BEEKDAELEN

GEMEENTEBLAD

Officiële uitgave van de gemeente Beekdaelen

Nr. 33063

12 februari

2019

Besluit van het college van burgemeester en wethouders van de gemeente Beekdaelen houdende regels omtrent informatiebeveiliging Informatiebeveiligingsbeleid gemeente Beekdaelen

1 INLEIDING

Informatieveiligheid bij de gemeente Beekdaelen is gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), wet- en regelgeving, zoals de jaarrekeningcontrole, Algemene Verordening Gegevensbescherming (AVG) en normenkaders voor audits, conform de ENSIA verantwoording.
Dit document geeft richting aan de beheerstructuur van informatiebeveiliging, de maatregelen voortkomend uit het beleid worden uitgewerkt in het informatie-beveiligingsplan. Zo worden verantwoordelijkheden voor informatiebeveiliging belegd en informatiebeveiliging ingebed in de reguliere planning- en control (P&C) cyclus binnen de kwaliteitshandhaving van de bedrijfsvoeringprocessen.
Het informatiebeveiligingsbeleid van de gemeente Beekdaelen wordt minimaal eens per drie jaar herzien om richting te kunnen blijven geven in veranderende omstandigheden.

1.1 INFORMATIEBEVEILIGING EN PRIVACY

Informatiebeveiliging is de verzamelnaam voor de processen, die ingericht worden om de betrouwbaarheid van processen, de gebruikte informatiesystemen en de daarin opgeslagen gegevens te beschermen tegen al dan niet opzettelijke bedreigingen. De volgende aspecten spelen daarin een rol:

- **Beschikbaarheid**/ continuïteit: het zorgdragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen voor gebruikers op elke gewenste tijd en plaats;
- **Integriteit**/ betrouwbaarheid: het waarborgen van de juistheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking;
- **Vertrouwelijkheid**/ exclusiviteit: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor diegenen die hiertoe geautoriseerd zijn.

Deze drie elementaire aspecten worden tezamen aangeduid als **BIV**.
Naast informatiebeveiliging is privacy een belangrijk onderwerp op de gemeentelijke agenda. De gemeente werkt met persoonsgegevens en de wet- en regelgeving omtrent persoonsgegevens schept belangrijke kaders waaraan de gemeente moet voldoen.

Voor de kaders m.b.t. het werken met persoonsgegevens wordt verwezen naar het Privacybeleid gemeente Beekdaelen.

1.2 WAAROM INFORMATIEBEVEILIGING?

Beschikbare en betrouwbare informatie is essentieel voor de gemeente Beekdaelen om zich verantwoordelijk te gedragen, aanspreekbaar en servicegericht te zijn, en om transparant en proactief verantwoording af te leggen aan haar stakeholders. Informatiebeveiliging is het proces om de aspecten beschikbaarheid, integriteit en vertrouwelijkheid te borgen van de grote hoeveelheden informatie, die de gemeente Beekdaelen voorziet in het classificeren van die informatie en het toepassen van de juiste niveaus van beveiliging om de veiligheid van informatie te borgen. Het proces van informatiebeveiliging is primair gericht op gecontroleerd ontsluiten van informatie: het maakt nieuwe, innovatieve manieren van werken en elektronische dienstverlening op verantwoorde wijze mogelijk.

1.3 REIKWIJDTE EN AFBAKENING INFORMATIEBEVEILIGING

Informatiebeveiliging omvat de organisatie, bedrijfsvoeringprocessen, onderliggende informatiesystemen en informatie van de gemeente Beekdaelen in de meest brede zin van het woord. Dit beleid is naast het uitwisselen van informatie in alle verschijningsvormen, zoals elektronisch, op papier en mondeling, ook van toepassing op alle fysieke ruimten van de organisatie, alsmede op apparaten die door medewerkers gebruikt worden bij de uitoefening van hun taak op diverse locaties. Dit beleid heeft betrekking op de informatie die daarbinnen verwerkt wordt. Ook als systemen of informatie buiten de organisatie voor de gemeente Beekdaelen worden beheerd of bewerkt (bijvoorbeeld bij uitbesteed

beheer) is dit beleid van toepassing of biedt het richtlijnen die gesteld worden aan het beheer van deze systemen en informatie. Bovenal is het niveau van informatiebeveiliging afhankelijk van bewust en verantwoord gedrag van medewerkers van de gemeente Beekdaelen.

1.4 OPBOUW DOCUMENT

Het document is opgebouwd overeenkomstig de strategische, tactische en operationele uitwerking van BIG en beslaat de volgende onderwerpen (achtereenvolgens uitgewerkt): informatiebeveiligingsbeleid, organisatie van informatiebeveiliging, beheer van bedrijfsmiddelen, beveiliging van personeel, fysieke beveiliging, beheer van communicatie en bedienprocessen, logische toegangsbeveiliging, verwerving, onderhoud en ontwikkeling, beheer van incidenten, bedrijfscontinuïteitsbeheer en naleving.

