Beleid Informatieveiligheid 2020-2024

Gemeente 's-Hertogenbosch

Definitief

’s-Hertogenbosch, 23-12-2019

A. Kieboom

Projectidentificatie

Projectnaam: Beleid Informatieveiligheid
Status: Definitief

Documenthistorie

Status	Datum	Versie	Auteur(s)	Toelichting
Concept	05-10-00	0.1	A. Kieboom	· Voorgelegd aan controllersoverleg
Definitief	19-02-01	1.0	A. Kieboom	· Definitieve versie; vastgesteld door Controllersoverleg en het College van B&W (in juli 2003)
Definitief	06-10-06	1.0	A. Kieboom	· Tekstuele aanpassing
Definitief	27-12-10	2011-2015	A. Kieboom	· Tekstuele aanpassing · Aanpassingen aan huisstijl
Definitief	28-05-13	2013-2017	A. Kieboom	· Tekstuele aanpassing
Definitief	10-01-14	2014-2018	A. Kieboom	· Tekstuele aanpassing · Expliciete aandacht voor beveiliging Suwinet · Expliciete aandacht voor bewustwording informatieveiligheid medewerkers · Normenkader Baseline Informatiebeveiliging Gemeenten (BIG) als uitgangspunt voor beveiligingsplannen
Definitief	30-10-15	2015-2019	A. Kieboom	· Tekstuele aanpassingen
Definitief	03-11-17	2017-2021	A. Kieboom	· Tekstuele aanpassingen
Definitief	18-09-18	2018-2022	A. Kieboom	· Aangepast aan AVG
Definitief	23-12-19	2020-2024	A. Kieboom	· Aangepast aan BIO

Auteur(s) laatste versie

Naam	Afdeling/organisatie	Rol
A. Kieboom	FIB/ICT	Adviseur Informatiebeveiliging

Inhoud

1 Inleiding

Het voorliggende “Beleid Informatieveiligheid 2020-2024” geeft richting en biedt ondersteuning aan de leiding van de organisatie om de informatiebeveiliging binnen de organisatie daadwerkelijk en krachtig door te voeren.

Het Beleid Informatieveiligheid is een beschrijving van strategische uitgangspunten en de kernpunten van het beveiligingsbeleid. Ook is de beveiligingsorganisatie en de beveiligingscyclus binnen de gemeente beschreven. Middels het “Beleid Informatieveiligheid gemeente ’s-Hertogenbosch” onderschrijft de leiding van de gemeente ’s-Hertogenbosch de doelstellingen en principes van de informatiebeveiliging. Het “Beleid Informatieveiligheid gemeente ’s-Hertogenbosch” vormt daarom het uitgangspunt voor effectuering van het Beleid Informatieveiligheid in de gehele organisatie.

2 Beleid Informatieveiligheid

2.1 Aanleiding

Het ambtelijk management van de gemeente ‘s-Hertogenbosch onderkent dat het toenemende gebruik van datacommunicatiemogelijkheden (internet), de complexiteit van en verwevenheid tussen geautomatiseerde systemen, de massaliteit van de dagelijkse communicatie, de omvang van de bestanden alsmede de toenemende professionalisering van de computercriminaliteit leiden tot een grote afhankelijkheid en kwetsbaarheid van de geautomatiseerde informatievoorziening binnen de gemeente ’s-Hertogenbosch. De risico's die hiermee samenhangen zijn zeer aanzienlijk en kunnen een bedreiging vormen voor de vertrouwelijkheid, integriteit en continuïteit van de informatie en kunnen van essentieel belang zijn voor de bedrijfsvoering van de organisatie, het naleven van de wet en het imago van de gemeente ‘s-Hertogenbosch

2.2 Definitie

De definitie van informatieveiligheid luidt als volgt:

"Het bieden van een raamwerk van beleidsuitgangspunten met betrekking tot de exclusiviteit, integriteit en beschikbaarheid van de informatievoorziening, waarbinnen een evenwichtig (doeltreffend en doelmatig) stelsel van onderling samenhangende maatregelen ontwikkeld wordt, teneinde de geautomatiseerde informatievoorziening te beschermen tegen interne en externe bedreigingen."

