is verantwoordelijk voor de informatie. Hieruit volgt dat de eigenaar van de informatie bepaalt welke classificatieniveaus vereist zijn. Dit heeft als consequentie dat de eigenaar bepaalt welke maatregelen er vereist zijn. De eigenaar van de informatie bepaalt wie toegang krijgt tot welke informatie.
2) Er wordt gestreefd naar een zo 'laag' mogelijk classificatieniveau. Met dit principe wordt invulling gegeven aan de transparantie van de overheid. Daarnaast leidt hogere classificatie tot potentieel hogere kosten. Het classificatieniveau wordt gekozen op basis van het doelbindingsprincipe, welke samenhangt met de taak die wordt uitgevoerd.

2.1.1 Wat is er nu voor personeel?

Een classificatie kan alleen werken als er per niveau personen worden geautoriseerd om informatie in te zien. Hierbij gaan we uit van het principe dat de informatie essentieel is voor de uitvoering van de primaire taak. (*Need-to-know*) Om te bepalen dat een medewerker correct met de informatie omgaat kan men screening laten uitvoeren. Op dit moment gebeurt dit voor interne medewerkers bij het moment van in dienst treden via een Verklaring Omtrent Gedrag (VOG). Daarnaast leggen de interne medewerkers ook de ambtseed af, waarin via artikel 7 zij dit nogmaals bevestigen. Externe medewerkers kunnen niet gebonden worden aan de Ambtseed. Zij tekenen daarvoor een geheimhoudingsverklaring bij de start van hun werkzaamheden.

2.1.2 Wat is er nu voor techniek?

Op dit moment is er de classificatie van informatie binnen Andreas technisch ondersteund. Er bestaat een mogelijkheid om de classificatie ook in andere workflow systemen op te nemen.
DICT heeft wel een Infrastructuur Risico Policy beschreven. Deze is gebaseerd op de Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV). Op basis van een BIV-rating wordt bepaald welke technische eisen er worden gesteld aan ICT-diensten. Deze BIV-rating is gebaseerd op vier verschillende niveaus.[9]
Daarnaast beschikken verscheidene Document Management Systemen over de mogelijkheid om vertrouwelijkheid van informatie aan te geven. In de Metadatastandaard van het Stadsarchief is het aangeven van de classificatie van het dossierniveau verplicht. De implementatie van de voorgestelde classificatie dient dan ook aan te sluiten bij de ontwikkelingen van het Stadsarchief.

2.1.3 Wat is er nu in het proces?

De technische mogelijkheden worden momenteel alleen voor de bestuurlijke informatie vastgelegd. De invoering van een classificatie van informatie voor ambtelijke informatie zal vragen om nadere beschrijvingen van de processen binnen de stad. De ideale manier om dit te inventariseren is het Business Informatieplanningstraject, zoals deze reeds worden uitgevoerd binnen de clusters.

[9] Infrastructuur Risico Policy, DICT, 2014

CONCEPT

2.2 Wat ontbreekt er?

De vier uitgangspunten uit 2.1 zijn echter nog onvoldoende vastgelegd om invulling te geven aan de BIG. Dit komt door het ontbreken van een tussenniveau (*Vertrouwelijk*). Deze tussenclassificatie ligt tussen geheim en openbaar in, zodat er binnen Amsterdam samengewerkt kan worden.

De BIG is verdeeld in twee onderdelen, een strategisch deel en een tactisch deel. Gecombineerd bieden zij gemeenten de mogelijkheid de informatiebeveiliging vorm te geven. Over classificatie staat in de strategische Baseline enkel vermeld dat er een classificatie moet zijn. In de tactische baseline wordt enkel verwezen naar het feit dat de gekozen classificatie overeen moet komen met bestaande wetgeving, zoals de Wet Bescherming Persoonsgegevens (Wbp).
In de BIG wordt voorgesteld dat gemeenten gebruik gaan maken van de classificatie van het Rijk, zoals vastgelegd in het Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIR-BI 2013). In de BIG wordt uitgegaan van het basisniveau *Departementaal Vertrouwelijk* uit de VIR-BI, vertaald naar de gemeentelijke situatie is dat *(Gemeentelijk) Vertrouwelijk*. Bijzondere informatie is informatie waar kennisname door niet geautoriseerden nadelige gevolgen kan hebben voor de belangen van de gemeente, van zijn ketenpartners of medeoverheden.[10]
Daarnaast is het uitgangspunt van de BIG dat het beveiligingsniveau in lagen is opgebouwd. Er kunnen zonder inbreuk te doen op het basisniveau lagen worden toegevoegd.[11]

2.3 Beleidskeuzes

Het beschermingsniveau van data wordt uitgedrukt in classificatieniveaus voor beschikbaarheid, integriteit en vertrouwelijkheid (BIV) van informatie.

