Bijlage 1 – Begrippenlijst

Applicatie:
Een applicatie is software die bedoeld is voor computers of mobiele apparaten zoals smartphones, tablets en smartwatches.

Bedrijfsmiddel:
Elk middel waarin of waarmee bedrijfsgegevens kunnen worden opgeslagen en/of verwerkt en waarmee toegang tot gebouwen, ruimten en IT-voorzieningen kan worden verkregen:
een bedrijfsproces, een gedefinieerde groep activiteiten, een gebouw, een apparaat, een IT-voorziening of een gedefinieerde groep gegevens.

Beschikbaarheid / Continuïteit:
Het zorg dragen voor het beschikbaar zijn van informatie en informatieverwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers.

Beveiliging:
Het brede begrip van informatiebeveiliging, d.w.z. inclusief fysieke beveiliging, bedrijfscontinuïteitsbeheer, ofwel beschikbaarheid van bedrijfsprocessen en persoonlijke veiligheid en integriteit.

Beveiligingsincident:
Informatiebeveiligingsincidenten zijn alle gebeurtenissen die inbreuk maken op de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens en bijbehorende processen.

Baseline Informatiebeveiliging Overheid (BIO):
De BIO is het normenkader voor informatiebeveiliging binnen de overheid, lees Rijksdienst, Provincie, Waterschappen, Gemeentes. De BIO kan gezien worden als de ‘kapstok’ waaraan de elementen van informatiebeveiliging opgehangen kunnen worden. Centraal staat de organisatie en de verantwoording over informatiebeveiliging binnen de gemeenten.De BIO bevordert de beschikbaarheid, integriteit en vertrouwelijkheid van gemeentelijke informatie(systemen). Deze BIO is een richtlijn die een totaalpakket aan informatiebeveiligingscontrols en –maatregelen omvat die voor iedere noodzakelijk is om te implementeren.

Classificatie:
Systematische identificatie en/of ordening van bedrijfsactiviteiten en/of records in categorieën overeenkomstig logisch gestructureerde afspraken, methodieken en procedurele voorschriften.

Cloud (applicatie):
Cloud is het via een netwerk – vaak het internet – op aanvraag beschikbaar stellen van software (waaronder applicaties) en gegevens, buiten de eigen infrastructuur.

ENSIA:
Eenduidige Normatiek Single Information Audit is een systematiek om verschillende informatiebeveiligingsonderdelen in audits en zelfevaluaties samen te voegen.

Gegeven:
Weergave van een feit, begrip of aanwijzing, geschikt voor overdracht, interpretatie of verwerking door een persoon of apparaat. Gegevens op zich behoeven niet noodzakelijkerwijs te zijn vastgelegd.

Governance:
Stelsel van regels met betrekking op goed bestuur, toezicht en verantwoording. Betrokkenen dienen zich, los van vastgestelde regels, te houden aan toepasselijke waarden en normen.

Hardware:
Dit is een verzamelnaam voor alle fysieke onderdelen die samenhangen met het computersysteem, zoals de computer zelf, de servers, het fysieke netwerk, de monitor, de printer en de modem.

IT-voorzieningen:
Applicaties en technische infrastructuur waarop deze applicaties zijn geïnstalleerd.

Informatie:
Betekenisvolle gegevens verzameld en uitgewerkt om te dienen als communicatie tussen personen. Informatie behoeft evenmin als gegevens noodzakelijkerwijs te zijn vastgelegd.

Informatiebeheer:

1. Het systematisch verzamelen, verwerken, toegankelijk maken, gebruiken, onderhouden en verwijderen van informatie, opdat deze duurzaam toegankelijk en betrouwbaar is. De informatiebeheerder ondersteunt de gebruiker, die informatie creëert en raadpleegt.
2. De inrichting en uitvoering van het opslaan, het bewaren en beheren, het ontsluiten of (actief) leveren, en waar nodig, het overdragen, verplaatsen, verwijderen of vernietigen van informatie.

Informatiebeveiliging:
Het proces van vaststellen van de vereiste betrouwbaarheid van informatieverwerking in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.

Informatiesysteem:
Een samenhangend geheel van gegevensverzamelingen en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie.

Integriteit:
Het waarborgen van de juistheid en volledigheid en tijdigheid van informatie en de verwerking ervan. Als de tijdigheid van gegevens bepaald wordt door omstandigheden buiten het systeem, kan deze vanzelfsprekend niet als integriteitseis voor het systeem gesteld worden.