2 INFORMATIEBEVEILIGINGSBELEID GEMEENTE BEEKDAELEN

In het kader van de herindeling is het informatiebeveiligingsbeleid van de gemeenten Nuth, Onderbanken en Schinnen onderling opgesteld en afgestemd. Dit is ook de basis voor het informatiebeveiligingsbeleid van de gemeente Beekdaelen.
Het College van B&W (hierna: College) en Management van de gemeente Beekdaelen spelen een cruciale rol in het sponsoren en tot uitvoer brengen van dit informatiebeveiligingsbeleid.
Risicomanagement ligt aan de basis van beheersing van informatieveiligheid. De verantwoordelijkheid voor de juiste uitvoering hiervan ligt bij het Management. Iedere medewerker van de gemeente Beekdaelen heeft een rol binnen informatiebeveiliging en draagt verantwoordelijkheid om informatieveiligheid tot een succes te maken.
Voor de verantwoordelijkheid voor de uitvoer van het beleid geldt:

- Er is wetgeving waar altijd aan voldaan moet worden, zoals (niet uitputtend): Basis Registratie Personen (BRP), Paspoort Uitvoeringsregeling Nederland, Basisregistratie Adressen en gebouwen (BAG), maar ook de Archiefwet 1995 en de AVG/Meldplicht datalekken;
- Een gemeenschappelijk normenkader: Baseline Informatieveiligheid Gemeenten (BIG).

BIG (gestoeld op ISO-norm NEN/ISO 27002:2007 [1]) ligt aan de basis van de tactische en operationele uitvoer van informatiebeveiliging. Hiermee ligt risicomanagement aan de basis van identificeren, vaststellen en uitvoeren van maatregelen en dienen de verantwoordelijkheden expliciet gedefinieerd en vastgelegd te worden. De aanpak van informatiebeveiliging bij de gemeente Beekdaelen is dan ook 'risk-based'. De normenkaders waaraan getoetst wordt, zijn de BIG en interne normenkaders.
Door periodieke controle en organisatie brede planning én- coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie.
Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening.
Het plan wordt periodiek (jaarlijks) bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en risicoanalyses, conform de PDCA-cyclus. Ook dient het jaarlijks vaststellen van het geüpdatete informatiebeveiligingsplan evenals het vaststellen van het geüpdatete informatiebeveiligingsbeleid en rapportage (over delen) daarvan opgenomen te worden in de P&C-cyclus. Elke drie jaar wordt het informatiebeveiligingsbeleid compleet opnieuw bekeken.

2.1 PDCA

Informatiebeveiliging is een continu verbeterproces. De Deming-cirkel ('Plan, do, check en act') vormt de basis van het managementsysteem van informatiebeveiliging.

1) ISO-norm NEN/ISO 27002:2007 geeft richtlijnen en principes voor het initiëren, implementeren, onderhouden en verbeteren van informatiebeveiliging binnen een organisatie.

- Plan: Tijdens deze fase wordt het informatiebeveiligingsbeleid opgesteld, op basis van wet- en regelgeving, de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en best practices. Planning geschiedt op jaarlijkse basis en wordt indien nodig tussentijds bijgesteld. De planning op hoofdlijnen is uitgewerkt in het informatiebeveiligingsplan.
- Do: Implementeren van (technische) maatregelen en bevordering van beveiligingsbewustzijn geschiedt op dagelijkse basis en maakt integraal onderdeel uit van het werkproces.
- Check: Monitoren en rapporteren is onderdeel van het werkproces met als doel: waarborgen van de kwaliteit van informatie en ICT, en compliance aan wet- en regelgeving.
- Act: Deze fase ligt aan de basis van de uitvoering van verbeteracties. De cyclus is een continu proces; de bevindingen van controles zijn weer input voor de jaarplanning en de beveiligingsplannen. De bevindingen worden in beginsel gerapporteerd aan de directie.

2.2 INFORMATIEBEVEILIGINGSBELEID EN ARCHITECTUUR

Informatiebeveiliging is onderdeel van de informatiearchitectuur van de gemeente Beekdaelen waarin onder meer principes, richtlijnen en maatregelen op basis van de verschillende beschermingsniveaus (classificatie) worden beschreven.

2.3 SAMENHANG

Samen met het informatiebeveiligingsplan vormt het informatiebeveiligingsbeleid het fundament voor een adequate informatiebeveiliging en daarmee een kwalitatief goede informatiehuishouding. Deze informatiehuishouding omvat alle informatie die nodig is om de dienstverlening en de processen die daarvoor nodig zijn, uit te kunnen voeren.
De volgende hoofdstukken corresponderen met de hoofdstukken 6 tot en met 15 uit de BIG.

3 ORGANISATIE VAN INFORMATIEBEVEILIGING

3.1 INTERNE ORGANISATIE

Het College en het Management van gemeente Beekdaelen zijn formeel eindverantwoordelijk voor beveiliging van informatie van de gemeente Beekdaelen. Informatie ligt aan de basis van elk primair proces van de gemeente. Daarnaast zijn het College en het Management verantwoordelijk voor het op- en vaststellen van het informatiebeveiligingsbeleid en het realiseren van de daaruit voortvloeiende verplichtingen.
Het College belegt de adviserende, coördinerende en controlerende aspecten van haar verantwoordelijkheid voor informatiebeveiliging bij de Controller Informatie en Data (CISO), die de bijbehorende taken voor de gemeente Beekdaelen uitvoert.

Elke afdelingsmanager is als proceseigenaar verantwoordelijk voor de (informatie)beveiliging en de betrouwbaarheid van het eigen proces. Hij is tevens verantwoordelijk voor het uitdragen van het informatiebeveiligingsbeleid en in woord en daad ondersteunen van het beleid. Daarnaast laat hij maatregelen uit het informatiebeveiligingsplan die op de afdeling van toepassing zijn uitvoeren. Ook het bevorderen van bewustwording op het gebied van informatiebeveiliging van medewerkers valt onder zijn verantwoordelijkheid.

