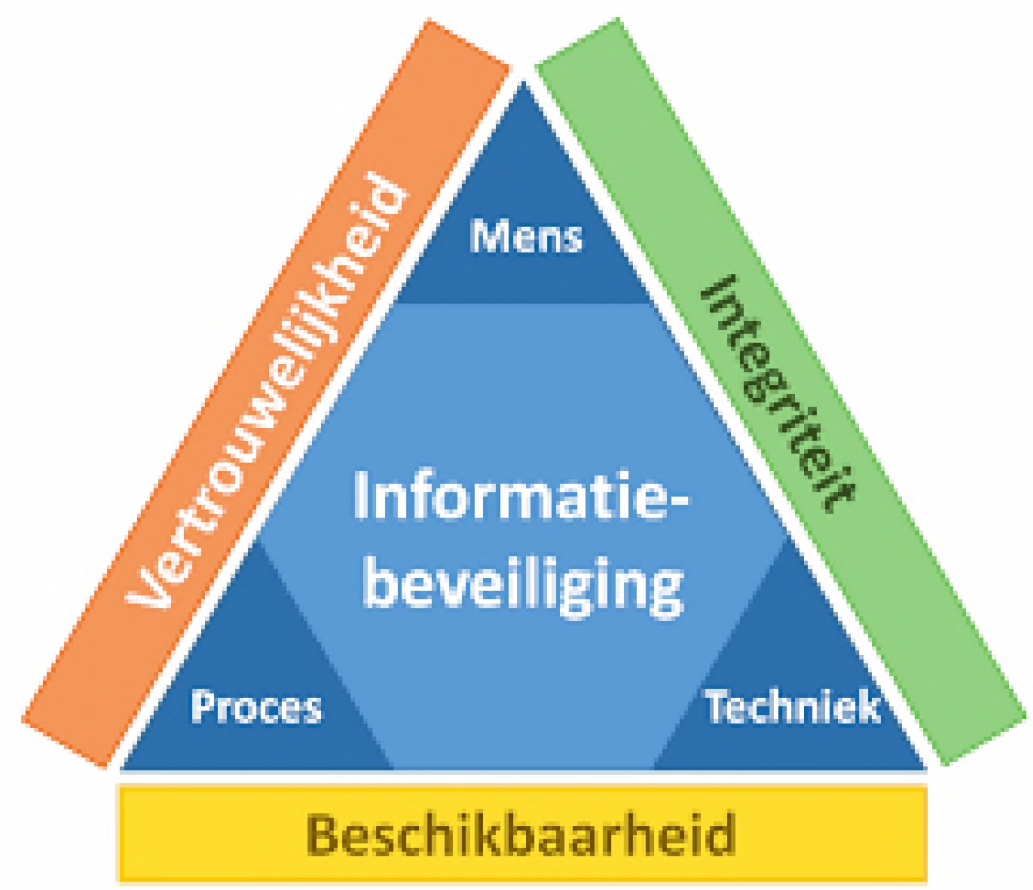
Informatiebeveiligingsbeleid Gemeente Meppel



Documentbeheer

Beheersinformatie	
Document of registratie	Informatiebeveiligingsbeleid gemeente Meppel
Bewaartermijn	-
Classificatie	-

Versiebeheer			
Versie	Datum	Auteur	Opmerkingen
0.98	03-11-2022	CISO (RT)	
0.99	06-09-2023	CISO (RT)	Verwerken van optimalisatie aspecten vanuit de organisatie (Directie / Management)
1.0	19-09-2023	CISO (RT)	Na vaststelling door College

Distributielijst		
Versie	Datum	Verspreid aan
0.99	29-06-2023	Directie, Management, Concern Controller, FG en VIC

Eigenaar			
Versie	Datum	Eigenaar	Herziening
0.99	29-06-2023	CISO	

Inhoudsopgave

Voorwoord

Bedrijven, maar vooral gemeentes, die beschikken over en werken met persoonsgegevens moeten zich houden aan de wettelijke eisen op het gebied van informatiebeveiliging. In mei 2018 werd de Algemene verordening gegevensbescherming (AVG), in het Engels ook wel GDPR genoemd, van kracht waarbij de wetgeving rondom gegevensbescherming wordt uitgebreid naar de hele EU.