Integriteit / betrouwbaarheid:
Het waarborgen van de juistheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking.

1. Informatie is betrouwbaar als zij authentiek en volledig is.
2. Een record is betrouwbaar als de inhoud kan worden vertrouwd als een volledige en nauwkeurige weergave van de transacties, activiteiten of feiten waarvan het getuigt en waarop men zich kan verlaten bij de uitvoering van latere transacties of activiteiten.

IT-infrastructuur:
Dit is de fysieke verkeersinfrastructuur ten behoeve van het transport van digitale data, met als hoger doel informatie te delen of aan te bieden en te consumeren

Planning en Control:
Planning en control omvat „strategic planning", „management control" en „task control". Het is het proces van besluitvorming over - het bereiken van - de strategische doelen van de organisatie, het toedelen van taken aan leden van een organisatie om deze strategie te implementeren en het waarborgen dat de taken effectief en efficiënt worden uitgevoerd.
NB. Control is niet hetzelfde als controle!

Software:
Programma's die een computer (of ander apparaat) een bepaalde taak laten vervullen zoals spelletjes, tekstverwerker, webbrowser, etc.

Technische infrastructuur:
Het deel van de IT-infrastructuur dat is gericht op de exploitatie van de systemen (hardware, systeemsoftware, bijbehorende documentatie, etc.). Samen met de applicatiesoftware en de bijbehorende documentatie en procedures vormt dit de IT- infrastructuur.

Toegankelijk:
Informatie is toegankelijk als deze vindbaar, interpreteerbaar en uitwisselbaar is voor daartoe bevoegde personen of systemen.

Vertrouwelijkheid / Exclusiviteit:
Het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.

Volledig:
Informatie met betrekking tot een proces is volledig als alle informatie is vastgelegd en wordt beheerd die aanwezig zou moeten zijn conform het beheerregime dat voor dat proces is vastgesteld.

Bijlage 2. Rollen en verantwoordelijkheden

Gemeenteraad
De gemeenteraad stelt middelen beschikbaar voor informatiebeveiliging. Daarnaast heeft de gemeenteraad een controlerende functie ten aanzien van de informatiebeveiliging.

College van Burgemeester & Wethouders / Dagelijks Bestuur
Het college van B&W / DB is eindverantwoordelijk voor de adequate beveiliging van informatie binnen de gemeente. Eén lid van het college heeft informatiebeveiliging expliciet in de portefeuille. Het is de verantwoordelijkheid van het college om dit proces te faciliteren door:

- het informatiebeveiligingsbeleid vast te stellen;
- ervoor te zorgen dat voldoende middelen beschikbaar gesteld worden voor de adequate inrichting van informatiebeveiliging;
- toezicht te houden op de uitvoering van het informatiebeveiligingsbeleid;

MT (lijnmanagement)
Het MT is in haar sturende rol verantwoordelijk de uitvoering van het informatiebeveiligingsbeleid. Eén lid van het MT heeft informatiebeveiliging expliciet in het takenpakket. Het MT zorgt ervoor dat zij:

- stuurt op bedrijfsrisico's;
- controleert of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze voldoende bescherming bieden;
- toezicht houdt op de uitvoering van het informatiebeveiligingsplan;
- een positieve en actieve houding heeft ten aanzien van informatiebeveiliging;
- zorg draagt dat de medewerkers voldoende security training krijgen om de taken goed te kunnen uitvoeren;
- fungeert als voorbeeld richting de medewerkers.

Chief Information Security Officer (Informatiebeveiligingsfunctionaris)
De CISO is verantwoordelijk voor de organisatie van informatiebeveiliging. Dit is een rol op strategisch niveau binnen de gemeentelijke organisatie. De CISO heeft als taak informatiebeveiliging op een hoger niveau te brengen en om het vervolgens structureel te laten borgen in de organisatie. De lijnorganisatie blijft zelf verantwoordelijk voor informatiebeveiliging. De belangrijkste bevoegdheid van de CISO is om op elke plek binnen de organisatie gevraagd en ongevraagd onderzoek te kunnen (laten) doen en zo nodig zaken voor te schrijven. De taken van de CISO ten aanzien van informatiebeveiliging zijn als volgt samen te vatten:

- Beleid & Coördinatie
- Controle & Registratie
- Communicatie & Voorlichting
- Advies & Rapportage

