Beleid

Leden van de gemeenteraad
Fractie Hart voor Bloemendaal
t.a.v. de heer R.M. Slewe
Postbus 201
2050 AE OVERVEEN

Gemeente Bloemendaal
Postbus 201
2050 AE Overveen
T 14 023
www.bloemendaal.nl

Datum	:	17 december 2019
Ons kenmerk	:	2019008224
Behandeld door	:	College
Doorkiesnummer	:	023-5225555
Onderwerp	:	reactie op artikel 40 RvO vraag (2019007969) m.b.t. back up beleid/ college en audit commissie
Verzonden	:	
Bijlage(n)	:	Tactisch Informatieveiligheidsbeleid

Geachte heer Slewe,

Op 25 november 2019 heeft u vragen gesteld over het back-up beleid van de gemeente. In deze brief leest u onze reactie.

Vraag 1
Kunt U mij een kopie van het back up beleid overhandigen? Aangezien het een wettelijke verplichting is moet het er zijn.

Antwoord 1
Bijgevoegd het in 2017 door de Raad vastgestelde Tactische Informatieveiligheidsbeleid.

Vraag 2
Wordt de gemeente Bloemendaal jaarlijks geaudit?

Antwoord 2
In 2017 is de ENSIA audit voor alle overheden ingevoerd. Ook de gemeente Bloemendaal doet hier met ingang van 2017 aan mee.

Vraag 3
Voer de gemeente deze Ensia audit uit?

Antwoord 3
Ja, met ingang van 2017 voert de gemeente de ENSIA audit jaarlijks uit. Dit is een zelfaudit aan de hand van het verplichte normenstelsel voor Informatieveiligheid voor gemeenten (de BIG). Deze zelfaudit wordt door een externe auditor gecheckt.

Vraag 4
Tekent de burgemeester ook jaarlijks een Ensia verklaring?

Antwoord 4
De rapportage van de zelfaudit met de verslagen van de auditor wordt in het voorjaar door het college van burgemeester en wethouders vastgesteld. In juni worden deze stukken gezamenlijk met de financiële jaarlijkse verantwoording aan de gemeenteraad voorgelegd.

Vraag 5
Kunt U ons laten weten wie die verklaringen met betrekking op de informatiebeveiliging heeft getekend de afgelopen jaren (vanaf 2010 svp)? Graag document met handtekening.

Antwoord 5
De ENSIA audit is pas in 2017 ingegaan. Deze stukken zijn door het college vastgesteld en zijn door het college in 2017 en 2018 aan de raad voorgelegd.

Vraag 6
Kunt U mij verklaren hoe het dan mogelijk is dat aan de heer Schneiders is medegedeeld door de gemeentesecretaris en vanuit de organisatie dat er geen back up is?

Antwoord 6
Als er gevraagd is naar data die langer dan een half jaar geleden is verwijderd, dan klopt het dat daar geen back-up van is, dat is conform het uitgewerkte beleid.
De back-up is een instrument om de continuïteit van de bedrijfsvoering te waarborgen. Bedoeld om bij verstoringen, incidenten of crashes programmatuur en bijbehorende data terug te kunnen zetten. Met de bedoeling dat de verstoring zo kort mogelijk is, en verlies van gegevens beperkt wordt.
Voor programmatuur (alle software waar de gemeente specifieke processen in worden uitgevoerd) en de bijbehorende data worden dagelijkse back-ups gemaakt die twee weken worden bewaard, en een weekendback-up die 26 weken wordt bewaard. De manier waarop deze systemen werken houdt in dat de back-up overschreven wordt als de maximale bewaartermijn is verstreken (respectievelijk 14 dagen en 26 weken).

Vraag 7
Kunt U mij verklaren waarom wethouder de Rooij, Tames Kokke en Ict medewerker V voor de rechter hebben verklaard dat er geen back up is en dus mails niet konden worden teruggehaald?

Antwoord 7
Indien u doelt op een rechtszaak die u als privé persoon voerde tegen een besluit op één van uw Wob-verzoeken, dan betreft dit een privé aangelegenheid. In deze zaak is onherroepelijk uitspraak gedaan.

Met vriendelijke groet,

burgemeester en wethouders van Bloemendaal,

, burgemeester

, secretaris

Tactisch gemeentebreed informatieveiligheidsbeleid

Versie	: Definitief 2.0
Auteurs	: Wineke de Porto, Ugur Balci
Begeleiding	: Ugur Balci (BMC)
Datum	: 4 augustus 2017

I Voorwoord

I.I Totstandkoming

In dit document is het tactische informatieveiligheidsbeleid beschreven van de gemeenten Bloemendaal en Heemstede.

Het informatieveiligheidsbeleid is gebaseerd op de internationale standaarden voor informatieveiligheid: NEN/ISO 27001 en NEN/ISO 27002. Op basis van deze standaard is de Baseline Informatiebeveiliging Nederlandse Gemeenten (VNG/KING) opgeleverd. Deze Baseline Informatiebeveiliging geeft een specifieke invulling aan de wijze waarop de veiligheid van informatie binnen gemeentelijke organisaties moet zijn geborgd. De uitgangspunten uit deze baseline zijn integraal opgenomen in dit "Tactisch gemeentebreed informatieveiligheidsbeleid". Hierdoor is een actueel en volledig naar de laatste inzichten opgesteld beleidsplan voor de gemeenten Bloemendaal en Heemstede ontstaan.

Dit tactische beleid is zodanig opgezet dat het een naslagwerk vormt voor medewerkers en management, die in het kader van werkzaamheden moeten weten aan welke kwaliteitsaspecten aandacht moet worden besteed. De intentie is dat alle medewerkers globaal weten wat er in het informatieveiligheidsbeleid staat, hoe het te gebruiken en wat de belangrijkste uitgangspunten zijn.

De basis van dit informatieveiligheidsbeleid wordt gevormd door Baseline Informatiebeveiliging Nederlandse Gemeenten (VNG/KING).

I.II Leeswijzer en ambitieniveau

Dit document bevat een verdere tactische uitwerking van hetgeen in het strategische informatieveiligheidsbeleid beschreven en vastgesteld is. Door vaststelling van het strategische informatieveiligheidsbeleid door de colleges van B en W is automatisch ingestemd met de verdere tactische uitwerking van het strategische beleid. De uitwerking hiervan vindt plaats in voorliggend document.

De gebieden waar informatieveiligheid betrekking op heeft, worden tijdens de fase van een informatieveiligheidsanalyse, de risicoanalyse en de dataclassificatie geïnventariseerd en vervolgens van een prioriteit voorzien (zie hoofdstuk 1 van het strategisch informatieveiligheidsbeleid). De organisatie maakt tijdens dit proces zelf keuzes over de prioritering en fasering van de implementatie van de onderdelen van het beleidsplan. Enkele beleidsuitgangspunten hebben betrekking op aandachtsgebieden die pas actueel worden indien de organisatie voor een dergelijke keuze of vraagstuk staat, bijvoorbeeld de aanschaf van een nieuw informatiesysteem. In dat specifieke geval hanteert de organisatie de beleidsuitgangspunten in dit document om de veiligheid van informatie bij deze keuze te vergroten.

Met dit document wordt daarnaast bepaald dat de organisatie bij voorkomende keuzes en vraagstukken ten aanzien van de veiligheid van informatieprocessen de beleidsregels in dit document en die uit het strategische informatieveiligheidsbeleid als uitgangspunt hanteert.

1. Beveiligingsaspecten ten aanzien van personeel

Doelstelling:
Het verminderen van de risico's van menselijke fouten, diefstal, fraude of misbruik van voorzieningen.

Resultaat:
Werknemers, ingehuurd personeel en externe gebruikers kennen en begrijpen hun verantwoordelijkheden en zijn geschikt voor de rollen waarvoor zij (beoogd) worden benoemd.

1.1 Algemene uitgangspunten ten aanzien van personele beveiligingsaspecten

Hieronder volgen de geldende algemene uitgangspunten:

- De leidinggevende is verantwoordelijk voor het juist afhandelen van de beveiligingsaspecten van het aangaan, wijzigen en beëindigen van een dienstverband of een overeenkomst met externen. De afdeling P&O houdt toezicht op dit proces;
- De leidinggevende bepaalt welke rol(len) de medewerker moet vervullen en welke autorisaties voor het raadplegen, opvoeren, muteren en afvoeren van gegevens moeten worden verstrekt;
- Bij inbreuk op de beveiliging gelden voor medewerkers de gebruikelijke disciplinaire maatregelen, zoals onder meer genoemd in gemeentelijke regelingen;
- Regels die volgen uit dit beleid en andere gemeentelijke regelingen gelden ook voor externen, die in opdracht van de gemeente werkzaamheden uitvoeren.

1.2 Voorwaarden tewerkstelling vast personeel

Iedere vaste medewerker in dienst van de gemeenten Bloemendaal en Heemstede, legt de eed/belofte af (met terugwerkende kracht). Alle medewerkers worden geacht te handelen conform de voorschriften zoals vermeld in het integriteitsprotocol dat ter ondertekening wordt voorgelegd. Daarnaast overleggen alle medewerkers eenmalig een Verklaring Omtrent Gedrag (VOG). Bij indiensttreding wijst de leidinggevende de werknemer op de aanwezigheid van eventueel aanvullende, specifieke gedragsregels ten aanzien van een informatiesysteem of afdeling. Dit laatste gebeurt in ieder geval bij de Basisregistratie Personen (BRP), Waardedocumenten en SUWI. De documenten zijn terug te vinden op het intranet.

1.3 Voorwaarden tewerkstelling externen

Externen die tewerkgesteld worden bij de gemeenten Bloemendaal en Heemstede, zoals uitzendkrachten, stagiaires en ingehuurde externe personen (zoals leveranciers) die toegang hebben tot vertrouwelijke gemeentelijk informatie tekenen een geheimhoudingsverklaring en worden geacht te handelen conform de voorschriften zoals vermeld in het integriteitsprotocol dat ter ondertekening wordt voorgelegd. Ook overleggen zij eenmaal een Verklaring Omtrent Gedrag (VOG) indien de functie daarom vraagt[3]. Daarnaast wijst de leidinggevende de tijdelijke werknemer op de aanwezigheid van eventueel aanvullende, specifieke gedragsregels ten aanzien van een informatiesysteem of afdeling. Dit laatste gebeurt in ieder geval bij de Basisregistratie Personen (BRP,) Waardedocumenten en SUWI. De documenten zijn ook hier terug te vinden op het intranet.