- **Beschikbaarheid**: hoeveel en wanneer informatie toegankelijk is en gebruikt kan worden.
- **Integriteit**: het in overeenstemming zijn van informatie met de werkelijkheid en dat niets ten onrechte is achtergehouden of verdwenen. Met andere woorden de juistheid, volledigheid en tijdigheid van informatie wordt gegarandeerd.
- **Vertrouwelijkheid**: de bevoegdheden en de mogelijkheden tot muteren, kopiëren, toevoegen, vernietigen of kennisnemen van informatie voor een gedefinieerde groep van gerechtigden.

Op basis van de BIV kan worden bepaald welke beveiligingseisen er gelden en welke maatregelen er genomen moeten worden.

Er wordt voorgesteld om de volgende normen voor beschikbaarheid, integriteit en vertrouwelijkheid te implementeren op basis van de ontbrekende onderdelen in de huidige classificatie:

De onderscheiden niveaus van beschikbaarheid zijn:

1. **Niet nodig**: de informatie kunnen zonder gevolgen langere tijd niet beschikbaar zijn. Schending van beschikbaarheid heeft geen gevolgschade.
2. **Noodzakelijk**: de informatie of service mag incidenteel uitvallen, het bedrijfsproces staat incidentele uitval toe. De continuïteit zal op redelijke termijn moeten worden hervat. Schending van deze classificatie kan enige (in)directe schade toebrengen.
3. **Belangrijk**: de informatie of service mag nooit uitvallen, het bedrijfsproces staat nauwelijks uitval toe. De continuïteit zal snel moeten worden hervat. Schending van deze classificatie kan serieuze (in)directe scharde toebrengen.

[10] Vrij naar art 1 lid a van het Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere informatie 2013

[11] Strategische Baseline Informatiebeveiliging Gemeenten, versie 1.0 mei 2013, IDB

CONCEPT

4. **Essentieel**: de informatie of service mag alleen in zeer uitzonderlijke situaties uitvallen, bijvoorbeeld als gevolg van een calamiteit. Het bedrijfskritische proces staat eigenlijk geen uitval toe. De continuïteit zal zeer snel moeten worden hervat. Schending van deze classificatie kan (zeer) grote schade toebrengen.

De onderscheiden niveaus van integriteit zijn:

1. **Geen impact**: deze informatie mag worden veranderd. Er is geen extra bescherming van integriteit noodzakelijk. Een schending van integriteit heeft geen gevolgschade.
2. **Beschermd**: het bedrijfsproces dat gebruik maakt van deze informatie staat enkele (integriteits-)fouten toe. Een basisniveau van beveiliging is noodzakelijk.. Schending van deze classificatie kan enige (in)directe schade toebrengen.
3. **Hoog**: het bedrijfsproces dat gebruik maakt van deze informatie staat zeer weinig (integriteits-)fouten toe. Bescherming van integriteit is absoluut noodzakelijk. Schending van deze classificatie kan serieuze (in)directe schade toebrengen.
4. **Absoluut**: het bedrijfsproces dat gebruik maakt van deze informatie staat geen (integriteits-)fouten toe. Schending van integriteit kan (zeer) grote schade toebrengen.

De onderscheiden niveaus van vertrouwelijkheid zijn:

1. **Openbaar:** Alle informatie die algemeen toegankelijk is voor een ieder en ook geschikt is om te publiceren. Er is geen schending van deze classificatie mogelijk.
2. **Intern:** Informatie die toegankelijk mag zijn voor alle medewerkers van de gemeente. Vertrouwelijkheid is gering. Schending van deze classificatie kan enige (in)directe schade toebrengen.
3. **Vertrouwelijk:** bestemd voor beperkte groep medewerkers die deze informatie nodig hebben voor hun werk (“need to know”). De informatie wordt op basis van vertrouwen beschikbaar gesteld. Schending van deze classificatie kan serieuze (in)directe schade toebrengen.
4. **Geheim:** bestemd voor een enkele persoon of een zeer beperkte groep personen, het belang van de gemeente wordt ernstig geschaad als ongeautoriseerden inzage krijgen.