2.3 Afbakening

Het Beleid Informatieveiligheid behandelt de strategische uitgangspunten, de kernpunten op het gebied informatieveiligheid en de beveiligingsorganisatie zoals ze de komende jaren door de gemeente ’s-Hertogenbosch worden gehanteerd.

2.4 Doelstelling en doelgroep

Het Beleid Informatieveiligheid maakt deel uit van het algehele beveiligingsbeleid van gemeente ’s-Hertogenbosch.

Alle leidinggevenden dienen ervoor zorg te dragen, dat aan de in het Beleid Informatieveiligheid geformuleerde beleidsuitgangspunten wordt voldaan bij de inrichting van de organisatie, procedures, werkwijze en de daarbij gehanteerde informatiesystemen.

De belangrijkste doelstelling van het Beleid Informatieveiligheid luidt:

“Het bieden van richting en ondersteuning aan het management ten behoeve van de informatiebeveiliging. Het management geeft een duidelijke richting aan en demonstreert dat zij informatiebeveiliging een hoge prioriteit geeft door het accorderen van het Beleid Informatieveiligheid voor de gemeente ’s-Hertogenbosch”

Overige doelstellingen van het Beleid Informatieveiligheid:

- Bepalen strategische uitgangspunten.
- Toewijzen eindverantwoordelijkheden voor informatiebeveiliging en bepalen van de beveiligingsorganisatie.
- Het beschrijven van de kernpunten voor beveiliging. De kernpunten voor beveiliging bieden een primair uitgangspunt voor een totale informatiebeveiliging binnen de gemeente ’s-Hertogenbosch.

2.5 Strategische uitgangspunten

De strategische uitgangspunten vormen de basis, die wordt gebruikt voor de vertaling van de Baseline Informatiebeveiliging Nederlandse Overheid (BIO) naar de kernpunten van het Beleid Informatieveiligheid van de gemeente ’s-Hertogenbosch.

- De informatieveiligheid van de gemeente ‘s-Hertogenbosch sluit aan bij haar bedrijfsconcept, waarin het fundament gelegd wordt voor een cultuur waarin betrouwbaarheid, continuïteit, integriteit en authenticiteit de basis vormen.
- Alle relevante wet- en regelgeving met betrekking tot omgang met informatie (o.a. privacy, archivering, openbaarheid bestuur) is richtinggevend voor de maatregelen op het gebied van informatieveiligheid binnen onze organisatie.
- De gemeente ’s-Hertogenbosch streeft geen maximaal beveiligingsniveau na, maar een optimaal niveau, waarbij, op basis van een risicoafweging door het management, wordt uitgegaan van reducering van de informatieveiligheidsrisico's tegen acceptabele kosten. Dit is van toepassing op alle volgende uitgangspunten op het gebied van informatieveiligheid:

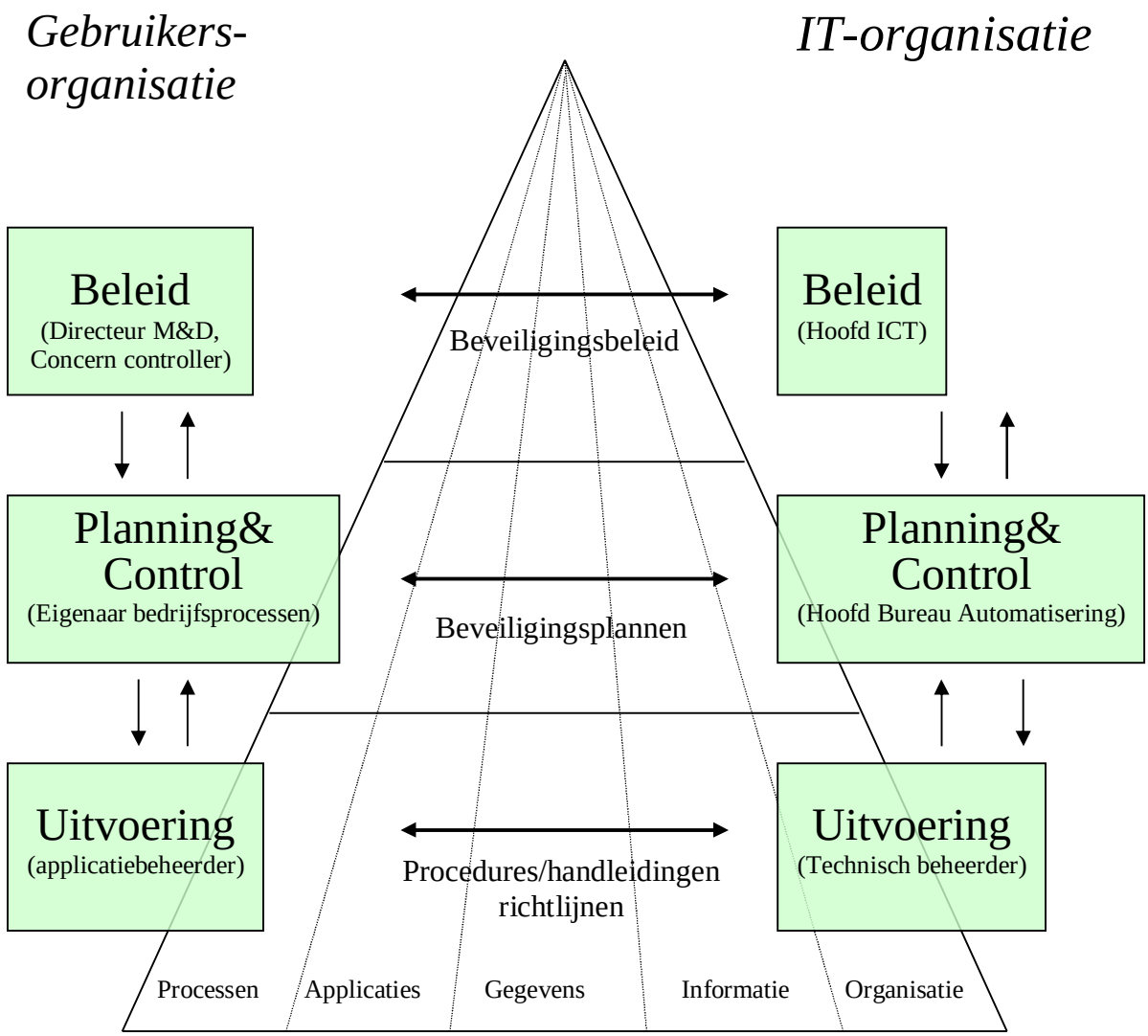
  . Het personeelsbeleid is er mede op gericht een bijdrage te leveren aan de vertrouwelijkheid, integriteit, continuïteit en authenticiteit van de informatievoorziening van onze organisatie;
  . Opdrachten aan derden voor het uitvoeren van werkzaamheden worden zodanig omgeven met maatregelen dat er geen inbreuk op de vertrouwelijkheid, integriteit en continuïteit van de geautomatiseerde informatievoorziening kan ontstaan.

  . De fysieke toegangsbeveiliging zorgt ervoor dat ongeautoriseerde personen geen toegang krijgen tot de bedrijfsgebouwen, en computerruimten in het bijzonder.
  . Logische toegangsbeveiliging zorgt ervoor dat ongeautoriseerde personen of processen geen toegang krijgen tot de geautomatiseerde systemen, gegevensbestanden en programmatuur van de gemeente ‘s-Hertogenbosch.

  . Er zijn calamiteitenplannen en -voorzieningen om de continuïteit van de geautomatiseerde informatievoorziening te waarborgen.
  . Aanschaf, installatie en onderhoud van geautomatiseerde gegevensverwerkende systemen, alsmede inpassing van nieuwe technologieën, mogen geen afbreuk doen aan het niveau van veiligheid van de geautomatiseerde informatievoorziening.
  . Bij de geautomatiseerde informatievoorziening zijn strikte scheidingen aangebracht tussen de ontwikkelingsomgeving, de test/acceptatie-omgeving en de productie-omgeving.
  . Er zijn voorzieningen aanwezig om de inhoudelijke juistheid, de volledigheid en de juiste werking van de geautomatiseerde systemen te kunnen vaststellen.
  . Datatransport is zodanig met beveiligingsmaatregelen omkleed, dat geen inbreuk kan worden gepleegd op de vertrouwelijkheid, integriteit van de gegevens en de informatievoorziening als geheel.
  . Teneinde computervirusinfecties te voorkomen wordt er slechts gewerkt met geautoriseerde versies van (legale) programmatuur.
  . Het beheer en de opslag van gegevens is zodanig dat geen informatie verloren kan gaan.