1.4 Kwetsbare functies

De gemeente kiest voor een zorgvuldige selectieprocedure ter waarborging van een betrouwbaar personeelsbestand. Er wordt geen onderscheid gemaakt tussen functies. Van elke medewerker wordt verwacht dat hij/zij integer handelt.

1.5 Toegang en bevoegdheden personeel

Bij indiensttreding worden de fysieke en logische toegangsbevoegdheden volgens een vastgestelde procedure toegekend. De beslissing hierover moet door geautoriseerde personen worden genomen. Bij dienstbeëindiging of bij wijziging van functie worden alle bedrijfsmiddelen van de organisatie geretourneerd. Autorisaties worden in opdracht van het lijnmanagement met onmiddellijke ingang en volgens een vastgestelde procedure verwijderd of aangepast aan de nieuwe status (zie hoofdstukken 2 en 4).

1.6 Opleiding en communicatie

Alle medewerkers (en voor zover van toepassing externe gebruikers van de gemeentelijke systemen) krijgen training in procedures die binnen de gemeente of afdeling gelden voor informatieveiligheid. Deze training dient regelmatig te worden herhaald om het beveiligingsbewustzijn op peil te houden. Ten aanzien van communicatie en bewustwording geldt dat:

- Alle medewerkers binnen de organisatie worden ingelicht over het informatieveiligheidsbeleid en de (beveiligings)procedures van de gemeente en informatie krijgen over het correcte gebruik van de ICT- en toegangsvoorzieningen. Dit geldt eventueel ook voor externe gebruikers;
- De gemeentesecretaris, het MT en de leidinggevenden de algehele communicatie en bewustwording rondom informatieveiligheid bevorderen;
- De leidinggevenden bevorderen dat medewerkers (en externe gebruikers van onze systemen) zich houden aan beveiligingsrichtlijnen;
- In werkoverleggen periodiek aandacht wordt geschonken aan informatieveiligheid. Voor zover relevant worden hierover afspraken vastgelegd in planningsgesprekken.

1.7 Bijzondere situaties

In het geval van ernstige verdenkingen tegen een medewerker op het gebied van verduistering of gedrag dat in strijd is met de interne regels, is het mogelijk dat de gemeenten Bloemendaal en Heemstede gebruik maken van opsporingsmogelijkheden zoals (verborgen) camera's, microfoons en loggegevens. Ook de door de gemeenten verstrekte telefoon en automatiseringsmiddelen kunnen in deze gevallen worden onderzocht. Voor de inzet van deze middelen is schriftelijke toestemming nodig van de gemeentesecretaris.

2. Fysieke beveiliging

Doelstelling:
De fysieke bescherming van gebouwen, terreinen, informatie en (informatie)systemen tegen onbevoegde fysieke toegang, schade of verstoring van continuïteit.

Resultaat:
Maatregelen en procedures waarmee gebouwen, informatie- en ICT-voorzieningen adequaat worden beschermd tegen ongeautoriseerde toegang, kennisneming, verminking of diefstal, waardoor schade en verstoringen worden voorkomen.

2.1 Algemene uitgangspunten ten aanzien van fysieke beveiliging

- De schade door bedreigingen van buitenaf (zoals brand, overstroming, explosies, oproer, stroomonderbreking) wordt beperkt door passende preventieve maatregelen;
- Toegang tot niet-openbare gedeelten van gebouwen of beveiligingszones is alleen mogelijk na autorisatie daartoe;
- De uitgifte van toegangsmiddelen wordt geregistreerd;
- De kwaliteit van toegangsmiddelen (deuren, sleutels, sloten, toegangspassen) is afgestemd op de zonering (en het risicoprofiel);
- Indien gebruik gemaakt wordt van beeldmateriaal wordt dit beperkt door de Wet bescherming persoonsgegevens en nadere regels;
- De fysieke toegang tot ruimten waar zich informatie en ICT-voorzieningen bevinden is voorbehouden aan bevoegd personeel;
- Serverruimtes, datacenters en daaraan gekoppelde bekabelingsystemen zijn ingericht in lijn met geldende 'best practices'.

2.2 Inventarisatie van bedrijfsmiddelen

Om een passend beveiligingsniveau te kunnen bieden, moeten de informatie en de bedrijfsmiddelen worden geïnventariseerd en de waarde en het belang ervan worden onderkend. De afdeling Facilitaire Zaken voor gemeente Bloemendaal en de afdeling Bouwkunde voor gemeente Heemstede, houdt een registratie bij van alle bedrijfsmiddelen die verband houden met de veiligheid van ruimten, gebouw(en) en de directe omgeving van de gebouwen:

- De preventieve, detectieve, correctieve en repressieve systemen met betrekking tot inbraak, ontruiming, brand en toegang;
- Overzicht van toegangsrechten van personen tot ruimten, gebouwen en directe omgeving van het gebouw.

2.3 Servicetaken

Indien voor de bewaking van de gebouwen, personen en goederen een externe bewakingsdienst wordt ingehuurd, voldoet deze bewakingsdienst aan de eisen volgens de Wet Particuliere Beveiligingsorganisaties en Recherchebureaus, beschikt deze over een vergunning van het Ministerie van Justitie en is deze

aangesloten bij een brancheorganisatie. Er worden afspraken gemaakt bij wie de bewakingsdienst verantwoording moet afleggen.

2.4 Fysieke toegang computer- en datacomruimten

De fysieke toegang tot specifieke computer-/serverruimten onder beheer van de uitvoeringsorganisatie Gemeenschappelijke Regeling Informatie Technologie (GRIT) is voorbehouden aan de volgende categorieën personen:

- De leden van de uitvoeringsorganisatie GRIT die uit hoofde van de functie (technische) werkzaamheden aan de centrale computers of telecom apparatuur moeten verrichten;
- De door de verantwoordelijke manager (informatisering en automatisering) geautoriseerde personen (zoals bijvoorbeeld de Bedrijfshulpverlening);
- Personen die niet onder de genoemde categorieën vallen, mogen de specifieke ruimten alleen betreden onder begeleiding van een geautoriseerde medewerker van de uitvoeringsorganisatie GRIT.

2.5 Bewegwijzering computerruimten

Binnen de gebouwen zijn geen wegwijzers aangebracht waaruit de locaties van de ICT-ruimten kunnen worden afgeleid. Ook zijn deze ruimten niet aangegeven op publieke plattegronden of in publicaties, tenzij hieraan andere eisen worden gesteld, bijvoorbeeld door de brandweer.

2.6 Verwijderen apparatuur en gegevensdragers

De uitvoeringsorganisatie GRIT heeft een procedure voor het verwijderen of gereed maken voor hergebruik van overbodige apparatuur en gegevensdragers waarop gemeentelijke informatie en in licentie gebruikte software is opgeslagen.
Denk hierbij aan de harde schijven van pc's en netwerkservers, cd's/dvd's, back-up tapes, USB sticks en overige gegevensdragers. In deze procedure staan voorschriften voor het verwijderen en zo nodig onbruikbaar maken of vernietigen van die informatie.

2.7 Datakluizen en reserve apparatuur

- De datakluizen voldoen aan de eisen die gesteld worden om opgeslagen gegevensdragers in voldoende mate te beschermen tegen stof, brand, water, beschadiging en diefstal;
- Reserve apparatuur en back-ups worden gescheiden bewaard op een andere locatie of een datacenter om de gevolgen van een calamiteit te minimaliseren.

2.8 Clean desk en clear screen beleid

De gemeenten Bloemendaal en Heemstede hebben een 'clean desk' beleid vastgesteld voor papieren en verwijderbare opslagmedia, zodat dit soort materialen niet onbeheerd op het bureau liggen. Daarnaast is er een 'clear screen' beleid voor ICT-voorzieningen. Dit betekent dat alle medewerkers bij het verlaten van de werkplek het scherm vergrendelen en dat na een bepaald tijdsverloop het beeldscherm "op zwart" gaat en de toegang tot het werkstation wordt geblokkeerd middels een toegangscode. Dit om het risico van onbevoegde toegang tot, verlies van of schade aan informatie, informatiedragers en ICT-voorzieningen tijdens en buiten normale werktijden te beperken.

2.9 Beveiliging van (mobiele) apparatuur

Informatie verwerkende mobiele apparatuur moet zowel binnen als buiten het gebouw fysiek beschermd worden. Dit betreft laptops, PDA's, tablets (bijvoorbeeld iPad's), memorysticks en mobiele telefoons (smartphones). Voor het gebruik van deze apparaten worden richtlijnen vastgesteld:

- Apparatuur en bijbehorende media mogen buiten de locatie niet onbeheerd worden achtergelaten;
- Bij het verwerken van vertrouwelijke, privacygevoelige en/of kritische gegevens zijn aanvullende maatregelen getroffen passend bij het classificatieniveau, zoals encryptie, wachtwoordbeveiliging, antivirusscanners enzovoort;
- Bij gebruik van draadloze apparatuur, via een aansluiting op een lokaal of publiek netwerk, zijn beveiligingsmaatregelen getroffen om ongeautoriseerde toegang te voorkomen.

3. Beheer van communicatie- en bedieningsprocessen

Doelstelling:
Het garanderen van correcte en veilige bediening en beheer van de ICT-voorzieningen.

Resultaat:
Maatregelen en procedures voor het beheer en de bediening van de ICT-voorzieningen en het adequaat reageren op incidenten.

3.1 Organisatorische uitgangspunten ten aanzien van communicatie- en bedieningsprocessen

- In beginsel mag niemand autorisaties hebben om een gehele cyclus van handelingen in een informatiesysteem te beheersen, zodanig dat beschikbaarheid, integriteit of vertrouwelijkheid kan worden gecompromitteerd;
- In beginsel is er een scheiding tussen beheertaken en overige gebruikstaken. Hierbij worden beheerwerkzaamheden alleen uitgevoerd wanneer ingelogd als beheerder, normale gebruikstaken alleen wanneer ingelogd als gebruiker. Er wordt echter per specifieke situatie bezien of deze scheiding een werkbare situatie oplevert en of de veiligheid hierdoor in dit specifieke geval wordt verhoogd.