Bovenstaande classificatie is een vertaling van de bestaande classificatie van informatie zoals deze is opgesteld door Rotterdam en KING[12]. Hierdoor is de classificatie ook toepasbaar op de bestuurlijke informatie. Door het vaststellen van deze rubricering zal het onderscheid tussen geheim en strikt geheim vervallen. De beperkte verzending van strikt geheime stukken kan echter nog wel door de griffie worden uitgevoerd zoals nu gebeurd.

Streven is om de informatie in de rubriek Open zoveel mogelijk middels Open Data beschikbaar te stellen. Hierbij moet de informatie wel voldoen aan de wettelijke eisen.

De classificatie dient te worden opgenomen op elke pagina van een document of in de Service Level Agreement die van toepassing is op een database. De classificatie wordt toegepast op alle informatie die door de gemeente wordt gegenereerd/ ontvangen. Conform de Baseline Informatiebeveiliging Gemeenten (BIG) wordt bij het niet opgeven van een classificatie het niveau *Vertrouwelijk* toegepast.

[12] Handreiking Data Classificatie Gemeente Rotterdam, 11 januari 2011, Handreiking Dataclassificatie, KING, januari 2014

CONCEPT

De CISO is verantwoordelijk dat de business bovenstaande classificatie implementeert. Hiervoor kan de CISO de classificatie onderdeel maken van zijn plan van aanpak met betrekking tot de Baseline Informatiebeveiliging Gemeente (BIG). De praktische uitvoering kan per cluster worden belegd.

CONCEPT

3 Praktische Handreiking

Om de ambtenaar in staat te stellen om informatie met een vertrouwelijk karakter als zodanig te behandelen, volgen hierna een aantal voorbeelden en gedragsregels die van toepassing zijn op de verschillende niveaus. Daarbij worden ook maatregelen genoemd die de invoering, borging en handhaving van de voorgestelde classificatie mogelijk maken. Voor een goede invoering van de classificatie dient onderstaande uitwerking ook voor beschikbaarheid en integriteit te worden uitgevoerd. Het streven is om dit in september 2014 aan te bieden aan het AT ter besluitvorming.

Open(baar)
Alle informatie die algemeen toegankelijk is voor een ieder. Er is geen schending van deze classificatie mogelijk.

Een voorbeeld van informatie met het kenmerk open is dit beleidsstuk. Er staan immers geen uitspraken in die wettelijk een vertrouwelijk karakter hebben en er is ook geen schade te voorzien voor de gemeente bij openbaring.

Daarom kunnen we dit stuk “gewoon” in de mail versturen, ook naar eventueel geïnteresseerden vanuit de G4 of ketenpartners. Het stuk kan ook opgeslagen worden op een cloudoplossing (bijvoorbeeld Evernote) zonder dat we ons zorgen hoeven te maken over het “meekijken” door derden. Het stuk kan worden bewerkt en gelezen in een publieke plaats (denk aan de trein of een coffeeshop) zonder dat we ons moeten bedenken of er over onze schouder wordt meegelezen.

Aan de andere kant is informatie met een open karakter niet per definitie “te publiceren” informatie; persberichten en websites worden met zorg voorbereid. Het is dus niet meteen de bedoeling open informatie actief te verspreiden. Het open karakter geeft aan dat passieve verspreiding geen problemen zal opleveren en dat het dus zonde is om tijd en geld te besteden deze informatie tegen publieke inzage te beveiligen.