De Controller Informatie en Data (CISO) is primair aanspreekpunt voor informatie-beveiliging voor alle medewerkers van de gemeente Beekdaelen. De Controller Informatie en Data (CISO) houdt tevens de nieuwste ontwikkelingen – zoals de stand van de techniek – bij, blijft op de hoogte van gewijzigd beleid van andere overheden, aangepaste wet- en regelgeving, veranderende taken en dienstverlening van de gemeente Beekdaelen zelf die van invloed zijn op het informatiebeveiligingsbeleid en -plan en bewaakt dat dit beleid en plan jaarlijks worden geëvalueerd en, waar nodig, aangepast. Ook is hij verantwoordelijk voor het beheer en naleving van de beveiligingsvoorschriften voor BRP, AVG en andere vigerende wet- en regelgeving.
Hij verzorgt ook jaarlijkse rapportage daarover en is contactpersoon (ACIB/ VCIB) van de Informatie Beveiligingsdienst Nederlandse Gemeenten (IBD).
Hij draagt ook namens de gemeente zorg voor het vullen en review daarop van het Information Security Management System [2] (ISMS).
Ook is er een Controller Informatie en Data (Functionaris Gegevensbescherming) aangesteld, die adviseert over de vertaling van privacy wet -en regelgeving naar privacybeleid en de uitvoering van bepalingen van de Algemene Verordening Gegevensbescherming (AVG), zoals bijvoorbeeld de Meldplicht datalekken, de controle op verwerkingsgrondslagen, doelbinding, noodzakelijkheid, etc.

2) ISMS is een managementsysteem voor informatiebeveiliging, waarin de complete set van maatregelen, processen en procedures wordt vastgelegd.

De Controller Informatie en Data (FG) adviseert interne afdelingen over AVG-vraagstukken, zorgt voor interne bewustwording bij het naleven van de AVG, bewaakt de borging van privacy (zowel voor de burger, als voor de medewerkers van de gemeente Beekdaelen) en legt hiërarchisch gezien verantwoording af aan de gemeentesecretaris/ algemeen directeur. Bestuurlijk gezien legt de FG verantwoording af aan het College, danwel, -afhankelijk van de vraag welk orgaan verantwoordelijk is voor een gegevensverwerking- aan de burgemeester of de gemeenteraad.

3.2 OVERLEGSTRUCTUUR

Het forum informatiebeveiliging bestaat uit beide Controllers Informatie en Data (CISO en FG) en een vaste vertegenwoordiging uit de afdelingen van gemeente Beekdaelen met een taakstelling op het gebied van informatiebeveiliging, namelijk de adviseur Informatiebeheer, de adviseur Publieksdiensten, de medewerker Facilitair en een lid van het managementteam.
Het forum informatiebeveiliging komt vier keer per jaar (of vaker, indien nodig) bij elkaar. Een belangrijk doel van het forum is het informeren over en afstemmen van ontwikkelingen op het gebied van informatiebeveiliging. Daarnaast is de voortgang van implementatie van de maatregelen uit het informatiebeveiligingsplan een vast onderwerp. Eens in de zoveel tijd worden de belangrijkste ontwikkelingen op het gebied van informatiebeveiliging onder de aandacht van de medewerkers gebracht.

3.3 DOELGROEPEN

Dit informatiebeveiligingsbeleid is van toepassing op alle in- en externe medewerkers van de gemeente Beekdaelen, evenals leveranciers, die toegang hebben tot de informatie van de gemeente Beekdaelen. Het betreft de volgende doelgroepen:

Doelgroep	**Relevantie voor IB-beleid**
College B&W en Management	Integrale verantwoordelijkheid
Controller Informatie en Data (CISO)	Kaderstelling en implementatie
Management	Sturing op informatieveiligheid en verantwoordelijk voor naleving informatiebeveiligingsbeleid
Medewerkers	Gedrag en naleving
Gegevenseigenaren	Classificatie: bepalen van beschermingseisen van informatie
Proceseigenaren	Sturing op informatieveiligheid en verantwoordelijk voor naleving informatiebeveiligingsbeleid
Beleidsadviseurs	Planvorming binnen informatiebeveiligingskaders
Controller Informatie en Data (FG)	Borging van privacy wet -en regelgeving
Personeelszaken (HRM)	Arbeidsvoorwaardelijke informatiebeveiliging gerelateerde zaken
Inkoop	Inkoop gerelateerde informatiebeveiligings zaken
Medewerker Facilitair	Fysieke toegangsbeveiliging
ICT-diensten (Parkstad-IT, leveranciers etc.)	Technische beveiliging
Controller Informatie en data (CISO)	Interne toetsing
Externen (Auditors)	Onafhankelijke toetsing
Leveranciers en ketenpartners	Naleving van informatiebeveiligingsbeleid en wettelijke kaders

3.4 AFSPRAKEN EN RAPPORTAGES

Afspraken over informatiebeveiliging, wet- en regelgeving en dienstverlening worden vastgelegd in overeenkomsten. Monitoring van de dienstverlening vindt continu plaats. Op basis van rapportages over deze monitoring en controles, wordt de directie periodiek geïnformeerd door de Controller Informatie en data (CISO) over de status van informatiebeveiliging. Het Management bewaakt de algehele status van informatiebeveiliging en draagt zorg dat het informatiebeveiligingsbeleid en bijbehorende plannen en richtlijnen worden aangepast.