Wetten veranderen continue, naast de AVG heeft de gemeente sinds 2021 ook te maken met de Wet Politiegegevens, vanuit haar taak en rol op gebied van Openbare Orde en Veiligheid, uitgevoerd door de Buitengewoon Opsporing Ambtenaren (BOA). Deze wet is van invloed op het informatiebeveiligingsbeleid.

Vanuit de EU wordt de Network en Information Security (NIS2) directive ingevoerd vanaf 2024, deze, deze directive (een EU wet), richt zich op risico's, die netwerk- en informatiesystemen bedreigen, zoals cyberbeveiligingsrisico's en brengt mogelijk extra verplichtingen met zich mee, vanuit aspecten als zorgplicht, meldplicht en toezicht.

De dreiging door Cybercriminelen en ondermijning neemt toe. Continue, 24u/7dagen per week gedurende 365 dagen per jaar proberen onbevoegden een ingang te vinden in het gemeentelijke netwerk. Ook de (potentiële) gevolgen van een aanval, denk hierbij aan sabotage of datadiefstal wordt groter. Om die reden is toezicht en controle steeds noodzakelijker.

Naast wetten zijn er ook richtlijnen en normen, zoals de Baseline Informatiebeveiliging Overheid die continue aan verandering onderhevig is. Naar verwachting, in 2024 komt er een nieuwe BIO 2.0 uit, waarbij de focus vooral ligt op de organisatie en haar verantwoordelijkheid, in plaats van het implementeren en uitvoeren van grotendeels technische maatregelen. Tegelijkertijd is duidelijk geworden dat de controle op zowel de organisatie, het proces of de maatregelen steeds verder en dieper gaat.

Gemeenten verantwoorden zich elk jaar, over de kwaliteit van de informatieveiligheid, van de in gebruik zijnde informatiesystemen. Per juli 2017 moeten gemeenten dit verplicht doen via de audit systematiek ENSIA: Eenduidige Normatiek Single Information Audit. Rijk toezichthouders, zoals bijvoorbeeld voor DigiD (Logius) en Suwinet, dwingen een collegeverklaring hieromtrent af, inclusief bijhorende Assurance verklaring van een door de Nederlandse Orde van Register EDP-Auditor (NOREA), erkende auditor.

Zo heeft Logius vastgesteld dat de gemeente Meppel weliswaar voldaan heeft aan de voorwaarden voor de continuering van het gebruik van DigiD in 2023 is hieraan ook een actiepunt gekoppeld ter aanpassing van informatiebeveiligingsbeleid. Zo moet het informatiebeveiligingsbeleid nu ook waarborgen bieden voor webapplicatie gerelateerde onderwerpen, zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer. Het informatiebeveiligingsbeleid moet uiterlijk 31-12-2023 hierin voorzien.

Alle aspecten hierboven, maar ook belangrijke toekomstverwachtingen zijn de oorzaak, dat er nu een nieuw informatiebeveiligingsbeleid voor u ligt, geldend vanaf 2023 voor de gemeente Meppel.

Burgemeester Gemeente Meppel
R.T.A. Korteland

1. Inleiding

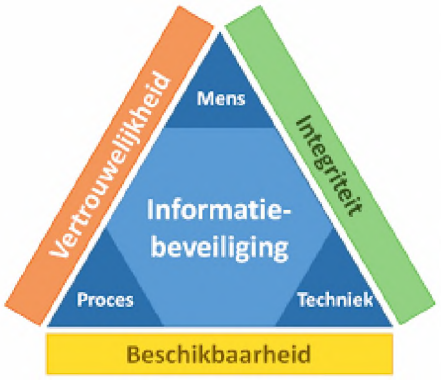
1.1 Wat is Informatiebeveiliging

Informatiebeveiliging is het nemen van alle nodige maatregelen om de veiligheid van informatie te garanderen, met als doel de informatie en daarbij informatievoorziening te borgen en de eventuele risico's hieromtrent te voorkomen. Informatiebeveiliging is een verplichting voor alle gemeentes.