OK	Niet OK
Opslaan in een publieke cloudoplossing (Evernote, iCloud, SkyDrive, Google Drive, etc.) Lezen/bewerken waar mensen onverhoopt kunnen meekijken Delen met geïnteresseerde ketenpartners (G4, WiGo4IT, enz) E-mailen zonder beperkingen/maatregelen	Actief publiceren en uitdragen op bijv. een privé blog

CONCEPT

Intern **Informatie die toegankelijk mag zijn voor alle medewerkers van de gemeente.**	
Informatie die beschikbaar is op intranet heeft een intern vertrouwelijk karakter. Deze informatie is bedoeld om de medewerkers van de gemeente te informeren en te ondersteunen in hun werkzaamheden. Deze informatie kan gebruikt worden buiten een (beveiligde) kantooromgeving. Incidenteel kan deze informatie worden gedeeld met een ketenpartner. Het is echter niet de bedoeling om het volledige intranet te kopiëren en te delen met buitenstaanders. Dit kan op basis van het principe van doelbinding. Een gemeentelijk vertrouwelijk karakter is niet gebaseerd op specifieke regels, maar moet vooral met gezond verstand worden toegepast.	
OK	Niet OK
Informatie opslaan in een publieke cloudoplossing (Evernote, iCloud, SkyDrive, Google Drive, etc.) Informatie delen met geïnteresseerde ketenpartners (G4, WiGo4IT, enz) Informatie lezen/bewerken waar mensen onverhoopt kunnen meekijken Informatie e-mailen zonder beperkingen/maatregelen Geheel opslaan in een private cloudoplossing (netwerkschijf of toekomstige ADW-clouddrive)	Complete dossiers opslaan in een publieke cloudoplossing (Evernote, iCloud, SkyDrive, Google Drive, etc.) Complete dossiers delen met geïnteresseerde ketenpartners (G4, WiGo4IT, enz) Complete dossiers lezen/bewerken waar mensen onverhoopt kunnen meekijken Integraal e-mailen zonder beperkingen/maatregelen

CONCEPT

(Gemeentelijk) vertrouwelijk **bestemd voor beperkte groep medewerkers die deze informatie nodig hebben voor hun werk (“need to know”).**	
Als er een Europese aanbesteding wordt gedaan, worden er door de projectgroep veel voorbereidingen gedaan. Het publiceren van informatie op de aanbestedingskalender is maar een deel van het werk; die informatie betreft in principe openbare informatie, namelijk: wat vragen we en hoe beoordelen we? Naast die openbare informatie worden er ook ramingen gedaan met betrekking tot de te verwachten kosten (eenmalig of op jaarbasis) en misschien wordt er zelfs geld gereserveerd om juridische regelingen te treffen. Deze ramingen moeten vertrouwelijk worden behandeld, want als marktpartijen precies weten wat ze kunnen vragen, zullen ze daar logischerwijs op inspelen (of een concurrentievoordeel mee behalen als niet alle marktpartijen deze informatie tot hun beschikking hebben). Dit heeft meestal een financiële schade voor de gemeente tot gevolg (we betalen liever nog minder dan vooraf geraamd en eventuele schikkingen proberen we uiteraard in beginsel te vermijden) Documenten met zulke kostenramingen of reserveringen hebben dus de classificatie “vertrouwelijk”. Dit betekent dat ik een uitputtende lijst moet geven met namen en functies van mensen die het wèl mogen inzien en er vervolgens zorg voor moet dragen dat niemand buiten die groep (“need to know” mensen) er kennis van kan nemen. Daarom sla ik zo’n document alleen op in een map waarvan ik weet dat alleen die groep mensen erbij kan. Ook mail ik het hen alleen met een versleuteling (encryptie), want e-mail is helaas een onveilige omgeving. Ik sla het document nooit op in Evernote, want dan heeft de gemeente geen controle meer over de toegang. Ook ga ik niet met de rode pen het document doornemen in de trein, waar mensen over mijn schouder mee kunnen lezen.	
OK	Niet OK
Opslaan in een private cloudoplossing waar alleen de beperkte groep toegang toe heeft (bijvoorbeeld de netwerkschijf of toekomstige ADW-clouddrive) E-mailen met versleuteling *(dus een functionele eis aan de ADW)*	Opslaan in een publieke cloudoplossing (Evernote, iCloud, SkyDrive, Google Drive, etc.) Delen met geïnteresseerde ketenpartners (G4, WiGo4IT, enz) Lezen/bewerken waar mensen onverhoopt kunnen meekijken E-mailen zonder beperkingen/maatregelen