2.6 Beveiligingsorganisatie

De gebruiksorganisatie is en blijft, als eigenaar van de bedrijfsprocessen, eindverantwoordelijke voor de door haar gebruikte (geautomatiseerde) informatiesystemen en processen. Bureau Automatisering is de houder van de overeengekomen technische infrastructuur, met inbegrip van de infrastructurele beveiligingsmiddelen en biedt een basis beveiligingsniveau van de technische infrastructuur aan.

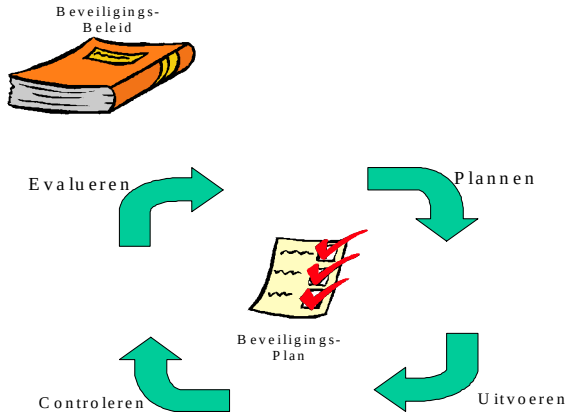


De verantwoordelijkheden voor de bescherming van individuele gegevens en voor het uitvoeren van bepaalde beveiligingsprocedures dienen expliciet in de beveiligingsplannen te worden gedefinieerd.

De afdeling SIM BAZ/M&D is verantwoordelijk voor het beheer en de opslag van documenten, voor wat betreft de permanent te bewaren archiefbescheiden is dit een taak van de afdeling Erfgoed.

Gelet op de mogelijke impact van verstoringen op de continuïteit van de gemeente 's-Hertogenbosch berust eindverantwoordelijkheid voor het beleid inzake de beveiliging en de interne controle van de geautomatiseerde informatievoorziening bij de sectordirecteuren van de gemeente 's-Hertogenbosch.

De beveiligingscyclus verloopt nu als volgt: Op basis van het Beleid Informatieveiligheid en een risicoanalyse kunnen door de eigenaren (eventueel met ondersteuning security officer) van de informatiesystemen en processen beveiligingsplannen worden gemaakt waarin expliciete beveiligingsmaatregelen en een invoeringsplan worden gedefinieerd. Als uitganspunt worden hierbij de normen uit de Baseline Informatiebeveiliging Overheid (BIO) gehanteerd. De beveiligingsplannen worden vervolgens geïmplementeerd de door de technisch beheerder of de applicatie beheerder. Hierover wordt gerapporteerd aan de eigenaar van het informatiesysteem. Ook zullen er periodiek audits plaatsvinden waarvoor de eigenaar van het systeem opdracht geeft. Dit kunnen zowel interne als externe audits (externe accountant) zijn. De auditprocedure dient een onderdeel te zijn van het beveiligingsplan. Vervolgens zal bij evaluatie blijken of de beveiligingplannen en eventueel het beveiligingsbeleid dienen te worden bijgesteld.



2.7 Kernpunten Beleid Informatieveiligheid

De navolgende kernpunten zijn afgeleid uit de Baseline Informatiebeveiliging Overheid. De paragrafen 2.7.11 tot en met 2.7.33 vinden hun oorsprong in wet- en regelgeving, De paragrafen 4 tot en met 2.7.88 zijn zogenaamde '*best practices*' die bij het opzetten van de informatiebeveiliging de eerste aandacht verdienen. Deze punten worden nader uitgewerkt in het beveiligingsbeleid. Daarna kunnen overige maatregelen worden getroffen zoals eveneens beschreven in de BIO. Deze maatregelen worden opgenomen in het Plan Informatieveiligheid.