BEEKDAELEN

4 BEHEER VAN BEDRIJFSMIDDELEN

4.1 VERANTWOORDELIJKHEID VOOR BEDRIJFSMIDDELEN

Verantwoordelijkheid voor bedrijfsmiddelen wordt belegd bij de eigenaar van het middel, als het algemeen gebruikte middelen betreft (informatiesystemen, informatie die gebruikt wordt door meerdere medewerkers of in meerdere processen, etc). Verantwoordelijkheid voor bedrijfsmiddelen in gebruik bij medewerkers om hun taak goed uit te oefenen, ligt bij de medewerker, die hiervoor een verklaring van gebruik aflegt.
Voor alle informatie en bedrijfsmiddelen zijn maatregelen genomen ter voorkoming van onbevoegde openbaarmaking, toegang, modificatie, verwijdering of vernietiging. Procedures hiervoor worden beschreven in het informatiebeveiligingsplan. Ten aanzien van verwijderbare media en ICT-apparatuur zijn beheerprocedures beschreven en vastgesteld voor onder andere het gebruik, hergebruik en afvoer.
De classificatie van de informatie wordt in acht genomen bij het bepalen van de specifieke technische en procedurele maatregelen.

4.2 CLASSIFICATIE VAN INFORMATIE

Om te kunnen bepalen welke beveiligingsmaatregelen moeten worden getroffen ten aanzien van processen en informatiesystemen worden beveiligingsclassificaties gebruikt. Classificatie maakt het vereiste beschermingsniveau zichtbaar en maakt duidelijk welke maatregelen nodig zijn om de informatie op het juiste niveau te beschermen. Binnen de gemeente Beekdaelen wordt geclassificeerd op de drie betrouwbaarheidsaspecten van informatie: beschikbaarheid, integriteit (juistheid, volledigheid) en vertrouwelijkheid.
De gemeente heeft vier beschermingsniveaus gedefinieerd (geen, laag, midden en hoog). De niveaus zijn in onderstaande tabel weergegeven, waarbij voorbeelden worden gegeven. Deze niveaus zijn gedefinieerd om het proces van classificeren te vereenvoudigen en bijbehorende maatregelen te kunnen identificeren en uniform te kunnen toepassen.
Om dataclassificatie succesvol in te voeren en te implementeren in de organisatie dient de gehele organisatie te worden ingelicht en dataclassificatie actief uit te dragen. Dit gebeurt op basis van samenhangende procedures voor de classificering en verwerking van informatie overeenkomstig het vastgestelde classificatiesysteem.
De classificaties worden als volgt weergegeven op basis van de vier beveiligingsniveaus en de drie informatiebeveiligingsaspecten:

Niveau	Vertrouwelijkheid	Integriteit	Beschikbaarheid
Geen	**Openbaar** Informatie mag door iedereen worden ingezien *(bv: algemene informatie op de externe website van de gemeente)*	**Niet zeker** Informatie mag worden veranderd *(bv: templates en sjablonen)*	**Niet nodig** Gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn *(bv: ondersteunende tools als routeplanner)*
Laag	**Bedrijfsvertrouwelijk** Informatie is toegankelijk voor alle medewerkers van de organisatie *(bv: informatie op het intranet)*	**Beschermd** Het bedrijfsproces staat enkele (integriteits-) fouten toe *(bv: rapportages)*	**Noodzakelijk** Informatie mag incidenteel niet beschikbaar zijn *(bv: administratieve gegevens)*
Midden	**Vertrouwelijk** Informatie is alleen toegankelijk voor een beperkte groep gebruikers *(bv: persoonsgegevens, financiële gegevens)*	**Hoog** Het bedrijfsproces staat zeer weinig fouten toe *(bv: bedrijfsvoering-informatie en primaire procesinformatie, zoals vergunningen)*	**Belangrijk** Informatie moet vrijwel altijd beschikbaar zijn, continuïteit is belangrijk *(bv: primaire proces informatie)*
Hoog	**Geheim** Informatie is alleen toegankelijk voor direct geadresseerde(n) *(bv: zorggegevens en strafrechtelijke informatie)*	**Absoluut** Het bedrijfsproces staat geen fouten toe *(bv: informatie op de website)*	**Essentieel** Informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten *(bv: basisregistraties)*

De classificaties, zoals hiervoor aangegeven, worden toegepast op alle informatie, die door de gemeente Beekdaelen beheerd dan wel verwerkt wordt. Gezien het belang van dataclassificatie in het kader van de BIG, worden de volgende te hanteren uitgangspunten hier expliciet benoemd, zoals die binnen de procedure van toepassing zijn. [3]

- De classificatietabel heeft betrekking op alle in beheer zijnde gegevensverzamelingen, gegevensdragers, informatiesystemen, servers en netwerkcomponenten. De classificatie op systemen dient te worden toegepast op basis van de hoogste categorie informatie die door de systemen wordt verwerkt.
- De eigenaar van de gegevens (veelal ook de proceseigenaar) bepaalt het vereiste beschermingsniveau (classificatie).
- Het object van classificatie is informatie. Classificeren geschiedt op het niveau van informatiesystemen. Alle classificaties van alle bedrijfskritische systemen zijn centraal vastgelegd door de Controller Informatie en Data (CISO) en dienen jaarlijks geëvalueerd te worden door de eigenaren.
- Informatie kan meer of minder gevoelig of kritisch zijn. Voor bepaalde informatie kan een extra niveau van bescherming of een speciale verwerking nodig zijn.
- Elke classificatie wordt gekoppeld aan een niveau van beveiliging en voor elk niveau gelden verschillende maatregelen.