CONCEPT

Geheim **bestemd voor een enkele persoon of een zeer beperkte groep personen, het belang van de gemeente wordt ernstig geschaad als ongeautoriseerden inzage krijgen.**	
Informatie met de classificatie geheim kan bij niet geautoriseerde toegang de vitale belangen van de gemeente kan schaden. Bijvoorbeeld bijzondere persoonsgegevens die in bepaalde processen worden gevraagd om een burger/ bedrijf een dienst te kunnen verlenen. Deze informatie mag in het kader van doelbinding en rechtmatigheid niet buiten het proces worden gebruikt. Hierdoor zullen enkel betrokkenen in het proces toegang moeten krijgen tot de informatie. Informatie die aan de gemeente wordt verstrekt over de koninklijke familie of buitenlandse delegaties ten behoeve van de veiligheid. De directie Openbare Orde en Veiligheid maakt hiervan gebruik om de persoonlijke veiligheid van de betreffende personen te borgen. Daarnaast wordt deze informatie gebruikt om de openbare orde te waarborgen. Een ander voorbeeld is de informatie die de gemeente heeft met betrekking tot nutsvoorzieningen in de stad. De uitval van deze voorzieningen leidt tot economische schade. Hierdoor moet voorkomen worden dat niet geautoriseerden deze informatie kunnen inzien. Als je met zulke informatie werkt, dien je het dus ook met zorg te behandelen. Dat betekent dat het nooit onversleuteld (evt. als bijlage) in een e-mail verzonden wordt, dat het nooit in een publieke cloudoplossing wordt opgeslagen waarover de gemeente geen of weinig zeggenschap in heeft en dat je het nooit in de trein gaat annoteren. Al deze acties kunnen leiden tot het “lekken” van de informatie.	
OK	Niet OK
Opslaan in een gemeentelijke cloudoplossing waar alleen ik toegang toe heb (“Mijn Documenten” in de ADW of toekomstige ADW-clouddrive) E-mailen met versleuteling *(dus een functionele eis aan de ADW)*	Opslaan in een publieke cloudoplossing (Evernote, iCloud, SkyDrive, Google Drive, etc.) Delen met geïnteresseerde ketenpartners (G4, WiGo4IT, enz) Lezen/bewerken waar mensen onverhoopt kunnen meekijken E-mailen zonder beperkingen/maatregelen

CONCEPT

4 Consequenties

Het vaststellen van de voorgestelde classificatie zal op de volgende onderdelen doorwerken. Om het beleidskader te kunnen implementeren moet er een plan van aanpak worden opgesteld. Dit plan van aanpak dient te worden opgesteld door DICT, Dienstverlening, het Stadsarchief, Concern Communicatie en de Bestuursdienst Amsterdam. De CISO is verantwoordelijk voor de uitvoering van de implementatie door de verschillende onderdelen in de stad. De business kan tijdens de implementatie van de classificatie via de CISO eventuele knelpunten adresseren. Hierbij moet ook worden gekeken naar de praktische toepasbaarheid van de classificatieniveaus.

4.1 Personeel

Er zal gekeken moeten worden naar het gedrag van medewerkers. Als een medewerker om moet gaan met vertrouwelijke informatie zal hij goed moeten nadenken in welke omstandigheden dat goed mogelijk is. Bewustwording is hierbij zeer belangrijk. Concern Communicatie heeft al gedragsregels uitgegeven voor de omgang met gemeentelijke informatie op Internet. Deze zullen herijkt worden en aangevuld waar nodig. Op basis daarvan zullen de regels actief gecommuniceerd worden. Daarnaast dient Concern Communicatie haar gedragsregels omtrent sociale media uit te breiden met gedragsregels die de omgang met informatie mogelijk maken.
Door SHP wordt een nieuw proces van screening ingevoerd met betrekking tot de omgang van informatie die van buiten de gemeente komt. De Verklaring Omtrent Gedrag is enkel bruikbaar voor de classificaties Intern en Vertrouwelijk. Er dient een lijst te worden opgesteld met functies die de hoogste classificatie moeten kunnen inzien. Deze functies moeten overeenkomstig worden gescreend. Hiervoor dient overleg te worden gepleegd met het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Zij is als ministerie verantwoordelijk voor de screening. De screening wordt uitgevoerd door de Algemene Inlichtingen- en Veiligheidsdienst (AIVD). Het voorschrift over classificatie voor het Rijk maakt gebruik van drie typen screening.
Zodra een werknemer niet meer in dezelfde functie werkzaam is, zal de toegang tot de geclassificeerde informatie worden beëindigd.