3.2 Technische uitgangspunten ten aanzien van communicatie- en bedieningsprocessen

- Bij het openen of wegschrijven van bestanden worden deze geautomatiseerd gecontroleerd op virussen, trojans en andere malware. Ook e-mail verkeer wordt hierop gecontroleerd. De update voor de detectiedefinities vindt in beginsel dagelijks plaats;
- Op verschillende niveaus binnen de ICT-infrastructuur (netwerkcomponenten, servers, pc's) wordt antivirus software toegepast;
- Het is niet toegestaan niet-geautoriseerde (pc)programmatuur te gebruiken of te installeren op gemeentelijke ICT voorzieningen;
- Alle apparatuur die is verbonden met het netwerk van de gemeente moet kunnen worden geïdentificeerd;
- Documenten, opslagmedia, in- en uitvoergegevens en systeemdocumentatie worden beschermd tegen onbevoegde openbaarmaking, wijziging, verwijdering en vernietiging;
- Het (ongecontroleerd) kopiëren van vertrouwelijke gegevens is niet toegestaan, behalve voor back-up door bevoegd systeembeheer;
- Updates die ten behoeve van het verhogen van de veiligheid worden vrijgegeven door de leverancier worden zo spoedig mogelijk via de geëigende wijzigingsprocedure doorgevoerd. Dit geldt zowel voor besturingssoftware, informatiesystemen, als voor ondersteunende software (bijvoorbeeld Java, Java applets, ActiveX, Flash en Adobe) en besturingssystemen voor mobiele apparatuur en actieve componenten;
- Het netwerk wordt gemonitord en beheerd zodat aanvallen, storingen of fouten ontdekt en hersteld kunnen worden en de betrouwbaarheid van het netwerk niet onder het afgesproken minimum niveau (service levels) komt;
- Gegevens op papier worden beschermd door een deugdelijke opslag en regeling voor de toegang tot archiefruimten.

3.3 Beheerprocedures en verantwoordelijkheden

De verantwoordelijkheden en procedures voor het beheer van de bediening van de ICT-voorzieningen zijn beschreven en vastgesteld. Procedures zijn voor zover mogelijk in lijn gebracht met de ISO 20000-1 en ISO 20000-2 (ITIL 3).

Documentatie van beheerprocedures
De beheerprocedures zijn gedocumenteerd en worden bijgehouden. Deze procedures bevatten instructies voor de planmatige uitvoering van de activiteiten met betrekking tot ICT-voorzieningen. Het gaat om de volgende processen:

Change management / release management – doorvoeren van vernieuwingen en wijzigingen
Het aanbrengen van wijzigingen in de informatie-infrastructuur of het installeren van nieuwe versies vindt plaats volgens een vastgestelde wijzigingsprocedure waarin de formele goedkeuring geregeld is. Dit geldt voor apparatuur, programmatuur, productiesystemen en procedures. Voornaamste aspect bij dit proces is het garanderen van de continuïteit van het productiesysteem. Uitgangspunten hierbij zijn:

- Nieuwe systemen, upgrades en nieuwe versies worden getest op impact en gevolgen en pas geïmplementeerd na formele acceptatie en goedkeuring door de opdrachtgever (veelal de systeemeigenaar) en ICT. De test en de testresultaten worden gedocumenteerd;
- Systemen voor Test en/of Acceptatie (TA) zijn logisch gescheiden van Productie (P);
- Faciliteiten voor Testen, Acceptatie en Productie (TAP) zijn gescheiden om onbevoegde toegang tot of wijziging in het productiesysteem te voorkomen;
- In de TA worden testaccounts gebruikt. Er wordt in beginsel niet getest met productie accounts, mits voor de test absoluut noodzakelijk;
- Vertrouwelijke data uit de productieomgeving mag niet worden gebruikt in de ontwikkel-, test-, opleidings-, en acceptatieomgeving tenzij de gegevens zijn geanonimiseerd. Indien het toch noodzakelijk is om data uit productie te gebruiken, is uitdrukkelijke toestemming van de eigenaar van de gegevens vereist en dienen er procedures te worden gevolgd om data te vernietigen na ontwikkelen en testen;
- Het gebruik van ICT-middelen wordt gemonitord ten behoeve van een tijdige aanpassing van de beschikbare capaciteit aan de vraag.

Incident management – afhandeling van incidenten in de ICT infrastructuur
Om te waarborgen dat incidenten snel, effectief en ordelijk worden afgehandeld, zijn verantwoordelijkheden en procedures voor beheer vastgesteld. Hierbij worden verschillende typen incidenten onderscheiden en wordt gezorgd voor registratie en gedocumenteerde afhandeling van de incidenten.

Capaciteitsmanagement – omgang met de capaciteit van ICT voorzieningen
Om te waarborgen dat informatiesystemen conform de gestelde eisen van continuïteit en snelheid blijven werken stelt de uitvoeringsorganisatie GRIT verantwoordelijkheden en procedures op ten aanzien van de monitoring van de capaciteit.

Problemmanagement – identificeren en afhandelen van fouten in de ICT infrastructuur
De uitvoeringsorganisatie GRIT richt een organisatie in en stelt procedures op ten aanzien van het achterhalen en geprioriteerd wegnemen (of accepteren) van fouten in de infrastructuur.

IT service continuity management – waarborgen van de continuïteit van de ICT-dienstverlening in geval van calamiteiten
De uitvoeringsorganisatie GRIT stelt procedures op ten aanzien van voldoende technische, financiële en organisatorische voorzieningen ten behoeve van het waarborgen van de overeengekomen continuïteit van de ICT-dienstverlening in geval van calamiteiten. Uitgangspunten hierbij zijn:

- In opdracht van de eigenaar van data maakt de uitvoeringsorganisatie GRIT reservekopieën van alle essentiële bedrijfsgegevens en programmatuur, zodat de continuïteit van de gegevensverwerking kan worden gegarandeerd;
- De omvang en frequentie van de back-ups is in overeenstemming met het belang van de data voor de continuïteit van de dienstverlening en de interne bedrijfsvoering, zoals gedefinieerd door de eigenaar van de gegevens;
- De back-up wordt iedere dag buiten het gebouw opgeslagen, zodanig dat een incident op de oorspronkelijke locatie niet leidt tot schade aan de back-up;
- De back-up- en recovery-maatregelen worden regelmatig, doch minimaal één maal per jaar op een uitwijkcentrum en één keer per jaar in de eigen ICT-omgeving, getest;
- Over het resultaat van de test wordt aan de procesverantwoordelijken, de coördinator informatieveiligheid en de controller informatieveiligheid gerapporteerd.

Configuratie management – registratie van ICT voorzieningen
De uitvoeringsorganisatie GRIT stelt procedures op ten aanzien van het registreren en muteren van ICT voorzieningen en de daaraan gerelateerde documentatie.

Information security management – omgang met de veiligheid van ICT voorzieningen
De coördinator informatieveiligheid richt een organisatie in, stelt procedures op en traint personeel zodanig dat aan de eisen van het Informatieveiligheidsbeleid wordt voldaan.

3.4 Uitgangspunten voor controle en logging

Het gebruik van informatiesystemen, alsmede uitzonderingen en informatiebeveiligingsincidenten, worden vastgelegd in logbestanden op een manier die in overeenstemming is met het risico, en zodanig dat tenminste wordt voldaan aan alle relevante wettelijke eisen, met name ten aanzien van de wet BRP en SUWI. Relevante zaken om te loggen zijn:

- type gebeurtenis (zoals back-up/restore, reset wachtwoord, betreden ruimte);
- handelingen met speciale bevoegdheden;
- (poging tot) ongeautoriseerde toegang;
- systeemwaarschuwingen;
- (poging tot) wijziging van de beveiligingsinstellingen.

Een log-regel bevat minimaal de volgende zaken:

- een tot een natuurlijk persoon herleidbare gebruikersnaam of ID;
- de gebeurtenis;
- waar mogelijk de identiteit van het werkstation of de locatie;
- het object waarop de handeling werd uitgevoerd;

- het resultaat van de handeling;
- de datum en het tijdstip van de gebeurtenis.

In een logregel worden alleen de voor de rapportage noodzakelijke gegevens opgeslagen. Er worden maatregelen getroffen om te verzekeren dat gegevens over logging beschikbaar blijven en niet gewijzigd kunnen worden door een gebruiker of systeembeheerder. De bewaartermijnen zijn in overeenstemming met de wettelijke eisen.
Ten aanzien van SUWI vraagt de Security Officer SUWI meerdere keren per jaar een rapportage op bij het BKWI over het gebruik van SUWInet door de gemeente. Ten aanzien van de BRP worden logging rapportages minimaal maandelijks beoordeeld door de BRP beheerder.

3.5 Beheer van de dienstverlening door een derde partij

Bij externe hosting van data en/of services (uitbesteding, cloud computing) blijft de gemeente eindverantwoordelijk voor de betrouwbaarheid van uitbestede diensten. Dit is gebonden aan regels en vereist goede (contractuele) afspraken en controle hierop.
Uitgangspunten bij externe hosting van data en/of services zijn:

- Goedgekeurd door de verantwoordelijke leidinggevende van de gemeenten Bloemendaal en Heemstede;
- Voldoet aan de criteria voor leveranciers van webapplicaties en webservices opgenomen in de norm ICT-beveiligingsassessments DigiD;
- In overeenstemming met informatieveiligheidsbeleid en algemeen gemeentelijk beleid;
- Vooraf gemeld bij de uitvoeringsorganisatie GRIT ten behoeve van toetsing op beheeraspecten;
- De beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de (verwerkers)overeenkomst voor dienstverlening door een derde partij worden geïmplementeerd en uitgevoerd;
- De diensten, rapporten en registraties, die door de derde partij worden geleverd, worden gecontroleerd en er bestaat de mogelijkheid voor het uitvoeren van (periodieke) audits;
- In de basis-SLA voor dienstverlening is aandacht besteed aan informatieveiligheid;
- Er is een basiscontract voor de toegang tot de ICT-voorzieningen en/of de informatievoorziening (bestanden, gegevens) door derden waarin de kaders staan voor de toegang tot ICT-voorzieningen door derden.