5 BEVEILIGING VAN PERSONEEL

Het Management bevordert dat medewerkers (en externe gebruikers van de systemen) zich houden aan de beveiligingsrichtlijnen. Ditzelfde wordt ook gevraagd van externen, die in opdracht van de gemeente Beekdaelen werkzaamheden uitvoeren. Het Management bevorderen algehele communicatie en bewustwording rondom informatieveiligheid. Hiertoe wordt bij het indiensttredingsproces een eerste aanzet gegeven (bijvoorbeeld in de vorm van een Verklaring Omtrent Gedrag (VOG)).
Het personeel heeft dagelijks te maken met gevoelige informatie. Deze informatie en de processen, volgens welke ze werken, vergen integere medewerkers. Medewerkers tekenen verklaringen om aan te geven dat ze integer omgaan met de hen ter beschikking gestelde informatie en middelen, door middel van geheimhoudingsverklaringen en het bekend raken met regels en richtlijnen voor goed gedrag. Daarnaast is elke medewerker op de hoogte gebracht van zijn rol en verplichtingen op het gebied van informatie-beveiliging en binnen de processen en deel van de organisatie, waarvoor hij werk verricht.

6 FYSIEKE BEVEILIGING

De gemeente Beekdaelen voorkomt verlies, schade of diefstal van informatie en middelen door bescherming tegen fysieke bedreigingen en gevaren van zowel binnen- als buitenaf. Binnen de organisatie en de bedrijfsgebouwen van de gemeente Beekdaelen, is in kaart gebracht wat het risicoprofiel is van fysieke ruimtes. Op basis van het risicoprofiel worden preventieve maatregelen bepaald die de schade door bedreigingen van buitenaf (zoals brand, overstroming, explosies, oproer, stroomonderbreking) beperken.
Voor adequate fysieke beveiliging worden toegangsmiddelen binnen de gemeente Beekdaelen beheerd. Toegangsmiddelen zijn onder andere deuren, sleutels, sloten, en toegangspassen/ druppels. Onder beheer wordt verstaan dat de uitgifte van toegangsmiddelen wordt geregistreerd, zodat controle hierop kan plaatsvinden. Deze uitgifte wordt periodiek geëvalueerd, evenals toegekende rechten. Tevens wordt onder beheer verstaan dat de kwaliteit van toegangsmiddelen is afgestemd op het risicoprofiel van de ruimte.
Het uitgangspunt voor ICT-voorzieningen – welke kritieke of gevoelige bedrijfsactiviteiten ondersteunen – is dat deze fysiek moeten worden ondergebracht in beveiligde ruimten en beveiligd zijn met geschikte beveiligingsbarrières en toegangsbeveiliging, zodat deze beschermd zijn tegen toegang door onbevoegden, schade en storingen. Tevens worden (data)verbindingen afdoende beschermd tegen interceptie of beschadiging. Wanneer middelen van locatie gaan, wordt hiervoor toestemming verleend door de vertegenwoordiger van de organisatie. Dit is de leidinggevende van de betreffende medewerker of de medewerker die verantwoordelijk is voor de uitgifte van het bedrijfsmiddel (de eigenaar). Dit geldt ook wanneer informatie of informatiedragers van locatie worden gebracht, hetzij voor werkdoeleinden,

3) Andere uitgangspunten dienen in de procedure opgenomen te worden en worden niet in het beleid beschreven.

hetzij voor verwerking of verwijdering/ vernietiging. Dit laatste wordt vastgelegd in een procedure voor middelen die de kantoren van de gemeente Beekdaelen verlaten.

7 BEHEER VAN COMMUNICATIE EN BEDIENPROCESSEN

Verantwoordelijkheden en procedures omtrent beveiliging van IT-middelen en informatie worden vastgesteld.

7.1 ORGANISATORISCHE ASPECTEN

Ten aanzien van de inrichting van de organisatie zorgt de gemeente Beekdaelen waar mogelijk, dat medewerkers niet over de mogelijkheid beschikken een volledige cyclus aan handelingen in een informatiesysteem te beheren. Ten behoeve van deze 'functiescheiding' zijn rollen en verantwoordelijkheden binnen processen vastgesteld. Deze rollen zijn overeenkomstig in de relevante applicaties en systemen ingericht. Als basis hiervoor is een autorisatiematrix opgesteld.
De gemeente Beekdaelen past waar mogelijk scheiding toe tussen beheertaken en dagelijkse werkzaamheden binnen de bedrijfsprocessen. Dit geldt ook in het geval van uitbesteed beheer, waarbij geldt dat de gemeente Beekdaelen te allen tijde verantwoordelijk is voor de betrouwbaarheid van uitbestede diensten.
Medewerkers van de gemeente Beekdaelen worden gewezen op de verantwoor-delijkheden die gelden voor de omgang met (vertrouwelijke) informatie en de ICT-middelen waarmee die informatie toegankelijk is. De inrichting van systemen wordt aangepast op deze verantwoordelijkheden. Hetzelfde geldt voor externe partijen. Afspraken zijn duidelijk en eenduidig vastgelegd, waarbij de specifieke taken die belegd worden, benoemd zijn en afspraken over monitoring en rapportages expliciet gemaakt en gemonitord worden.