Voor het bestuur van de gemeente zal de invoering van de voorgestelde classificatie ook een verandering opleveren. Weliswaar kent zij al een classificatie van informatie, maar de voorgestelde classificatie heeft gevolgen voor de behandeling van informatie door het college van B&W en/ of de gemeenteraad. Op basis van de Wet Openbaarheid van Bestuur (Wob) artikel 10 kan zij informatie als geheim bestempelen. Deze informatie mag dan niet actief worden gedeeld buiten het gremium. Het schenden van deze geheimhoudingsplicht is een misdrijf in de zin van het Wetboek van Strafrecht (art. 272). Om de geheimhouding te borgen dienen leden van het college van B&W en/ of de gemeenteraad gescreend te worden.

4.2 Techniek

Het proces vraagt om een aantal functionele eisen die nader moeten worden uitgewerkt en moeten worden toegevoegd aan de Amsterdamse Digitale Werkplek (ADW) zoals versleuteling van e-mail (bijlagen) en de private clouddrive (Amsterdamse).
DICT dient hierbij de technische randvoorwaarde in te vullen, waarbij ADW de belangrijkste tool is. Tevens dient er op basis van de voorgestelde classificatie een impactanalyse te worden uitgevoerd door DICT, zodat inzichtelijk wordt wat er veranderd dient te worden. Dit gaat ook op voor functioneel beheer en gegevensmanagement. Het functionele beheer van de applicaties wordt uitgevoerd

CONCEPT

door de clusters. Deze dienen de classificatie gedurende de bewaartermijn bij te houden en beschikbaar te stellen. De betrokkenheid van het Stadsarchief zal zich met name richten op het beheer van de informatie en de betreffende classificatie.
Over de autorisatie, authenticatie en accounting zal er op basis van voorgestelde classificatie in 2014 een beleidskader worden opgeleverd door de CIO-office en SHP. Op basis hiervan kan de business samen met DICT de classificatie implementeren.
Voor de fysieke maatregelen zal in samenwerking met Dienstverlening (en/of externe leveranciers) een plan worden opgesteld. Met name de hoogste niveaus hebben impact op de te nemen maatregelen. Hierbij kan gedacht worden aan extra toegangscontrole of ruimte die afgesloten kunnen worden (bijvoorbeeld kast, brandkast of archiefruimte).

4.3 Proces

Op dit moment is alleen de bestuurlijke informatie geclassificeerd (openbaar, kabinet, beperkt kabinet). Dit betekent dat de ambtelijke informatie geclassificeerd moet worden. De classificatie wordt ingesteld per 01-08-2014 voor alle nieuwe projecten en individuele door ambtenaren gepubliceerde stukken. Als er geen opgave wordt gedaan van classificatie, dan wordt in principe de classificatie Vertrouwelijk gehanteerd, conform BIG. Dit gebeurt niet met terugwerkende kracht aangezien dat gezien de enorme aantallen bestaande documenten jaren werk zou vereisen.

Na vaststelling van de classificatie worden voor de nieuwe projecten/ programma's via het PPM-proces de classificatie opgegeven. Hierbij stelt de opsteller van het document de mogelijke rubricering voor. Bij de definitieve besluitvorming wordt de voorgestelde classificatie akkoord bevonden of aangepast in de passend niveau.

De bestuursdienst Amsterdam dient te worden betrokken om het systeem Andreas aan te passen, zodat zij in lijn is met de BIG. Hierbij zal DICT ook betrokken zijn. Daarnaast zullen de Document Management Systemen moeten worden aangepast.
De classificatie heeft een bepaalde looptijd. Hierin moet bepaald worden per informatieproces hoe lang een classificatie geldig is. Op deze manier kan geautomatiseerd de classificatie worden aangepast op het moment dat de informatie wordt overgedragen aan het Stadsarchief voor langdurige archivering. Hierbij moet de informatie aansluiten bij de geldende archiveringsregels. Na officiële overbrenging wordt de informatie openbaar. Deze openbaarheid kent op grond van de Archiefwet 1995 een drietal uitzonderingen voor bepaalde termijn:

1) de eerbiediging van de persoonlijke levenssfeer;
2) het belang van de Staat of zijn bondgenoten;
3) het anderszins voorkomen van onevenredige bevoordeling of benadeling van betrokken natuurlijke personen of rechtspersonen danwel derden.[13]

Dit betekent dat slechts het moment van openbaar worden wordt verschoven naar een later tijdstip.
De classificatie dient te worden opgenomen in de sjablonen van de gemeente. Tevens dient dit ook in het PPM-proces te worden toegevoegd als verplichte uitvraag.