3.6 Telewerken en thuiswerken

De gemeenten Bloemendaal en Heemstede staat telewerken toe (op afstand werken op het netwerk van de gemeente, bijvoorbeeld thuiswerken) na toestemming van de verantwoordelijke leidinggevende. Hiervoor worden beveiligingsmaatregelen vastgesteld en getroffen die in overeenstemming zijn met het gemeentelijk informatieveiligheidsbeleid en voor zover niet wordt verboden door wet en regelgeving.[1]

Minimaal wordt aan onderstaande punten aandacht besteed:

- Afspraken tussen de procesverantwoordelijke en "de telewerker", bij voorkeur in de vorm van een overeenkomst, over het omgaan met vertrouwelijke en/of kritische informatie en/of documenten;
- Richtlijnen voor identificatie en authenticatie;
- Richtlijnen voor wachtwoordgebruik;
- Richtlijnen voor de technische inrichting van de telewerkplek (firewall, virusscanner);

[1] Vanuit de SUWI regelgeving en de BRP regelgeving wordt thuisgebruik niet zondermeer toegestaan.

- Afspraken omtrent de telewerkplek (ARBO normen);
- Het inloggen met bijzondere systeembeheer bevoegdheden (administrator en root) via de telewerkplek is niet toegestaan tenzij er aanvullende maatregelen zijn getroffen.

3.7 Mobiele (privé-)apparatuur

Ten aanzien van 'Bring Your Own Device/ Choose Your Own Device" (BYOD/CYOD) wordt beleid opgesteld en worden beveiligingsmaatregelen vastgesteld en getroffen die in overeenstemming zijn met het gemeentelijk informatieveiligheidsbeleid en voor zover niet wordt verboden door wet- en regelgeving.[2]
Minimaal wordt aan onderstaande punten aandacht besteed:

- Afspraken tussen de procesverantwoordelijke en "de gebruiker van mobiele en/of privé apparatuur", bij voorkeur in de vorm van een overeenkomst, over het omgaan met vertrouwelijke en/of kritische informatie en/of documenten;
- Alle getroffen beveiligingsmaatregelen hebben betrekking op zowel door de gemeente verstrekte middelen als op privé-apparatuur;
- Op privé-apparatuur waarmee verbinding wordt gemaakt met het gemeentelijke netwerk is de gemeente bevoegd om beveiligingsinstellingen af te dwingen. Dit betreft onder meer een controle op wachtwoord, encryptie, aanwezigheid van malware, antivirusprogrammatuur en de instellingen van deze programmatuur, etc.;
- Het gebruik van privé-apparatuur waarop beveiligingsinstellingen zijn verwijderd ('jail break', 'rooted device') is niet toegestaan;
- Op verzoek van de gemeente dienen medewerkers de installatie van software om bovenstaande beleidsregel te handhaven toe te staan (denk bijvoorbeeld aan 'mobile device management software');
- De beveiligingsinstellingen, zoals bedoeld in bovenstaande regel, zijn uitsluitend bedoeld ter bescherming van gemeentelijke informatie en integriteit van het gemeentelijke netwerk;
- In geval van dringende redenen kunnen noodmaatregelen worden getroffen, zoals wissen van apparatuur op afstand. Deze noodmaatregelen kunnen, voor zover dit noodzakelijk is, betrekking hebben op privémiddelen en privébestanden.

3.8 Gebruik internet en email

E-mail- en internetprotocol
De gemeenten Bloemendaal en Heemstede hebben een protocol (gedragscode) ten aanzien van het gebruik van e-mail en het gebruik van internet. In deze protocollen zijn maatregelen opgenomen om beveiligingsrisico's, verbonden aan het gebruik van e-mail en internet, te beperken.

3.9 Sociale media

Het gebruik van sociale media door medewerkers van de gemeenten Bloemendaal en Heemstede is toegestaan. De medewerkers dienen zich ervan bewust te zijn dat ze online gezien worden als vertegenwoordigers van de organisatie. Uitingen op het internet worden permanent opgeslagen en kunnen eventueel via andere media opnieuw worden gepubliceerd. Voor het gebruik van sociale media wordt een protocol opgesteld. Hierin worden in ieder geval de volgende onderdelen belicht:

- Geef nooit persoonlijke gegevens van jezelf, collega's of burgers zoals adressen en telefoonnummers. Dit om identiteitsfraude te voorkomen;

[2] Vanuit de SUWI regelgeving en de BRP regelgeving wordt thuisgebruik niet zondermeer toegestaan.

- Ook op internet is het wettelijk kader van toepassing en besef dat smaad, laster, auteursrecht en wetgeving op het gebied van gegevensbescherming van toepassing is;
- Bij de uitingen op het internet dient rekening gehouden te worden met het effect op het imago van de gemeenten Bloemendaal en Heemstede;
- Uitingen op het internet mogen geen uitingen inzake klanten of zaken bevatten.

3.10 Uitwisseling van informatie over netwerken

Bij het beheren van netwerken moet onderscheid gemaakt worden tussen eigen netwerken en netwerken die de grens van de organisatie overschrijden. Voor transport van vertrouwelijke en privacygevoelige gegevens via openbare netwerken zijn extra maatregelen nodig.

Bij gebruik van andere netwerken moet geanalyseerd worden of eigen eisen en de eisen van het andere netwerk in overeenstemming met elkaar zijn en niet leiden tot onoverkomelijke problemen.

Verantwoordelijkheden en procedures voor toegang en het beheer van netwerken en apparatuur op afstand (inclusief de apparatuur op de werkplek) zijn vastgelegd en worden gecommuniceerd naar betrokken partijen.

4. Logische toegangsbeveiliging

Doelstelling:
Het beheersen van de toegang tot informatie en (informatie)systemen.

Resultaat:
Gedocumenteerd beleid en daarvan afgeleide maatregelen en procedures voor effectieve toegangsbeveiliging tot de informatie-infrastructuur en gegevens en het voorkomen van ongeautoriseerde toegang.

4.1 beleid voor logische toegangsbeveiliging

Om effectieve toegangscontrole tot vertrouwelijke en privacygevoelige informatie te kunnen implementeren en onderhouden is er een gemeentebreed toegangsbeleid. Naast dit gemeentebrede toegangsbeleid heeft ieder informatiesysteem nog een specifiek gedefinieerd toegangsbeleid, dat is afgestemd op de classificatie van de informatie.

Het toegangsbeleid is vastgesteld en bekend gemaakt aan de organisatie. In het beleid komen de volgende aspecten aan de orde:

- Aanvragen voor toegang worden geautoriseerd door de procesverantwoordelijke (eigenaar van de data/applicatie);
- Er worden in de regel geen 'algemene' identiteiten gebruikt. Voor herleidbaarheid en transparantie is het namelijk nodig om te weten wie een bepaalde actie heeft uitgevoerd. Indien dit geen (wettelijke) eis is kan worden gewerkt met functionele accounts;
- De gemeente maakt, waar mogelijk, gebruik van bestaande (landelijke) voorzieningen voor authenticatie, autorisatie en informatieveiligheid (zoals: DigiD en eHerkenning);
- Alle toegekende bevoegdheden worden geregistreerd en beheerd, bijvoorbeeld in een autorisatiematrix;
- Het gebruik van speciale bevoegdheden wordt beperkt en beheerd.

De procesverantwoordelijke draagt zorg voor de toetsing of de door de uitvoeringsorganisatie GRIT of applicatiebeheer geïmplementeerde bevoegdheden zijn toegekend of verwijderd conform de aanvraag.

4.2 Beheer van toegangsrechten

Voor de beheersing van toewijzing van toegangsrechten is een procedure vastgesteld, waarin de gehele cyclus is opgenomen van het registreren tot het afmelden van gebruikers. Naast wachtwoorden kunnen ook andere technologieën worden toegepast voor gebruikersidentificatie en authenticatie, zoals biometrie, handtekeningverificatie, hardware (bijvoorbeeld token), SMS authenticatie en cryptografische sleutels. Bij het beheer van gebruikerswachtwoorden is vastgelegd op welke wijze het initiële wachtwoord aan de gebruiker kenbaar wordt gemaakt en hoe gehandeld wordt bij het vergeten van het wachtwoord. Verstrekte wachtwoorden moeten onmiddellijk na het eerste gebruik door de gebruiker worden gewijzigd.

4.3 Externe toegang

De gemeente kan een externe partij toegang verlenen tot het gemeentelijke netwerk. Hiervoor dient een procedure gemaakt en gevolgd te worden. Externe partijen kunnen niet op eigen initiatief verbinding maken met het besloten netwerk van de gemeente, tenzij uitdrukkelijk overeengekomen.

De externe partij is verantwoordelijk voor authenticatie en autorisatie van haar eigen medewerkers. De gemeente heeft het recht hierop te controleren en doet dat aan de hand van de audit trail en interne logging.

4.4 Mobiel werken, thuiswerken en internetfaciliteiten

Uitgangspunten voor beleid ten aanzien van mobiel werken, thuiswerken en internetfaciliteiten:

- Voor werken op afstand is een thuiswerk- c.q mobiele werkplekomgeving beschikbaar. Toegang tot vertrouwelijke informatie wordt verleend op basis van multifactor authenticatie;
- Onbeheerde apparatuur (privé-apparaten of de 'open laptop') kan gebruik maken van draadloze toegangspunten (WiFi). Deze zijn logisch gescheiden van het gemeentelijke bedrijfsnetwerk;
- Mobiele bedrijfsapplicaties worden bij voorkeur zo aangeboden dat er geen gemeentelijke informatie wordt opgeslagen op het mobiele apparaat ('zero footprint'). Gemeentelijke informatie dient te worden versleuteld bij transport en opslag conform classificatie eisen;
- Voorzieningen als webmail, als ook sociale netwerk en clouddiensten (Dropbox, Gmail, etc.) zijn door het lage beschermingsniveau (veelal alleen naam, wachtwoord en het ontbreken van versleuteling) en internationale regelgeving (veelal beschikbaar voor buitenlandse onderzoekdiensten), niet geschikt voor het delen van vertrouwelijke informatie.

4.5 Controle op toegangsrechten

Alle medewerkers die van het netwerk of applicaties gebruikmaken, moeten door het systeem of applicatie op unieke wijze geïdentificeerd kunnen worden. Om de toegang tot de Informatiearchitectuur effectief te beheren, wordt periodiek een uitdraai gemaakt van de verstrekte toegangsmachtigingen. Deze uitdraai wordt gecontroleerd op juistheid en volledigheid door de controller informatieveiligheid.