7.2 TECHNISCHE ASPECTEN

Nieuwe systemen, updates en functionele/technische wijzigingen worden getest in een testomgeving alvorens deze geïmplementeerd worden volgens de wijzigingsbeheer-procedure, die is opgesteld conform best practice.
Ten behoeve van de vertrouwelijkheid van informatie, wordt versleuteling toegepast op informatie die een bepaald classificatieniveau toegekend heeft gekregen. Voor fysieke informatie geldt dat deze adequaat afgeschermd dient te worden, denk aan afgesloten archiefkasten en het toepassen van een clean-deskbeleid.
Ten behoeve van de beschikbaarheid van informatie en continuïteit van bedrijfsvoering wordt in kaart gebracht welke informatie kritisch is. Op basis hiervan wordt bepaald hoe de back-up en restore processen voor die informatie(middelen) wordt ingericht.
Gevoelige informatie wordt binnen het netwerk zoveel mogelijk ondergebracht in netwerksegmenten met gepaste beveiligingsmaatregelen. Verkeer tussen verschillende segmenten wordt gemonitord en waar nodig gefilterd en gescand op virussen, malware en andere, ongewenste vormen van verkeer. Er is een duidelijk gedefinieerd plan en procedure in geval van een uitbraak van een virus of inbreuk op de beveiliging van informatie. (Dit is ook verplicht in het kader van de AVG en de Meldplicht datalekken. Dit wordt verder uitgewerkt in het hoofdstuk Beheer van incidenten.)

7.3 MOBIEL EN THUISWERKEN

Voor werken op afstand is een thuiswerkomgeving beschikbaar. Hierbij wordt toegang tot vertrouwelijke informatie verleend op basis van 'multi-factor' authenticatie.
Onder andere privé-apparaten vallen niet onder het beheer van gemeente Beekdaelen. Derhalve zijn voorzieningen en maatregelen getroffen zodat deze onbeheerde apparatuur gebruik kan maken van draadloze toegangspunten (Wifi) welke logische gescheiden zijn van het bedrijfsnetwerk.
Mobiele bedrijfsapplicaties worden bij voorkeur zo aangeboden dat er geen informatie wordt opgeslagen op het mobiele apparaat ('zero footprint'). Tevens wordt de informatie versleuteld bij transport en opslag conform de eisen, die daaraan gesteld worden in het kader van dataclassificatie.
E-mail is ongeschikt als middel om vertrouwelijke of geheime informatie uit te wisselen. De medewerker heeft echter in bepaalde gevallen behoefte aan het uitwisselen van gevoelige informatie. De gemeente Beekdaelen maakt gebruik van een applicatie voor het veilig uitwisselen van privacygevoelige gegevens.
Voor het mobiel en/of thuiswerken tekent de medewerker een Verklaring mobiel werken, waardoor de medewerker zich bewust wordt van de geldende regels en de risico's die kleven aan mobiel werken.

7.4 UITWISSELING VAN INFORMATIE

Met betrekking tot de uitwisseling van informatie nemen medewerkers van de gemeente Beekdaelen de gedefinieerde classificaties in acht.
Communicatie via e-mail, usb sticks, et cetera wordt bewaakt om het ongewenst versturen van gevoelige informatie tegen te kunnen gaan of gecontroleerd en beheerst plaats te kunnen laten vinden.
Remote beheer, maar ook (externe) toegang door medewerkers wordt alleen toegestaan, indien noodzakelijk voor het uitoefenen van de functie en deze wordt gemonitord en waar ongewenst afgebroken.

7.5 LOGGING

Waar mogelijk worden kritische handelingen verricht in applicaties en systemen gelogd.
Logging vindt plaats, waarbij de inrichting van de logging dient te voldoen aan de gestelde eisen aan wettelijke bewaartermijnen en de kenmerken die bijdragen aan herleidbaarheid.

8 LOGISCHE TOEGANGSBEVEILIGING

De gemeente Beekdaelen beheerst het geheel aan maatregelen omtrent toegang tot gegevens en informatiesystemen. Hiermee worden risico's op ongeautoriseerde acties beperkt, zoals het ongeautoriseerd raadplegen, wijzigen, of gebruiken van gegevens en informatiesystemen. Een eerste stap in het beperken van deze risico's is de identificatie en authenticatie van gebruikers van applicaties en systemen. Logische toegang is gebaseerd op de classificatie van de informatie, zoals beschreven in hoofdstuk 4 van dit informatiebeveiligingsbeleid en op basis van het noodzakelijkheidscriterium. De eigenaar van de data is bevoegd toegang te verlenen tot een specifieke set aan informatie met een specifieke bevoegdheid (lees/schrijf/verwijder).