Om de classificatie te bepalen worden de volgende vier stappen doorlopen:

4.3.1 Stap 1: wettelijke eisen

Op basis van wet en regelgeving kan worden bepaald welke eisen er worden gesteld aan gebruik, distributie en opslag van data. Deze zijn opgenomen in bijlage 1.

[13] Artikel 15 van de Archiefwet 1995.

CONCEPT

Voor de werkzaamheden van de gemeente is met name de Wet Bescherming Persoonsgegevens (WBP) van invloed op het classificatieniveau. Hierbij dient de medewerker de belangen tussen de wet en het proces af te wegen. Hiervoor kan een jurist of de Directie Jurdische Zaken worden ingeschakeld.

4.3.2 Stap 2: Verantwoordelijkheden t.a.v. data

De verantwoordelijkheden ten aanzien data en/ of het informatiesystemen zijn de volgende factor die het niveau bepaald. Hierbij wordt de afweging gemaakt over:
Wie de data mag gebruiken?
Wie het beschermingsniveau bepaalt? En hoe is dat vastgelegd in gebruikersrechten?
Welke business heeft een belang bij de data?
In dit proces kan de functioneel beheerder en/ of de Cluster PIB-er/ CISO worden gevraagd om te ondersteunen bij het classificeren.

4.3.3 Stap 3: Analyse kritische bedrijfsprocessen

Het classificatieniveau wordt in grote mate bepaald door het belang van het bedrijfsproces en de waarde van de data. Dit kan op basis van de vragenlijst, die wordt opgesteld met de PIB-ers. Deze lijsten dienen digitaal bewaard te worden, zodat er audits op uitgevoerd kunnen worden. Hieronder staat de BIV-rating[14] voor een aantal van de processen die binnen de gemeente worden uitgevoerd, zoals deze is opgesteld door Govcert. Er ontbreken nog enkele processen, zoals bijvoorbeeld Onderwijs/ leerplicht, de drie decentralisaties. De clusters wordt gevraagd deze classificatie nader te onderzoeken per proces..

Proces	Beschikbaarheid	Integriteit	Vertrouwelijk
Burgerzaken (klantbegeleiding, afspraken)	Belangrijk	Absoluut	vertrouwelijk
Basisregistratie persoonsgegevens	Essentieel	Absoluut	Geheim
Overige basisregistraties	Essentieel	Absoluut	Open(baar)
Indienen en behandelen beroep en bezwaarschriften	Noodzakelijk	Absoluut	Open(baar)/ vertrouwelijk
Registratie ingekomen post burgers en bedrijven	Noodzakelijk	Hoog	Intern
Beheren gevonden voorwerpen	Noodzakelijk	Beschermd	Open(baar)
Bedrijvenloket	Noodzakelijk	Beschermd	Open(baar)
Publicatie van ruimtelijke plannen	Noodzakelijk	Absoluut	Open(baar)
Grootschalige Basiskaart Nederland (GBKN)	Noodzakelijk	Absoluut	Open(baar)
Kenbaarstelling Publiekrechtelijke beperkingen (WKPB)	Noodzakelijk	Absoluut	Open(baar)
Registratie risico's gevaarlijke stoffen (risicokaart)	Essentieel	Absoluut	Intern
Bodembeheer	Noodzakelijk	Hoog	Open(baar)
Aanvraag en verlening vergunning	Noodzakelijk	Absoluut	Vertrouwelijk
Bouw- en woningtoezicht	Noodzakelijk	Absoluut	Vertrouwelijk
Financieel beheer (betalingen leges, etc.)	Noodzakelijk	Hoog	Vertrouwelijk
Aangifte en heffing gemeentelijke	Noodzakelijk	Hoog	Vertrouwelijk

[14] Onderzoek Govcert, 2007

CONCEPT

belastingen/ heffingen			
Waardebepaling Onroerende Zaken (WOZ)	Noodzakelijk	Hoog	Intern
Sociale Zaken – Uitvoering/ verstrekkingen voorzieningen	Essentieel	Hoog	Geheim
Sociale Zaken – Handhaving en controle	Noodzakelijk	Absoluut	Geheim
Openbare Orde en veiligheid	Essentieel	Absoluut	Geheim
Handhaving en toezicht gemeentelijke verordeningen	Noodzakelijk	Absoluut	Vertrouwelijk
Gezondheidszorg – GGD	Belangrijk	Absoluut	Geheim

4.3.4 Stap 4: Afweging: criteria bij het bepalen van het classificatieniveau

Classificeren van data zal per situatie verschillen. Dit komt doordat de waarde van de data van belang is. Het risico op verlies van data dient te worden meegenomen in deze afweging. Met name de maatregelen hier tegen zijn een factor in de classificatie.