4.6 Toegangsbeveiliging met betrekking tot netwerkdomeinen en componenten

Aanbrengen van scheidingen
Daar waar de risico's dit noodzakelijk maken, is scheiding in de netwerken aangebracht. De toegang tussen deze gescheiden 'netwerkdomeinen' zijn beveiligd via bijvoorbeeld gateways, firewalls en routers. Afhankelijk van de toegangseisen voor de betreffende ICT-voorziening is het gebruik van de verbindingsmogelijkheden beperkt.

Demilitarized Zone (DMZ)
Voor wat betreft de internetfacing systemen moet gebruik worden gemaakt van een Demilitarized Zone (DMZ), waarbij compartimentering wordt toegepast en de verkeersstromen tussen deze compartimenten wordt beperkt tot alleen de hoogst noodzakelijke. Onder andere de webapplicaties die gebruik maken van DigiD bevinden zich in deze DMZ. Door middel van minimaal 2 (virtuele) firewalls worden verkeersstromen tussen het internet, de (web)applicaties in het DMZ en het interne netwerk waar de backoffice applicaties en de gemeentelijke basisregistraties zich bevinden, tot een minimum beperkt.

Intrusion Detection Systeem
De gemeente maakt gebruik van een intrusion detection systeem zodat tijdig wordt gedetecteerd dat kwaadwillenden misbruik willen maken van de webapplicatie. Intrusion Detection Systemen (IDS) helpen bij het detecteren van aanvallen op webapplicaties. Een IDS monitort continu het netwerk verkeer dat zich door de DMZ compartimenten verplaatst en kan, veelal op basis van aanvalspatronen, misbruik van webapplicaties en andere infrastructuurcomponenten detecteren.

Het detecteren van aanvallen gebeurt veelal op basis van bekende aanvalspatronen. Deze manier van detectie, op basis van 'handtekeningen' van bekende aanvallen, wordt ook wel signature-based genoemd. Tegenover de signature-based IDS'en staan de anomaly-based systemen. Deze systemen werken niet op basis van handtekeningen, maar op basis van afwijkingen (anomalieën).

Beveiliging van poorten voor diagnoseprotocollen
De poorten die gebruikt worden voor diagnoseprotocollen, zoals SNMP, moeten met een geschikt beveiligingsmechanisme beveiligd zijn.

Netwerkadres
Servers, werkstations, pc's, laptops en thin cliënts worden in het netwerk geïdentificeerd door een centraal systeem dat inkomend en uitgaand verkeer wel of niet doorlaat, bijvoorbeeld op basis van het netwerkadres (IP-adres).

Netwerken met externe verbindingen
Bij gebruik van externe koppelingen buiten het gemeentelijke data- en telecommunicatienetwerk, bijvoorbeeld voor internet of connectie naar andere gebouwen, voldoet de beveiliging hiervan tenminste aan de geldende aansluitvoorwaarden om ongeautoriseerde toegang via "achterdeuren" te voorkomen. Dit moet door middel van documentatie aangetoond worden.

Bij gebruik van een draadloze externe verbinding moeten aanvullende maatregelen worden getroffen om ongeautoriseerde toegang en misbruik door derden te voorkomen. Bij het aanbieden van online diensten en transacties via de eigen website zijn adequate beveiligingsmaatregelen getroffen.

Draadloze en openbare netwerken
Gebruik van draadloze netwerken vraagt om specifieke beveiligingsmaatregelen. Voor transport van vertrouwelijke en privacygevoelige gegevens via openbare netwerken zijn eveneens extra maatregelen nodig. Wettelijk is ten aanzien van persoonsgegevens minimaal encryptie vereist.

Actieve componenten
Voor logische toegang tot actieve componenten als routers, switches en firewalls gelden als basis dezelfde toegangsprocedures als voor de overige ICT voorzieningen. Daarbij voldoet de procedure ook aan de normen zoals gesteld in de Norm ICT-beveiligingsassessments DigiD.

4.7 Toegangsbeveiliging met betrekking tot werkstations

Inlogprocedure werkstations
De toegang tot een informatiesysteem verloopt via een inlogprocedure, bedoeld om het risico van ongeautoriseerde toegang te beperken. In de procedure is onder meer het maximale aantal toegestane inlogpogingen, wachtwoordlengte en frequentie van wijziging vastgelegd.

Gebruikersidentificatie en -authenticatie
Identificatie en authenticatie van de gebruiker vindt altijd plaats. Hierdoor zijn activiteiten in het (informatie)systeem herleidbaar tot een natuurlijk persoon. Identificatie en authenticatie kunnen plaatsvinden door middel van gebruikersnamen in combinatie met wachtwoorden, smartcards, tokens of SMS authenticatie.

Gebruik van systeemhulpmiddelen ('utilities')[3]
Het gebruik van systeemhulpmiddelen waarmee toegangscontroles in systemen en toepassingen kunnen worden getest en mogelijk worden doorbroken (bijvoorbeeld sniffers), wordt beperkt tot een klein aantal bevoegde gebruikers en nauwlettend beheerst.

Schermbeveiliging (clear screen)
Medewerkers moeten bij het verlaten van de werkplek het scherm vergrendelen en na een vaste periode van inactiviteit wordt een werkstation automatisch geblokkeerd. Bij werkstations op locaties met verhoogd risico moeten de programma- en netwerksessies afgesloten worden en wordt de gebruiker uitgelogd.

4.8 Toegangsbeveiliging met betrekking tot (informatie)systemen

Toegang tot (informatie)systemen
Autorisatie voor (informatie)systemen wordt verleend op grond van de rol van de medewerker. Binnen het (informatie)systeem krijgt de medewerker alleen toegang tot de functionaliteit en gegevens die nodig zijn voor de uitvoering van zijn of haar rol/taken. Alle medewerkers hebben een individueel gebruikersprofiel zowel op netwerk als op applicatieniveau waardoor mutaties en zo mogelijk ook raadplegingen altijd zijn terug te herleiden tot een individu.

Componenten van (informatie)systemen
Een (informatie)systeem kan uit meerdere componenten bestaan, zoals applicatie, pc, netwerk, besturingssysteem, database, firewall. Voor elk van deze componenten moet autorisatie apart worden verleend.

(Informatie)systemen met vertrouwelijke of privacygevoelige gegevens
(Informatie)systemen die vertrouwelijke of privacygevoelige gegevens verwerken, vereisen speciale maatregelen, zoals het plaatsen in een aparte beveiligde omgeving of domein. De procesverantwoordelijke stelt expliciet de gevoeligheid van een (informatie)systeem vast en de noodzaak voor aanvullende maatregelen.

[3] Deze tools worden uitsluitend door de ICT-specialisten conform procedure gebruikt.

5. Verwerving, ontwikkeling en onderhoud van systemen

Doelstelling:
Het waarborgen dat beveiliging wordt ingebouwd in (informatie)systemen en dat beveiligingseisen worden meegenomen in het proces van systeemontwikkeling en -onderhoud.

Resultaat:
(Informatie)systemen waarin zoveel mogelijk geautomatiseerde beveiligingsmaatregelen zijn ingebouwd. Maatregelen en procedures waarmee de beveiliging tijdens de ontwikkeling en het onderhoud van (informatie)systemen wordt gegarandeerd.

5.1 Beveiligingseisen voor (informatie)systemen

Bij de (opdracht tot) ontwikkeling van (informatie)systemen moeten beveiligingseisen vanaf aanvang in het ontwerpproces worden meegenomen. Dit geldt ook voor afdelingsoverstijgende (informatie)systemen. Bij standaardprogrammatuur moet voor aanschaf worden vastgesteld of geautomatiseerde beveiligingsmaatregelen zijn ingebouwd. Bij het onderhoud van (informatie)systemen moet informatieveiligheid een vast aandachtspunt zijn. De volgende aspecten moeten bij ontwikkeling en onderhoud aan de orde komen:

- Beveiligingseisen zijn zoveel mogelijk onderkend, gedocumenteerd en goedgekeurd voordat een (informatie)systeem wordt ontwikkeld of aangekocht;
- Benodigde beveiligingsmaatregelen met betrekking tot audit trails en validatie van invoergegevens, interne verwerking en uitvoergegevens zijn, waar mogelijk, ingebouwd;
- Voor (informatie)systemen die vertrouwelijke of privacygevoelige gegevens bevatten, kunnen aanvullende beveiligingsmaatregelen nodig zijn die, op basis van classificatie en risicoanalyse, zijn vastgesteld;
- Bij extern toegankelijke applicaties, bijvoorbeeld webapplicaties, wordt extra aandacht besteed aan het voorkomen van ongeautoriseerde toegang.

5.2 Cryptografische beveiliging

Cryptografische systemen en technieken moeten worden toegepast in (informatie)systemen die vertrouwelijke en/of privacygevoelige gegevens verwerken en die onvoldoende kunnen worden beveiligd door andere maatregelen. Dit geldt met name voor gegevens die via openbare, grensoverschrijdende en draadloze netwerken worden getransporteerd (ook USB-sticks) en voor systemen die als standalone toepassing gebruikt worden, bijvoorbeeld op laptops, PDA's, tablets en smartphones.

PKI-certificaten worden herkend in veel standaardtoepassingen, zoals webbrowsers en e-mailpakketten. Met behulp van algemene PKI-certificaten is de informatie die personen en organisaties over het internet sturen, op een hoog niveau beveiligd.
PKIoverheid-certificaten bieden aanvullende zekerheden. Een digitaal certificaat van PKIoverheid (Public Key Infrastructure voor de overheid) waarborgt op basis van Nederlandse wetgeving de betrouwbaarheid van informatie-uitwisseling via e-mail, websites of andere gegevens-uitwisseling.
PKIoverheid-certificaten worden gebruikt bij:

- het zetten van een rechtsgeldige elektronische handtekening;
- het beveiligen van websites;
- het op afstand authenticeren van personen of services;
- het versleutelen van berichten.

Wanneer er gebruik gemaakt wordt van cryptografische sleutels dan dient het sleutelbeheer te zijn georganiseerd. Het gaat dan met name om de bescherming van de sleutels, het inrichten van de beheersrollen en de recoverymogelijkheden. Een sleutelbeheersysteem moet er minimaal voor zorgen dat sleutels niet onversleuteld op de servers te vinden zijn.

5.3 Digitale handtekening

Bij gebruik van digitale handtekeningen als middel om de authenticiteit en integriteit van elektronische documenten te waarborgen, worden alle sleutels afdoende beveiligd tegen wijziging en vernietiging. Ook worden persoonlijke sleutels (private keys) beschermd tegen onbevoegde openbaarmaking.