8.1 AUTHENTICATIE EN AUTORISATIE

Ten aanzien van herleidbaarheid en transparantie van uitgevoerde handelingen geldt als uitgangspunt dat geen generieke identiteiten aanwezig zijn of het gebruik hiervan beperkt wordt. De gemeente Beekdaelen maakt - waar mogelijk – gebruik van bestaande (landelijke) voorzieningen voor authenticatie, autorisatie en informatiebeveiliging (zoals DigiD en eHerkenning).
Wachtwoorden voldoen aan complexiteitseisen, welke worden afgedwongen door het systeem. Voor medewerkers met speciale bevoegdheden - zoals systeem en functioneel beheerders – gelden strengere eisen. Daarnaast is de gebruiker verantwoordelijk voor het geheim blijven van zijn wachtwoord. Periodiek dienen deze veranderd te worden.
Het toekennen van autorisaties behoort te zijn gebaseerd op gedefinieerde rollen. Autorisaties worden toegekend via functie(s) en organisatieonderdelen. Op basis van de dataclassificatie tabel wordt bepaald welke wijze van authenticatie gewenst is voor elk specifiek niveau. De autorisaties per rol en functie worden vastgelegd in een autorisatiematrix.
Het management van de gemeente Beekdaelen is verantwoordelijk voor het bepalen van de rol die elke medewerker moet vervullen. Daarnaast wordt bepaald welke autorisaties nodig zijn voor het raadplegen, opvoeren, muteren en afvoeren van gegevens. Tevens bepaalt het lijnmanagement de verantwoordelijkheden voor het juist afhandelen van de beveiligingsaspecten voor het aangaan, wijzigen, en beëindigen van een dienstverband of een overeenkomst met externen. De HRM-medewerkers van de gemeente Beekdaelen houden toezicht op dit proces.

8.2 EXTERNE TOEGANG

De gemeente Beekdaelen heeft maatregelen genomen, zodat externe partijen niet op eigen initiatief verbinding kunnen maken met het besloten netwerk, tenzij uitdrukkelijk overeengekomen. Hiervoor is een procedure gemaakt, die ook wordt gevolgd.
De externe partij is verantwoordelijk voor authenticatie en autorisatie van haar eigen medewerkers. De externe partij doet dit in overeenstemming met de geldende richtlijnen van de gemeente Beekdaelen. De gemeente Beekdaelen heeft het recht hierop controles uit te voeren en doet dat aan de hand van de audit-trail en interne logging.

8.3 BEVEILIGING VAN INFORMATIESYSTEMEN (SOFTWARE)

8.3.1 Organisatorische aspecten

Toetsing op Informatiebeveiliging is onderdeel van de toets voor projecten met een ICT-component en onderdeel van de PSA (Project Startarchitectuur) en PEA (Project Eindarchitectuur). Toetsing op architectuur en informatiebeveiliging is hier onderdeel van. Projectmandaten worden ten behoeve van behandeling in overleg (onder meer) voorzien van een advies op informatiebeveiliging. In het programma

van eisen voor nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen worden ook relevante beveiligingseisen opgenomen.

8.3.2 Softwareontwikkeling en onderhoud

Applicaties worden ontwikkeld en getest op basis van landelijke richtlijnen voor beveiliging, zoals richtlijnen voor beveiliging van webapplicaties[4]. Er wordt tenminste getest op bekende kwetsbaarheden conform best practices (bijv. OWASP top-10[5]).

De uitvoerfuncties van programma's maken het mogelijk om de volledigheid en juistheid van de gegevens te kunnen vaststellen, bijvoorbeeld door middel van checksums. Alleen gegevens die noodzakelijk zijn voor de gebruiker worden uitgevoerd (doelbinding), rekening houdend met beveiligingseisen (classificatie). Toegang tot de broncode is beperkt tot de medewerkers, die deze code onderhouden of installeren. Technische kwetsbaarheden worden regulier met een minimum van vier keer per jaar gerepareerd door 'patchen' van software, of 'ad hoc' bij acute dreiging. Welke software wordt geüpdatet wordt mede bepaald door de classificatie van de risico's.

8.3.3 Encryptie (versleuteling)

De gemeente Beekdaelen gebruikt encryptie conform de PKI-overheid standaard. Intern dataverkeer ('machine to machine') wordt conform classificatie beveiligd met certificaten. Ook worden beveiligingscertificaten centraal beheerd binnen de organisatie.

9 VERWERVING, ONDERHOUD EN ONTWIKKELING

Bij uitbesteding van processen, beheer en onderhoud, zijn afspraken over de aard en kwaliteit van dienstverlening vastgelegd. Er wordt streng gecontroleerd op bedreigingen voor de veiligheid, zoals gebrek aan secure coding[6], inbouwen van achterdeuren in software en kwaliteit van software in het algemeen. Ook het proces van aanbesteding wordt nauw gevolgd, waarbij eisen en wensen duidelijk worden gecommuniceerd en acceptatiecriteria voorafgaand aan de implementatie worden gedefinieerd en gedurende de loop van de implementatie worden gemonitord. Voor gebruik van algoritmen en software wordt waar mogelijk gebruik gemaakt van (open) standaarden en formaten, om effectiviteit en efficiëntie te kunnen behalen.

Bij zwaktes in software en wanneer nieuwe patches worden uitgebracht, wordt een zorgvuldig proces gevolgd om te bepalen of het uitvoeren van de patch of update wenselijk en/of nodig is.

10 BEHEER VAN INCIDENTEN

10.1 MELDING EN REGISTRATIE

Beveiligingsincidenten worden bij de Controller Informatie en Data (CISO) gemeld en vervolgens geregistreerd en bijgehouden in de incident administratie en eventueel kortgesloten met andere relevante actoren binnen de organisatie zoals de Controller Informatie en Data (FG). Tevens wordt er in geval van virus -of malwaremeldingen contact opgenomen met de leverancier van de antivirus/ antimalware software om zo snel mogelijk geüpdatete virusdefinities te kunnen ontvangen en installeren. Ook wordt in geval van inbreuk naast het management de Informatie beveiliging Dienst op de hoogte gesteld en bij ernstige inbreuk in het kader van de Meldplicht datalekken melding gemaakt bij de Controller Informatie en Data (FG). Voor afhandeling van de melding geldt de reguliere rapportage en escalatielijn.