De Wet Bescherming Persoonsgegevens geeft in artikel 13 drie criteria over deze maatregelen:

1. De stand der techniek; wat is er beschikbaar en wat is nog relevant.
2. De kosten van de tenuitvoerlegging; de classificatie moet zowel technisch als organisatorisch niet tot hoge kosten leiden.
3. De risico's van verwerking van persoonsgegevens; hiermee wordt het risico bepaald van de verwerking. Hoe hoger de kans op verlies of onrechtmatige verwerking, des te hoger de classificatie van de data.

KING raad aan om de classificatie in workshop tot stand te brengen. Dit leidt tot een gewogen gemiddelde, wat op de langere termijn beter in stand te houden is.

Het beveiligingsniveau in de tactische Baseline (BIG) is:
Beschikbaarheid: Noodzakelijk
Integriteit: Hoog
Vertrouwelijkheid: Vertrouwelijk

Hiermee worden de meeste processen en ICT-voorzieningen voldoende gedekt. Zodra uit het classificatieproces blijkt dat de niveaus hoger zijn, dienen er op die onderdelen extra maatregelen te worden afgesproken.

CONCEPT

Bijlage 1

De juridische grondslag voor informatiebeveiliging is terug te vinden in wet- en regelgeving, zoals onder meer de Wet Bescherming Persoonsgegevens (WBP). Informatiebeveiliging en bescherming van persoonsgegevens zijn onlosmakelijk met elkaar verbonden. De WBP regelt in artikel 13 welke maatregelen organisaties moeten treffen in het kader van informatiebeveiliging om op een adequate manier persoonsgegevens te beschermen. Voor wat betreft de gemeente is daarnaast uitgegaan van de verwerking van persoonsgegevens, zoals bedoeld in artikel 16 van de WBP. Deze maatregelen maken deel uit van het informatiebeveiligingsbeleid van een gemeente. Er zijn veel wetten en regelgeving van toepassing op de gemeente. De gemeente dient zich aan al deze wetten en regelgeving te houden, waaruit maatregelen ontstaan op het gebied van informatiebeveiliging. Wetten en regelingen die van toepassing zijn (niet limitatief):

- Wet Bescherming Persoonsregistratie en Vrijstellingsbesluit
- Wet Bescherming Persoonsregistratie (WBP)
- Wet Openbaarheid van Bestuur (WOB)
- Wet Computercriminaliteit II
- Comptabiliteitswet
- Archiefwet
- Wet Particuliere Beveiligingsorganisaties en Recherchebureaus (WBPR)
- Wet Veiligheidsonderzoeken (WVO)
- Wet Politiegegevens (WPG)
- Ambtenarenwet
- Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007)
- Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie (VIRBI2012)
- Beveiligingsvoorschrift 2005 (BVR)
- CAR-UWO
- PUN
- Algemene Rijksvoorwaarden bij IT-overeenkomsten (ARBIT2010)
- Kader Rijkstoegangsbeleid
- Uitgangspunten online communicatie rijksambtenaren
- Programma van Eisen PKI Overheid
- Code voor Informatiebeveiliging (ISO 27001:2005 en ISO 27002:2007)
- Telecommunication Infrastructure Standard for Data Centers (TIA-942)
- Wet SUWI
- Wet op de identificatieplicht
- Wet Elektronisch Bestuurlijk Verkeer (WEBV)
- Wet GBA en wet BRP
- Wet Werk en Bijstand
- Wet Openbaar Bestuur
- Algemene wet bestuursrecht
- Richtlijnen van het NCSC

Tot slot dient de doelbinding te worden opgenomen. Hiermee kan worden bepaald of informatie een hogere classificatie behoeft.

CONCEPT