5.4 Uitbesteding ontwikkeling van (informatie)systemen

Als regel ontwikkelt de gemeente niet zelf een (informatie)systeem maar besteedt het ontwikkel- en productiewerk uit. De gemeente gaat vervolgens over tot aanschaf van het (informatie) systeem of afname van een dienst. Bij uitbesteding van de ontwikkeling van (informatie)systemen wordt rekening gehouden met:

- Aangaan van een formele overeenkomst op basis van de algemene leveringsvoorwaarden van de gemeenten Bloemendaal en Heemstede;
- Licentieovereenkomsten, eigendom van de broncode en intellectuele eigendomsrechten;
- Beoordeling en controle van de kwaliteit en nauwkeurigheid van het uitgevoerde werk;
- Privacygevoeligheid en bedrijfsvertrouwelijkheid van testgegevens, bijvoorbeeld door het gebruik van anonieme of fictieve gegevens en ingeval door de leverancier persoonsgegevens worden bewerkt of deze meewerkt aan de totstandkoming van een verwerkersovereenkomst met de gemeente in de zin van de Wet Bescherming Persoonsgegevens;
- Mogelijkheid tot uitvoeren van IT audits bij de leverancier op de interne beheersingsmaatregelen of bij de door de leverancier ingeschakelde derden namens de gemeente;
- Zorgen voor een borg in geval de externe partij in gebreke blijft (bv. Escrow);
- De leverancier een Third Party Memorandum (TPM) of ISAE3402 verklaring verzorgt, of vergelijkbare verklaring van een onafhankelijke partij (Register EDP auditor) over de relevante interne beheersing van processen en in het bijzonder de beveiligingsprocessen en aan de gemeente verstrekt indien deze daarom verzoekt;
- De beschrijving van de dienst is opgenomen in de overeenkomst. Verwijzing per geleverde dienst naar de betreffende service level specificaties. Denk hierbij aan een concrete beschrijving van diensten, servicetijden (normale servicetijden, weekends, feestdagen en vakantiedagen), service beschikbaarheid, responsetijden, oplostijden et cetera;
- De beschrijving van de overlegstructuren, de contactpersonen en de onderlinge communicatie is opgenomen in de overeenkomst. Vastleggen wanneer gestructureerd overleg plaatsvindt, wie aan dit overleg deelnemen. Ook zal een overzicht opgenomen moeten worden van alle contactpersonen en verantwoordelijken bij escalatie of calamiteiten (escalatiematrix);
- De beschrijving van de geschillenregeling is opgenomen in de overeenkomst. Beschrijving wat de procedure is bij het optreden van onderlinge conflicten of geschillen tussen gebruikersorganisatie en dienstverlener (-aanbieder);

- De beschrijving van prestatie indicatoren, de manier van meten en de rapportagestructuur is opgenomen in de overeenkomst. Beschrijving van de prestatie indicatoren (Key Performance Indicators (KPI's)), hoe deze worden gemeten en hoe hierover wordt gerapporteerd;
- Om zicht te hebben, te krijgen en te houden op alles wat te maken heeft met de dienstverlening. Denk hierbij aan afspraken over de inhoud, de frequentie en de verspreiding (distributie) van de rapportage;
- De leverancier toereikende technische en organisatorische maatregelen heeft genomen om de webapplicatie en gerelateerde gegevens te beveiligen tegen verlies, diefstal en inzage door daartoe niet bevoegde personen;
- De leverancier in de overeenkomst aangeeft dat de gehanteerde beveiligingsmaatregelen, zowel technisch als organisatorisch up to date worden gehouden en voldoen aan de laatst bekende beveiligingsinzichten, beveiligingsnormen en –richtlijnen;
- Of ingeval van een webapplicatie tenminste jaarlijks penetratietesten worden uitgevoerd waarbij uitgangspunt is dat de leverancier de gemeente in staat stelt om aan haar verplichtingen als verantwoordelijke, voortvloeiend uit de aan de DigiD gekoppelde wet- en regelgeving, en de Wet Bescherming Persoonsgegevens (WBP) te voldoen.

5.5 Hardening van systemen

De hardening van alle systemen maar met name de internet facing systemen dient strak te zijn geregeld. Voor de webapplicaties en systemen geldt: alles dat open staat moet een reden hebben en alles dat open staat moet secure worden aangeboden.

De hardening van interne systemen mag minder stringent. Voor interne systemen moeten de management functies secure zijn, er geen onveilige protocollen worden gebruikt, de default wachtwoorden zijn gewijzigd, en ongebruikte applicaties worden verwijderd.

Systeem hardening is een leverancier specifiek proces, aangezien de verschillende leveranciers het systeem op verschillende manieren configureren en voorzien van verschillende diensten tijdens het standaard (default) installatie proces. Alle componenten van de ICT-infrastructuur moeten deel uitmaken van het hardeningsproces.

Voorbeelden van risico's die door hardening teniet worden gedaan zijn:
- Indien (externe) systemen, zoals webservers en mailservers 'reclame' maken voor hun type en versie, wordt het een aanvaller makkelijker gemaakt om bekende zwakke plekken van deze systemen te exploiteren;
- Systemen die onnodige diensten draaien en poorten open hebben die niet open hoeven te staan zijn makkelijker aan te vallen omdat deze diensten en poorten mogelijkheden bieden om het systeem aan te vallen.

5.6 Hardening van websites

Speciale aandacht krijgen hierbij de websites van de gemeente. Aangezien niet langer gebruikte websites of verouderde informatie die toegankelijk zijn via het internet een beveiligingsrisico opleveren dient de gemeente deze informatie te (laten) verwijderen. De gemeente en in het bijzonder de eigenaar van de specifieke website is hiervoor verantwoordelijk.

6. Beveiligingsincidenten

Doelstelling:
Bewerkstelligen dat informatieveiligheidsgebeurtenissen en zwakheden, die verband houden met informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen.

Resultaat:
Formele procedures voor rapportage van gebeurtenissen en escalatie. Alle werknemers, ingehuurd personeel en externe gebruikers zijn op de hoogte van deze procedures voor het rapporteren van de verschillende soorten gebeurtenissen en zwakke plekken die invloed kunnen hebben op de beveiliging van de bedrijfsmiddelen.

6.1 Definitie beveiligingsincident

Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de beschikbaarheid, de integriteit of de vertrouwelijkheid van informatie of informatiesystemen in gevaar is of kan komen.

Hierbij staat beschikbaarheid voor de garanties over het afgesproken niveau van dienstverlening en over de toegankelijkheid en bruikbaarheid van informatie(systemen) op de afgesproken momenten. Integriteit staat voor de juistheid, volledigheid en tijdigheid van informatie(systemen). Vertrouwelijkheid heeft betrekking op exclusiviteit van informatie en de privacybescherming. Hiermee wordt bedoeld dat uitsluitend gemachtigden toegang mogen hebben tot informatie(systemen).

Voorbeelden van beveiligingsincidenten zijn: besmettingen met virussen en/of malware, pogingen om ongeautoriseerd toegang te krijgen tot informatie of systemen (hacken), niet beschikbaar zijn van de website met dienstverleningsportaal, verlies van usb-stick met gevoelige informatie, diefstal van data of hardware of een gecompromitteerde mailbox.

6.2 Procedure melding en omgang beveiligingsincidenten

Er is een procedure voor het rapporteren van beveiligingsgebeurtenissen vastgesteld, in combinatie met een reactie- en escalatieprocedure voor incidenten, waarin de handelingen worden vastgelegd die moeten worden genomen na het ontvangen van een rapport van een beveiligingsincident. Hiervoor gelden de volgende uitgangspunten:

- De coördinator informatieveiligheid is de beheerder van de registratie van beveiligingsincidenten;
- Een medewerker meldt geconstateerde of vermoede beveiligingslekken en beveiligingsincidenten bij de eindverantwoordelijke en bij de coördinator informatieveiligheid;
- Beveiligingsincidenten die worden gemeld bij de ICT servicedesk, worden als zodanig geregistreerd en eveneens doorgegeven aan de coördinator informatieveiligheid;
- Vermissing of diefstal van apparatuur of media die gegevens van de gemeente kunnen bevatten wordt altijd ook aangemerkt als informatiebeveiligingsincident;
- Informatie over de beveiligingsrelevante handelingen, bijvoorbeeld loggegevens, foutieve inlogpogingen, van de gebruiker wordt regelmatig nagekeken. De coördinator informatieveiligheid bekijkt periodiek een samenvatting van de informatie;

- Afhankelijk van de ernst van een incident is er, na overleg met de Functionaris Gegevensbescherming, een meldplicht bij de Autoriteit Persoonsgegevens (AP);
- Indien is aangesloten op de Informatieveiligheidsdienst (IBD) wordt er eveneens een procedure voor communicatie naar de Informatieveiligheidsdienst opgesteld;
- De informatie verkregen uit het beoordelen van beveiligingsmeldingen wordt geëvalueerd met als doel beheersmaatregelen te verbeteren (PDCA Cyclus).

7. Continuïteitsbeheer

Doelstelling:
Het voorkomen van onderbreking van activiteiten van de gemeentelijke ICT-infrastructuur en het beschermen van de kritische bedrijfsprocessen tegen de effecten van ingrijpende storingen of calamiteiten.

Resultaat:
Een beheerst proces voor het waarborgen van de bedrijfscontinuïteit, waarmee de gebruikers, binnen een vastgestelde periode na het optreden van een beveiligingsincident of calamiteit, op aanvaardbaar niveau hun taken kunnen hervatten.