1.2 Doel Informatiebeveiligingsbeleid

Het doel van dit Informatiebeveiligingsbeleid is het vast- en bekend stellen van de strategische uitgangspunten en randvoorwaarden die de gemeente Meppel hanteert voor haar informatiebeveiliging.

1.3 Waaruit bestaat het informatiebeveiligingsbeleid



Het informatiebeveiligingsbeleid bestaat uit veel onderlinge afhankelijkheden. Centraal staat de informatie en de beveiliging daarvan met kaders die invloed hebben hierop, op het gebied van:

- Werking systeem *(Beschikbaarheid)*,
- Juistheid *(Integriteit)*,
- Geheimhouding *(Vertrouwelijkheid)*.

De beveiliging van informatie wordt daarnaast beïnvloedt door gemeentelijke beleid, het gedrag van mensen en de (technische) middelen

- Doelmatigheid *(Proces)*,
- Rechtmatigheid *(Mens)*,
- Mogelijkheden *(Techniek)*.

1.4 Reikwijdte informatiebeveiligingsbeleid

Dit informatiebeveiligingsbeleid (IB) is van toepassing op alle gemeentelijke processen, onderliggende informatiesystemen, informatie en gegevens, in gebruik bij de gemeente, ongeacht locatie, tijdstip en gebruikte apparatuur.

1.5 Risico's ten aanzien van informatiebeveiliging

We zijn als samenleving steeds afhankelijker van de informatiesystemen van onze overheden en uitval van deze systemen grijpt steeds dieper in de samenleving. Wanneer sprake is van een (onverwachte) gebeurtenis die een of meerdere informatiesystemen treft spreken we van een informatiebeveiliging incident. Voorbeelden van incidenten zijn Pandemieën, brand, overstroming, maar ook overbelasting van systemen, veroudering of simpelweg uitval van apparatuur als gevolg van defecten. Allemaal risico's die meegenomen moeten worden in het nemen van de juiste beveiligingsmaatregelen. Daarnaast neemt de dreiging van Cybercriminelen ook toe. Continue, 24u/7dagen per week gedurende 365 dagen per jaar proberen onbevoegden een ingang te vinden in het gemeentelijke netwerk. Naast het continué risico hiervan, worden ook de (potentiële) gevolgen van een aanval, steeds ernstiger. Sabotage, datadiefstal maar ook ransomware en zelfs ondermijning, allemaal voorbeelden van risico's waardoor steeds zwaardere maatregelen noodzakelijk zijn, voor het voorkomen hiervan tot het mitigeren van deze risico's bij een eventuele aanval.

De mogelijke gevolgen van een informatiebeveiliging incident kan beperkt zijn van het tijdelijk niet beschikbaar zijn van informatie op de website of het tijdelijk niet uit kunnen geven van een paspoort tot het moeten toekennen van nieuwe Burger Service Nummers aan alle inwoners van de gemeente en het vervangen van alle identiteitsbewijzen (paspoorten en Europese Identiteitskaarten) en rijbewijzen zoals de hack van de gemeente Buren heeft geleerd.