Functionaris Gegevensbescherming
De Functionaris Gegevensbescherming (FG) houdt zich bezig met alle privacyaspecten binnen de gemeente. De functie is onafhankelijk van de lijn belegd en de functionaris heeft de bevoegdheid om rechtstreeks naar de gemeentesecretaris of het college van B&W te rapporteren. De taken van de FG zijn:

- adviseren (zowel gevraagd als ongevraagd) over vraagstukken die te maken hebben met de omgang met persoonsgegevens;
- toezien op de naleving van de AVG en andere privacy-gerelateerde wet- en regelgeving binnen de organisatie;
- het informeren van de organisatie betreffende de AVG en andere privacy-gerelateerde wet- en regelgeving;
- het zijn van een contactpunt voor betrokkenen (dit kunnen zowel inwoners als medewerkers zijn) m.b.t. de omgang met persoonsgegevens. De FG is daarbij gehouden aan geheimhouding;
- het coördineren van de afhandeling van datalekken conform de vastgestelde datalekprocedure;
- het contactpunt met de Autoriteit Persoonsgegevens.

Privacy Officer
De privacyofficer is verantwoordelijk voor de uitvoering en naleving van de privacywetgeving. Daarnaast adviseert de Privacy Officer over privacybescherming en activiteiten ter bescherming van persoonsgegevens.

Beveiligingsfunctionaris Burgerzaken
De beveiligingsfunctionaris is bevoegd om een jaarlijks intern onderzoek in te stellen naar de werking van de beveiligingsprocedures ten aanzien van reisdocumenten en rijbewijzen. Het college van B&W krijgt inzicht in de rapportage van bevindingen.

Security Officer Suwinet
De Security Officer Suwinet is binnen de organisatie toezichthouder betreft het proces rondom informatiebeveiliging binnen het Suwinetdomein en rapporteert direct aan het DB (zie ook aansluitbeleid Suwinet).

Proceseigenaren
De proceseigenaar gaat over de inrichting, het ontwerp en de resultaten van het proces. Hiervoor dient de proceseigenaar het proces te analyseren, risico's in kaar te brengen en passende maatregelen te treffen. Proceseigenaren informeren het lijnmanagement en de directie zodat zij beslissingen kunnen nemen ten aanzien van informatiebeveiliging.

Technisch applicatiebeheerder
De technisch applicatiebeheerder is verantwoordelijk voor het inrichten en in stand houden van de programmatuur.

Functioneel beheerder
De functioneel beheerder zorgt ervoor dat de applicatie is ingericht conform de daarvoor gestelde eisen en richtlijnen. De functioneel beheerder is verantwoordelijk voor het onderhouden van de programmatuur en het inregelen van de juiste autorisaties binnen de applicatie.

Gegevensbeheerder
De gegevensbeheerder is in een of meerdere informatiesystemen verantwoordelijk voor het geheel van activiteiten gericht op de inhoudelijke kwaliteitszorg betreffende het gegevens verzamelen, de gegevensverwerking en de informatievoorziening.

Het Shared Service Center (SSC) De Kempen
Het SSC De Kempen beheert de werkplekken, server platformen, lokale netwerken, WiFi verbindingen, externe netwerkverbindingen (zoals Gemnet en SUWInet) en verzorgt het technische (wijzigings-)beheer van databases, bedrijfsapplicaties en kantoorautomatisering hulpmiddelen. Verder zijn zij mede verantwoordelijk voor alle technische aansluitingen op andere ketenpartners en landelijke voorzieningen. Daarnaast zijn zij verantwoordelijk voor de implementatie van technische beveiligingsmaatregelen. Verantwoording over het gevoerde beheer van de getroffen beveiligingsmaatregelen wordt aan de procesverantwoordelijken voor (informatie-)systemen afgelegd. Namens SSC De Kempen sluit de beveiligingsbeheerder IT aan bij het informatieveiligheidsoverleg.

Facilitaire zaken
Facilitaire Zaken is lokaal geregeld (elke vestiging heeft een eigen facilitair beheerder). Zij zijn verantwoordelijk voor de fysieke toegangsbeveiliging en kantoorinrichting.

Personeelszaken
Personeelszaken is verantwoordelijk voor de advisering inzake de personele en de organieke aspecten binnen de organisatie en speelt hiermee een belangrijke adviesrol op het gebied van organisatie en informatieprocessen.