2.7.1 Beveiliging van gemeentelijke documenten

Belangrijke gemeentelijke documenten dienen te worden beveiligd tegen verlies, vernietiging en vervalsing. Uitgangspunten hierbij zijn o.a. het Besluit Informatiebeheer gemeente ’s-Hertogenbosch, de archiefwet, de archiefverordening gemeente 's-Hertogenbosch, de regeling geordende en toegankelijke staat archiefbescheiden, de regeling duurzaamheid archiefbescheiden en de Wet openbaarheid van bestuur.

2.7.2 Naleving van de wet- en regelgeving inzake bescherming persoonsgegevens

Toepassingen waarin gegevens over personen worden verwerkt, dienen te voldoen aan de Algemene Verordening Gegevensbescherming (AVG), de Wet basisregistratie personen, de Wet meldplicht datalekken, Paspoortuitvoeringsregeling Nederland 2001 en de Regeling SUWI. In het kader van Regeling SUWI is het Suwinet-Normenkader leidend voor de te nemen beveiligingsmaatregelen.

2.7.3 Voorkomen van onrechtmatig kopiëren van programmatuur

Auteursrechtelijk beschermd materiaal mag niet worden gekopieerd zonder toestemming van de eigenaar.

2.7.4 Beleidsdocument voor informatieveiligheid

Voor alle werknemers van de gemeente ’s-Hertogenbosch die verantwoordelijk zijn voor informatiebeveiliging dient een beleidsdocument beschikbaar te zijn. Dit document kan door de medewerker gebruikt om het Beleid Informatieveiligheid te vertalen naar passende maatregelen in het eigen gebied, vastgelegd in het beveiligingsplan voor dit gebied.

2.7.5 Toewijzing van verantwoordelijkheden voor informatieveiligheid

Van elk (geautomatiseerd) informatiesysteem, inclusief de daarbij behorende gegevens, dient expliciet één eigenaar te zijn benoemd. Het eigenaarschap impliceert de eindverantwoordelijkheid voor het betreffende systeem. Er wordt gesproken over **eind**verantwoordelijk omdat een aantal aspecten van het informatiesysteem uitbesteedt worden aan andere eigenaren.

2.7.6 Training, opleiding en bewustwording voor informatieveiligheid

Alle medewerkers behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige (bij)scholing van beleidsregels en procedures op het gebied van informatieveiligheid, voor zover relevant voor hun functie.

2.7.7 Rapportage beveiligingsincidenten

Beveiligingsincidenten dienen zo snel mogelijk via de juiste kanalen te worden gerapporteerd. Een beveiligingsincident is een gebeurtenis die ervoor heeft gezorgd, of ervoor had kunnen zorgen, dat bedrijfsmiddelen zijn beschadigd of verloren geraakt.

2.7.8 Het proces van continuïteitsplanning

Er dienen procedures te worden opgesteld voor het ontwikkelen en handhaven van continuïteitsplannen voor de gehele organisatie, met name voor wat betreft kritieke processen en diensten. Tenminste onderstaande onderdelen moeten in een continuïteitsplan aan de orde komen:

- Procedures voor noodsituaties: de beschrijving van de verantwoordelijkheden en de activiteiten die onmiddellijk na een calamiteit moeten worden ondernomen.
- Uitwijkprocedures: de beschrijving van de activiteiten die worden ondernomen om de kritieke bedrijfsprocessen en systemen, eventueel op alternatieve wijze, door te laten draaien of om deze processen of systemen zo spoedig mogelijk weer op gang te brengen. Belangrijk zijn hierbij afhankelijkheden en contracten met externe partijen.
- Vervolgprocedures: de activiteiten die de oorspronkelijke situatie en de normale bedrijfsvoering herstellen.
- Testschema's: oefenen, testen en up-to-date houden van de plannen. Continuïteitsplannen dienen regelmatig, minimaal één maal per jaar en altijd na belangrijke wijzigingen te worden getest.