1.6 Leeswijzer

Dit informatiebeleid is geschreven op hoofdlijnen, waarbij er voor gekozen is om niet alles in detail te willen vastleggen, tenslotte zijn het vooral beleidsuitgangspunten. Desondanks is er voor de duidelijkheid en leesbaarheid soms gekozen voor verdieping. Dit hoofdstuk, hoofdstuk 1 beschrijft vooral algemene aspecten. In hoofdstuk 2 worden vooral kaders en wetten toegelicht. Qua beleid, maar ook bepaalde risico aspecten, wat is specifiek voor Meppel, staat in Hoofdstuk3. Hoofdstuk 4 is volledig nieuw, ten opzichte van het vorige beleid en gaat heel diep in de op de organisatie van de informatiebeveiliging. Wie is verantwoordelijk voor wat, welke taken horen daarbij en hoe zijn deze functies verbonden met elkaar. Belangrijke processen worden besproken in hoofdstuk 5, maar specifieke (BIO) maatregelen worden alleen benoemd in hoofdstuk 6. Communicatie en Rapportage worden respectievelijk beschreven in hoofdstuk 7 en 8.

2. Kaders

2.1 Koers

In de visie Koers uit 2202 is onder andere weergegeven dat de gemeente Meppel een partner wil zijn voor iedereen in de gemeente waarbij betrouwbaarheid, privacy en dienstverlening voorop staan.

2.2 Collegeakkoord 2022-2026

Ook het collegeakkoord is van invloed op het informatiebeveiligingsbeleid van de gemeente, met onder andere de volgende ambitie:

"Mensen moeten op een laagdrempelige manier betrouwbare informatie kunnen krijgen"

2.3 Baseline Informatiebeveiliging Overheid

Het gemeentelijk Informatiebeveiligingsbeleid is gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO). De BIO beschrijft het minimale basisniveau voor informatiebeveiliging voor alle overheden. De BIO heeft als doel om de veiligheid te vergroten en is gebaseerd op internationale standaarden. Medio 2023 wordt naar verwachting de BIO2.0 van kracht, waarbij de organisatie van de informatiebeveiliging centraal staat, naast secundaire procesmatige of technische maatregelen.

2.4 Algemene Verordening Gegevensbescherming (AVG)

De belangrijkste regels voor de omgang met persoonsgegevens voor een gemeente zijn vastgelegd in de Algemene Verordening Gegevensbescherming (AVG). De AVG gaat over het rechtmatig omgaan met persoonsgegevens. Zo mogen gegevens alleen verwerkt worden voor een gerechtvaardigd doel en moet de betrokkenen weten hoe de gegevens verwerkt worden.

2.5 Wet Politie Gegevens (Wpg)

De Wet politie Gegevens (Wpg) regelt de verwerking van persoons gegevens voor de uitoefening van de politietaak door onder meer de Nationale Politie, de bijzondere opsporingsdiensten, de Koninklijke marechaussee en de Rijksrecherche. Voor organisaties waar Boa's werkzaam zijn, zoals bij de gemeente Meppel geldt ook de Wpg naast de hiergenoemde AVG. De kern van de WPG is vergelijkbaar aan de AVG en stelt ook dat alleen noodzakelijk, rechtmatig en doel gebonden gegevens verzameld mogen worden en dat de betrokkene moet weten hoe de gegevens verwerkt worden.

2.6 Wet Open Overheid (WOO)

De Wet open overheid (WOO) regelt het recht op informatie over alles wat de overheid doet. Het is de opvolger van de Wet openbaarheid van bestuur (Wob). Iedereen kan overheidsinformatie opvragen. Sommige informatie mag echter nooit openbaar gemaakt worden. Zoals vertrouwelijke of privacygevoelige informatie, of omdat het de veiligheid in gevaar brengt. Omdat de WOO meer openheid van overheden beoogt, betekent dit een omslag in het denken waarbij veel meer aan de voorkant nagedacht moet worden over welke gegevens wel en niet openbaar gemaakt mogen worden.

2.7 Overige Wetgeving

Naast bovenstaande wetgeving zijn er meer wetten en verordeningen, gericht op andere taakvelden van onze organisatie. Deze wetten of verordeningen, hebben raakvlakken, die impact hebben op informatiebeveiliging. Denk hierbij aan wettelijke eisen op gebied van beschikbaarheid en/of vertrouwelijkheid en daardoor eisen stellen aan het niveau van informatiebeveiliging. Deze kaders zijn hier niet verder beschreven, maar zijn onverminderd van kracht.