De administratie van incidenten wordt onder meer gebruikt om vaak voorkomende incidenten of trends te signaleren. Elk nieuw incident wordt geëvalueerd waarbij op basis van een risicoanalyse wordt afgewogen welke maatregelen genomen kunnen worden om optreden van eenzelfde soort incident in de toekomst te voorkomen. De evaluatie wordt uitgevoerd of gecoördineerd door Controller Informatie en Data (CISO), die er tevens over rapporteert.

Over ernstige incidenten wordt gerapporteerd in de kwartaalrapportage van de Controller Informatie en Data (CISO).

De incidentbeheerprocedure is uitgewerkt en vastgesteld en beschrijft in detail de processtappen, die genomen dienen te worden bij een melding. De procedure voor aanmelding van een incident is bekend bij de medewerkers van de gemeente Beekdaelen.

11 BEDRIJFSCONTINUÏTEITSBEHEER

Informatiebeveiliging is een integraal onderdeel van het totale bedrijfscontinuïteitsproces en andere beheerprocessen binnen de gemeente Beekdaelen. Zoals eerder beschreven is de aanpak voor

4) Nationaal Cyber Security Centrum, NCSC

5) https://www.owasp.org/index.php/Main_Page

6) Secure coding is het veilig schrijven van codes door ontwikkelaars om zwakke plekken in software te voorkomen.

BEEKDAELEN

informatiebeveiliging binnen de gemeente Beekdaelen risk-based. Hiertoe voert elke afdeling een business impactanalyse uit voor informatiesystemen en bij nieuwe projecten. Afhankelijk van de bevindingen worden per afdeling vervolgacties gepland. Tevens heeft elke afdeling een eigen, vastgesteld plan voor Business Continuity Management (BCM) (bedrijfscontinuïteitsbeheer). Ook worden minimaal jaarlijks oefeningen of testen gehouden om de BCM-plannen te toetsen (opzet, bestaan en werking). Aan de hand van de resultaten worden de plannen bijgesteld en wordt de organisatie bijgeschoold. Elke medewerker is dan ook op de hoogte van het bestaan van het bedrijfscontinuïteitsplan en zijn of haar rol in geval van een calamiteit.

11.1 BELEIDSUITGANGSPUNT

De gemeente Beekdaelen heeft voor de belangrijkste processen en systemen continuïteits-/uitwijkplannen beschreven, welke door middel van een beheerst proces tot stand komen. Dit proces bevat tevens activiteiten ten aanzien van het periodiek testen en actueel houden van de continuïteitsplannen.

12 NALEVING

Over het bewaken van naleving van vigerende wet -en regelgeving, maar ook naleving van het informatiebeveiligingsbeleid en gemaakte afspraken met derde partijen van de gemeente Beekdaelen wordt gerapporteerd aan het bevoegde orgaan. Dit bewaakt op basis van een jaarlijks bijgewerkte lijst van vigerende wetten en regelgeving of aan alle verplichtingen is voldaan. Hierin wordt ook meegenomen het voldoen aan wetgeving in het kader van intellectueel eigendom, auteursrechten en gebruiksrechten. Belangrijke registraties behoren te worden beschermd tegen verlies, vernietiging en vervalsing.

Het Management is verantwoordelijk voor de uitvoering en de beveiligingsprocedures en de toetsing daarop (o.a. jaarlijkse in control statement). De afdeling bedrijfsvoering en externe hosting providers leggen verantwoording af over de naleving van het informatiebeveiligingsbeleid. Bij uitbestede (beheer)processen kan een verklaring voor diensten bij leveranciers worden opgevraagd, zoals een TPM[7] of ISAE3402-verklaring. Regelmatige security tests worden gepland en de uitvoering en opvolging daarvan bewaakt.

13 AFKORTINGENLIJST

ACIB	Algemeen Contactpersoon Informatie Beveiligings Dienst
AVG	Algemene Verordening Gegevensbescherming
BAG	Basisregistratie Adressen en Gebouwen
BCM	Business Continuity Management (bedrijfscontinïteitsbeheer)
BIG	Baseline Informatiebeveiliging Nederlandse gemeenten
BIV	Beschikbaarheid, Integriteit, Vertrouwelijkheid
BRP	Basis Registratie Personen
CISO	Chief Information Security Officer (informatiebeveiligingsfunctionaris)
DigiD	Systeem waarmee personen zich kunnen identificeren voor de digitake dienstverlening
eHerkenning	Gestandaardiseerd inlogsysteem waarmee organisaties hun diensten online toegankelijk kunnen maken
ENSIA	Eenduidige Normatiek Single Information Audit
FG	Functionaris Gegevensbescherming
IBD	Informatie Beveiligings Dienst
Multi-factor authenticatie	Combinatie van twee authenticatie methoden, zoals een wachtwoord en een token
PKI	Public Key Infrastructure, de internationale standaard voor het beveiligen van gegevens en berichten

7) Een Third Party Mededeling (TPM) of Derdenverklaring is een verklaring die afgegeven wordt door een onafhankelijk audit partij over de kwaliteit van een ICT-dienstverlening en –beheersing van een organisatie.

PUN	Paspoort Uitvoeringsregeling Nederland
TPM	Third Party Mededeling (Derdenverklaring)
VCIB	Vertrouwelijk Contactpersoon Informatie Beveiligings Dienst