7.1 Proces van continuïteitsmanagement

Er is een beheerst proces vastgesteld om de bedrijfscontinuïteit van de organisatie als geheel te waarborgen. Het proces kent de volgende onderdelen:

- Elke gemeentelijke afdeling voert een business impactanalyse uit. Afhankelijk van de bevindingen worden per afdeling vervolgacties gepland;
- Elke afdeling heeft een eigen plan voor Business Continuity Management (BCM) (bedrijfscontinuïteits-beheer). In het continuïteitsplan worden de maatregelen beschreven waarmee de kritische bedrijfsprocessen van een afdeling na een onderbreking of verstoring voortgezet of tijdig hersteld kunnen worden. In de continuïteitsplannen wordt minimaal aandacht besteed aan:
  - De risico's van bedreigingen worden beoordeeld naar de waarschijnlijkheid dat zij zich voordoen, de eventuele schade als gevolg daarvan en het herstel;
  - Identificatie van essentiële procedures voor bedrijfscontinuïteit;
  - Wie het plan mag activeren en wanneer, maar ook wanneer er weer gecontroleerd wordt teruggegaan;
  - Veilig te stellen informatie (aanvaardbaarheid van verlies van informatie);
  - Prioriteiten en volgorde van herstel en reconstructie;
  - Documentatie van systemen en processen m.b.t de noodprocedures;
  - Kennis en kundigheid van personeel om de processen weer op te starten;
  - Wijze en frequentie van testen van het plan.
- Indien interne of externe uitwijk is gerealiseerd, wordt minimaal jaarlijks een uitwijktest uitgevoerd. De uitwijkprocedures zijn ondergebracht in het draaiboek uitwijk.

7.2 Relatie met nood- en ontruimingsplan

De afdeling Informatisering en Automatisering zorgt voor het vaststellen van een ontruimingsregeling voor de computerruimte(n). Dit in aansluiting op het algemene noodplan en ontruimingsplan. Hierin is aangegeven op welke wijze de computerfaciliteiten worden uitgeschakeld bij calamiteiten, eventueel van buitenaf op afstand te regelen. Voorts is vastgesteld hoe de afdeling Informatisering en Automatisering de afgesproken regeling zal testen en met welke frequentie.

7.3 Veiligstelling programmatuur

Voor alle systeemsoftware en informatiesystemen moet een afweging gemaakt worden of de broncodes door middel van bijvoorbeeld een Escrow-contract bij derden moeten worden ondergebracht.

7.4 Monitoring capaciteit

Voor alle relevante ICT-middelen wordt het capaciteitsbeslag dusdanig gepland dat continu wordt voldaan aan de eisen die gesteld worden vanuit de afspraken met de afnemers van het systeem. Performanceproblemen worden tijdig gesignaleerd en geanalyseerd op basis van betrouwbare gegevens.

8. Naleving

Doelstelling:
Het voorkomen van schending van strafrechtelijke of civielrechtelijke wetgeving, wettelijke, reglementaire of contractuele verplichtingen of beveiligingseisen en waarborgen dat systemen en processen voldoen aan het beveiligingsbeleid van de gemeenten Bloemendaal en Heemstede.

Resultaat:
Maatregelen en procedures waarmee naleving van wetten, verplichtingen en beveiligingseisen uit het beleid van de gemeente bewaakt wordt.

8.1 Organisatorische uitgangspunten

- Het verbeteren van de kwaliteit van informatieveiligheid is een continu proces en onderdeel van alle gemeentelijke processen waarin wordt gewerkt met gevoelige informatie. Informatieveiligheid is een kwaliteitskenmerk van het primaire proces, waarop het management van elke afdeling stuurt. De kwaliteit wordt gemeten aan:
  - de mate waarin een volledige set aan maatregelen is geïmplementeerd, gebaseerd op vastgesteld beleid;
  - efficiency en effectiviteit van de geïmplementeerde maatregelen;
  - de mate waarin de informatieveiligheid het bereiken van de strategische doelstellingen ondersteunt.
- De coördinator informatieveiligheid coördineert namens de gemeentesecretaris de uitvoering van het informatieveiligheidsbeleid;
- De uitvoeringsorganisatie GRIT en externe hosting providers leggen verantwoording af aan hun opdrachtgevers over de naleving van het informatieveiligheidsbeleid. Bij uitbestede (beheer)processen kan een verklaring bij leveranciers worden opgevraagd (TPM of ISAE3402-verklaring);
- Naleving van regels vergt in toenemende mate ook externe verantwoording, bijvoorbeeld voor het gebruik van DigiD, SUWI, BRP en Waardedocumenten. Aanvullend op dit informatieveiligheidsbeleid kunnen daarom specifieke normen gelden;
- Periodiek wordt de kwaliteit van informatieveiligheid onderzocht. Bijvoorbeeld door gemeentelijke auditors, onafhankelijke externen, audits, onderzoeken of zelfevaluaties. Jaarlijks worden audits/onderzoeken/zelfevaluaties uitgevoerd. De bevindingen worden gebruikt voor de verdere verbetering van de informatieveiligheid;
- In de P&C cyclus wordt gerapporteerd over informatieveiligheid aan de hand van het 'in control' statement;
- Er wordt een beveiligingsdocumentatiedossier aangelegd en onderhouden. Dit dossier bevat alle relevante verplichte en niet verplichte documenten waaruit blijkt of kan worden aangetoond dat aan de specifieke beveiligingseisen is voldaan.

8.2 Naleving van informatieveiligheidsbeleid en -plan

Om de naleving van de beveiligingseisen uit het informatieveiligheidsbeleid en -plan te bewaken, legt de procesverantwoordelijke adequate organisatorische en procedurele afspraken vast. Kernelementen in het controle- en evaluatieproces zijn:

- Zelfevaluatie en/of een audit, tenminste eenmaal per jaar, door de procesverantwoordelijke;
- Managementrapportages, tenminste eenmaal per jaar, getoetst door de controller informatieveiligheid op inhoud en vorm en ingebed in bestaande P&C -cyclus.

8.3 Naleving van wettelijke voorschriften

Relevante eisen uit wet- en regelgeving en contractuele eisen moeten voor ieder (informatie)systeem zijn vastgelegd. Er wordt deskundig advies over specifieke juridische eisen ingewonnen bij de juridische adviseur(s) van de gemeente. Conform de Archiefwet[4] beschikken de gemeenten Bloemendaal en Heemstede over een systeem waarin opslag, bewaartermijn en vernietiging van gegevens en informatie in analoge en digitale vorm is geregeld.

Aan de bescherming van persoonsgegevens stelt de Wet Bescherming Persoonsgegevens (WBP) duidelijke eisen. De gemeenten Bloemendaal en Heemstede stellen een privacybeheerder aan, die de uitvoering en de naleving van de WBP bewaakt.

Op 25 mei 2018 treedt de algemene verordening gegevensbescherming (AVG) in werking. Voor de gemeenten Bloemendaal en Heemstede zal het aanwijzen van een functionaris gegevensbescherming (FG) dan verplicht zijn (artikel 37 lid 1 AVG). De FG zal een centraal punt zijn binnen de gemeente wat betreft de gegevensbescherming binnen de organisatie en zal toezien op naleving van zowel de AVG en andere wetten met betrekking tot gegevensbescherming.

8.4 Beoordeling van de naleving

De procesverantwoordelijke leidinggevenden zorgen voor de controle en evaluatie op de naleving van wettelijke voorschriften van het informatieveiligheidsbeleid. Zij beoordelen of alle beveiligingsprocedures binnen hun verantwoordelijkheidsgebied correct worden uitgevoerd en of hun processen en (informatie)systemen voldoen aan relevante wet- en regelgeving, beveiligingsbeleid, normen en andere beveiligingseisen. Zij controleren de naleving van technische normen door productiesystemen te onderzoeken op de effectiviteit van de geïmplementeerde beveiligingsmaatregelen, bijvoorbeeld door het uitvoeren van een security scan. Daarnaast worden controles uitgevoerd door externe auditors (bv. BRP-, SUWI- en DigiD-audit) en door middel van zelfevaluaties.

[4] De wettelijke plicht voor een gemeentelijk documentair structuurplan (DSP) is afgeschaft, maar het blijft verplicht om als gemeente de archiefbescheiden (document-, proces- of zaakgericht) te ordenen.

Begrippenlijst

Acceptatieprocedure
Procedure om vast te stellen of een nieuw (informatie)systeem voldoet aan de gestelde eisen
Applicatiebeheer Onderhoud en exploitatie van de geautomatiseerde gedeeltes (software) van een informatiesysteem

Afdelingsoverstijgend informatiesysteem (AIS)
Systeem dat door meer dan één afdeling wordt gebruikt en waarin gegevens van meerdere organisatieonderdelen worden vastgelegd

Application controls
Geprogrammeerde maatregelen binnen een applicatie ter waarborging van de vertrouwelijkheid, juistheid en volledigheid van de data. We kunnen hierbij denken aan het afschermen van menukeuzes, waardoor informatie niet oproepbaar is of het controleren van input op juistheid (postcode check) of volledigheid.

Audit (informatieveiligheids-)
Het door een onafhankelijke deskundige kritisch beoordelen van de opzet, het bestaan en de werking van de (beveiligings-) voorzieningen en de organisatie voor informatietechnologie op betrouwbaarheid, doeltreffendheid en doelmatigheid

Authenticatie
Verificatie van de geclaimde identiteit, bijvoorbeeld door gebruik van wachtwoord, token, biometrie of een combinatie hiervan

Autorisatie / autoriseren
Toekenning / toekennen van rechten (aan (groepen van) personen, processen en/of systemen)

Back-up
Reservekopie van een computerbestand of programmatuur

Bedrijfskritisch
Van essentieel belang voor de continuïteit van de bedrijfsprocessen

Beschikbaarheid
zie Continuïteit

Beveiligingsincident
Voorval dat de betrouwbaarheid, beschikbaarheid of vertrouwelijkheid van de Informatievoorziening verstoort, en daarmee de informatieveiligheid kan aantasten

Calamiteit
Gebeurtenis die een zodanige verstoring van de geautomatiseerde gegevensverwerking tot gevolg heeft, dat aanzienlijke maatregelen moeten worden genomen om het oorspronkelijke werkingsniveau te herstellen

Change management
Beheer en beheersing van alle wijzigingen van componenten van (informatie)systemen en de ICT-infrastructuur

Classificatie
Indeling in risicoklassen voor de aspecten beschikbaarheid, betrouwbaarheid en vertrouwelijkheid

Clean desk
Een opgeruimde werkplek waar geen vertrouwelijke of privacygevoelige documenten of andere informatiebronnen rondslingeren

Clear screen
Een uitgeschakeld of afgesloten beeldscherm dat alleen met een inlogprocedure weer actief gemaakt kan worden

Compliance
Het begrip waarmee wordt aangeduid dat een persoon of organisatie werkt in overeenstemming met de geldende wet- en regelgeving.