2.8 Definitie Beveiligingsincident

Een beveiligingsincident is een inbreuk op de beveiliging, waarbij de beschikbaarheid, de integriteit of de vertrouwelijkheid van informatie in gevaar is of kan komen.

2.9 Definitie Datalek

Bij een datalek gaat het om ongeoorloofde of onbedoelde toegang tot persoonsgegevens. Maar ook om het ongewenst vernietigen, verliezen, wijzigen en verstrekken van persoonsgegevens.

3. Beleid

3.1 Ambitie

De gemeente Meppel wil vanuit haar ambitie volledig voldoen, aan de uitgangspunten zoals gedefinieerd in de richtlijn Baseline Informatiebeveiliging Overheid (BIO) en aanvullende wetgeving

3.2 Verantwoordelijkheid

Verantwoordelijkheid is binnen Meppel, principieel belegd in de lijnorganisatie. Dit betekent dat de teammanager functioneel eindverantwoordelijk is voor alle aspecten op het gebied van informatiebeveiliging voor wat betreft de kernprocessen en zijn team. Uitvoerend technische aspecten zijn grotendeels belegd bij het team I&ID.

3.3 Need To Know

Medewerkers moeten alleen toegang hebben tot het taakveld waarin zij werkzaam en voor opgeleid zijn. Het belangrijkste uitgangspunt is daarom, dat alle middelen, toegangsrechten, fysiek of logisch beperkt worden tot het directe taakveld van de medewerker, op basis van taak of rol. Dit wordt het Need To Know (N2K) principe genoemd. Met het hanteren van need to know uitgangspunt verklein je de kansen op fouten of misbruik van informatie door medewerkers.

3.4 Toegangsbeleid

Het gemeentehuis, en de toegang tot de andere gemeentelijk infrastructuur is gebaseerd op fysieke toegangsbeveiliging maatregelen, zoals een toegangsmedium maar ook, cameratoezicht, inbraakalarm en brandmelding systemen.

Logische maatregelen voor toegang tot informatie en systemen zijn gebaseerd op specifieke rollen die aan een medewerker zijn toegekend, waarbij N2K, Single Sign On en Multi-factor authenticatie, minimaal vereist zijn.

Voor meer details over het complete toegangsbeleid, zie bijlage 1.

3.5 Single Sign-On

Single Sign-on (SSO) betekent dat eindgebruikers zich eenmalig hoeven in te loggen. De SSO-software zorgt er daarna voor dat authenticatie tot andere applicaties automatisch verloopt. SSO is rand voorwaardelijk voor alle nieuw in te voeren informatiesystemen.

3.6 Multi-Factor identificatie

2-Factor identificatie is gebaseerd op het principe dat je alleen kunt inloggen als je iets weet, inlognaam en wachtwoord, **en** als je iets hebt, bijvoorbeeld een token of app op je smartphone. Dit is veel veiliger dan toegang met alleen iets wat je weet, maar blijkt in de praktijk vaak nog vrij eenvoudig te omzeilen. Daarom wordt tegenwoordig gebruik gemaakt van Multi-Factor identificatie die is gebaseerd op minimaal 3 pijlers, iets wat je weet, iets wat je hebt **en** iets wat je bent zoals een vingerafdruk of gezichts- of retina scan

zoals mobiele telefoons die bieden. MFA of in uitzonderingsgevallen 2FA is randvoorwaardelijk voor het gebruik van alle informatiesystemen.

3.7 Monitoring & Response

Het risico van cyberdreigingen, maar ook ondermijning neemt nog steeds toe. Het is daarom noodzakelijk, geautomatiseerd 24u/7, 365 dagen per jaar, afwijkend gedrag van zowel systemen als gedrag te monitoren op de ICT-infrastructuur, vervolgens te analyseren op risico en indien nodig (geautomatiseerd) maatregelen te treffen voor de mitigatie hiervan.