Configuratie management
Beheer en beheersing van de samenstelling en de status van de ICTinfrastructuur en de (informatie)systemen die er gebruik van maken

Configuratieschema
Overzicht van de onderdelen waaruit een (informatie)systeem is opgebouwd

Continuïteit (bedrijfs-)
De mate waarin bedrijfsprocessen ongestoord doorgang kunnen hebben

Continuïteitsmanagement
Stelsel van samenhangende activiteiten, mensen en middelen met als doel de continuïteit van de (kritische) bedrijfsprocessen te waarborgen

Database
Een bestand waarin gedigitaliseerde gegevens op een gestructureerde manier zijn opgeslagen en bevraagd kunnen worden

Datakluis
Brand- en inbraakwerende ruimte voor de opslag van (elektronische) gegevensdragers

Document Structuurplan (DSP)
Een DSP biedt een overzicht van alle aanwezige informatie- en archiefbestanden van een organisatie in relatie tot het werk dat in die organisatie gedaan wordt.

Eigenaar
De eigenaar van een proces of een systeem is vanuit het informatieveiligheidsbeleid verantwoordelijk voor het stellen van eisen en de inrichting van de controle hierop, zodat voldaan wordt aan het informatieveiligheidsbeleid en aan de wettelijke eisen.

Escrow
Specifiek in de softwaresector wordt escrow aangewend ter vrijwaring van de belangen van de softwareklant indien die zich wil indekken tegen bepaalde risico's in hoofde van de softwareleverancier (het meest gevreesde daarbij wellicht het faillissement van de leverancier).
De softwareleverancier zal de broncode van de software (en de bijhorende documentatie) in bewaring geven bij de escrowagent, en deze broncode regelmatig updaten indien nieuwe versies op de markt gebracht worden. Indien de leverancier dan failliet zou gaan, heeft de klant tenminste de broncode van haar applicatie en kan zij alsnog trachten haar applicatie aan de praat te houden.

Functiescheiding
Het scheiden van gerelateerde taken en bevoegdheden met als doel het voorkomen van fouten en fraude

Fysieke beveiliging
Beveiliging die met behulp van fysieke (bouwkundige, technische en/of organisatorische) middelen gerealiseerd wordt

Gateway
Verbinding tussen verschillende netwerken waarop wordt bijgehouden welke computers c.q. protocollen met elkaar verbonden mogen worden

Gebruiker / gebruikende partij
Degene die geautoriseerd gebruik maakt van een (informatie)systeem

Gegevensdrager
Een fysiek object waarin/waarop informatie is vastgelegd, bijvoorbeeld een boek, harde schijf, DVD of USB-stick

Gegevensverwerking
Handeling of geheel van handelingen met betrekking tot gegevens

Hardening
Het proces van het beveiligen van een systeem en het verminderen van kwetsbaarheden door middel van het reduceren van bijvoorbeeld (onbenodigde) software, functies, gebruikersnamen, logins of diensten. (Deze zouden namelijk toegang tot het systeem kunnen genereren via achterdeurtjes).

Informatie- en communicatietechnologie (ICT)
Het vakgebied dat zich bezighoudt met informatiesystemen, telecommunicatie en computers.
Hieronder valt het ontwikkelen en beheren van systemen, netwerken, databanken en websites. Ook het onderhouden van computers en programmatuur en het schrijven van administratieve software valt hieronder. Vaak gebeurt dit in een bedrijfskundige context.

ICT-component
Onderdeel van de informatie- en communicatie infrastructuur, zoals netwerk, bekabeling, servers, werkstations.

Identificatie
Bepaling van de identiteit van een persoon, bijvoorbeeld door een unieke gebruikersnaam of netwerkadres

Incident
Onverwachte of ongewone gebeurtenis

Incident management
Beheer en beheersing van de afhandeling van incidenten

Informatieveiligheid
Samenhangend stelsel van activiteiten, methoden en middelen ter waarborging van beschikbaarheid, betrouwbaarheid en vertrouwelijkheid.

Informatieveiligheidsbeleid
Strategie van een organisatie met betrekking tot informatieveiligheid.

Informatieveiligheidscontroller
Medewerker die zich richt op de verbijzonderde interne controle op de naleving van het informatieveiligheidsbeleid en de escalatie van beveiligingsincidenten.

Informatieveiligheidscoördinator / CISO
Medewerker die gemeentebreed adviseert over informatieveiligheidsvraagstukken in brede zin en activiteiten op het gebied van informatieveiligheid coördineert

Informatiesysteem
Een samenhangende, gegevensverwerkende functionaliteit voor de besturing of ondersteuning van één of meer bedrijfsprocessen

Informatieveiligheidsanalyse
Document waarin beschreven staat welke beveiligingsmaatregelen getroffen worden/zijn op basis van het informatieveiligheidsbeleid

Informatievoorziening
Het geheel aan processen, bestaande uit het verzamelen, het opslaan, het verwerken van gegevens en het beschikbaar stellen ervan

Internet Protocol (IP)
Veel gebruikt protocol voor netwerkverkeer

Information Technology Infrastructure Library (ITIL)

Een referentiekader voor het inrichten van de beheerprocessen binnen een ICT-organisatie. ITIL is geen methode of model, maar eerder een reeks van best practices (de beste praktijkoplossingen) en concepten.

Local Area Network (LAN)
Zie Lokaal netwerk

Logische (toegangs)beveiliging
(Toegangs)beveiliging die met behulp van programmatuur gerealiseerd wordt

Lokaal netwerk (LAN)
Fysiek afgegrensd, instellinggebonden netwerk

Maatwerkprogrammatuur
Op specifiek (deel)proces toegesneden programmatuur

MARAP
Management Rapportage

Medium (opslag-)
Fysieke gegevensdrager

Netwerk
Een verzameling objecten voor communicatie tussen tenminste twee knooppunten van apparatuur en programmatuur, waarbij gebruik gemaakt wordt van voorgeschreven communicatieprotocollen

Netwerkadres (IP Adres)
Unieke identificatie van een element in een netwerk

Netwerkconfiguratie
Overzicht van de objecten waaruit het netwerk bestaat en de relaties tussen deze objecten

Noodplan
Document waarin beschreven staat welke acties een organisatieonderdeel moet ondernemen in een noodsituatie

Ontruimingsplan
Document waarin beschreven staat op welke wijze een gebouw ontruimd moet worden in een noodsituatie

OTAP
Een methodiek die wordt gebruikt in de ICT. Dit geeft een pad aan dat wordt doorlopen tijdens onder andere softwareontwikkeling of het implementeren van nieuwe applicaties.
Het pad dat wordt doorlopen is als volgt: Een programma of component wordt eerst ontwikkeld in de ontwikkelomgeving. Als de programmeur denkt klaar te zijn wordt het gekopieerd naar de testomgeving. Daar kan gecontroleerd worden of het programma of component naar behoren werkt en of het goed kan communiceren met zijn omgeving. Als het goed is bevonden wordt het gekopieerd naar de acceptatieomgeving. Dit is een omgeving waar een gebruiker in kan kijken maar waar normaal gesproken geen gebruikers bij kunnen. De gebruiker kan dan beoordelen of aan zijn eisen en specificaties is voldaan.

Indien de gebruiker het programma of component goedkeurt wordt het gekopieerd naar de productieomgeving waar het gebruikt kan worden door alle gebruikers van het systeem.

Personal Digital Assistant (PDA)
Kleine computer, formaat "binnenzak"

PKI (Public Key Infrastructure)
Een Public Key Infrastructure (PKI) is een systeem waarmee uitgiften en beheer van digitale certificaten kan worden gerealiseerd. Een onafhankelijke partij waarborgt de integriteit en authenticiteit van het certificaat. Hiermee wordt gegarandeerd dat de identiteit van de certificaatbezitter klopt ("je bent wie je zegt dat je bent") en dat gegevens veilig kunnen worden uitgewisseld.

Privacy-beheerder
Medewerker die adviseert over privacybescherming en activiteiten ter bescherming van persoonsgegevens en privacy coördineert

Proces
Een samenhangende serie activiteiten ten behoeve van een van tevoren bepaald doel

Procesverantwoordelijkheid / procesverantwoordelijke
Verantwoordelijkheid / verantwoordelijke voor het geheel van activiteiten van een bepaald proces

Programmatuur
Het geprogrammeerde deel van (informatie)systemen

Recovery
Herstel van een computerbestand of programmatuur

Risicoanalyse
Methode die informatie oplevert over de schadeverwachting van bepaalde gebeurtenissen

Routering
Het bepalen van de weg die berichten volgen Security scan Gericht onderzoek naar de mate van implementatie van beveiligingsmaatregelen

Service Level Agreement (SLA)
Schriftelijke overeenkomst tussen een aanbieder (service provider) en een afnemer (klant) van bepaalde diensten

Smartphone
Programmeerbare telefoon die voor vele uiteenlopende doeleinden gebruikt kan worden, zoals internet

SNMP
Simple Network Management Protocol: een protocol voor netwerk management en beheer

Systeem

Een verzameling van één of meer samenhangende objecten met tezamen een gespecificeerde functionaliteit. Objecten kunnen zowel fysiek (computersysteem) als logisch (besturingssysteem) zijn

Systeemeigenaar
Verantwoordelijke voor een (informatie)systeem

Systeemhulpmiddel
Hulpprogramma voor beheer en onderhoud van (informatie)systemen en ICT-infrastructuur

Systeemklok
Interne klok in een computersysteem

Systeemprivilege
Recht op het gebruik van of toegang tot (een onderdeel van) een (informatie)systeem

Systeemprogrammatuur
Fundamentele, ondersteunende programmatuur die behoort tot de technische infrastructuur van een (informatie)systeem

Technisch beheer
Opslag en onderhoud van digitale informatie door middel van technische Maatregelen

Telewerken
Thuis of op een andere locatie werken op het netwerk van de organisatie met behulp van een externe lijnverbinding

Third Party Mededeling (TPM)
Verklaring van een onafhankelijke derde partij die door betrokken partijen vertrouwd wordt

Utility
Zie Systeemhulpmiddel

Voice over IP (VOIP)
Gebruik van dezelfde netwerkbekabeling voor zowel spraak- als datacommunicatie

Webapplicatie
Toepassingsprogrammatuur die via een internetbrowser benaderd kan worden

Wide Area Network (WAN)
Netwerk dat zich niet beperkt tot één fysieke locatie en waaraan meerdere lokale netwerken (LAN's) gekoppeld kunnen zijn.