3.8 Architectuur

Vanuit de strategie voor toekomstige informatievoorziening systemen is er in september 2022, besloten door het college B&W, om te kiezen voor een geleidelijke verschuiving van de applicaties en ICT-voorzieningen die we zelf beheren naar een situatie waarbij we de software en hardware buiten de organisatie plaatsen. Alle (nieuwe) informatiesystemen worden dus toekomstig zo veel als mogelijk via het Internet (de Cloud) beschikbaar gesteld. Omdat een groot deel van de informatievoorziening dan niet in meer "in eigen hand is" zijn eenduidige en kwalitatief goede overeenkomsten op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid een noodzakelijkheid.

3.9 ITIL

De gemeente Meppel heeft er vanuit het verbeterplan ICT 2021, voor gekozen om voor haar ICT-beheer processen zo veel mogelijk gebruik te maken van de Information Technology Infrastructure Library, meestal afgekort tot ITIL. ITIL is een "best practice" op het gebied van processen waaronder configuratie-, incident-, wijziging-, kwetsbaarheden- en configuratiebeheer. Deze processen moeten op basis van deze methodiek worden ingericht en uitgevoerd.

3.10 Risicoanalyse

Risicoanalyse wordt gebruikt om te bepalen hoe groot de risico's zijn, welke risico's op welke wijze verkleind kunnen worden, en welke risico's het meest urgent dienen te worden aangepakt. Vanuit het aspect informatiebeveiliging wordt een risico gedefinieerd als de kans dat een potentieel gevaar voor de informatiesystemen daadwerkelijk resulteert in een incident. Het gevolg beschrijft de ernst van de impact die het risico kan hebben voor de openbare orde en veiligheid, uitval van kritieke dienstverlening vanuit de gemeente, of de privacy van burgers. Vanuit een pragmatisch oogpunt, wordt een risicoanalyse altijd uitgevoerd met behulp van de volgende formule: Risico = Kans x Gevolg. De risicoanalyse is tevens input voor continuïteit plannen.

3.11 Bedrijfscontinuïteitsplan (BCP)

Het bedrijfscontinuïteitsplan (ook wel BCP genoemd) beoogt een zo snel mogelijke afhandeling, doorstart en herstel na een ernstige bedrijfscalamiteit. Dit om te voorkomen dat de gemeente financieel, organisatorisch en qua reputatie of imago zó zwaar beschadigd raakt, dat de wettelijk verplichte dienstverlening in gevaar komt of zelfs uitvalt.

Elk team heeft een eigen plan voor continuïteit van de "eigen" processen of taken, in dit continuïteitsplan wordt minimaal aandacht besteed aan:

- Gedegen risicoanalyse

- Identificatie van essentiële procedures voor bedrijfscontinuïteit;
- Afhankelijkheid van systemen of middelen
- Wie het bedrijfscontinuïteitsplan 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 bedrijfsprocessen;
- Kennis en kundigheid van medewerkers om de bedrijfsprocessen weer op te starten.

3.12 Beveiligingsniveau (Dataclassificatie)

Binnen de gemeente Meppel is de proceseigenaar ook systeemeigenaar van de bijbehorende informatiesystemen (in veel gevallen is dit de teammanager). De systeemeigenaar is verantwoordelijk voor het vaststellen en vastleggen van het juiste beveiligingsniveau van deze informatiesystemen. Dit beveiligingsniveau richt zich dan op eisen zoals de (ongestoorde) werking van het systeem (Beschikbaarheid), het borgen van de openbaarheid en geheimhouding van gegevens (vertrouwelijkheid), juistheid van informatie (integriteit). Voor het vaststellen van het juiste beveiligingsniveau, volgt de gemeente Meppel de "Handreiking Dataclassificatietoets BIO Gemeenten".

3.13 Aanvaardbaar Gebruik van (ICT) middelen

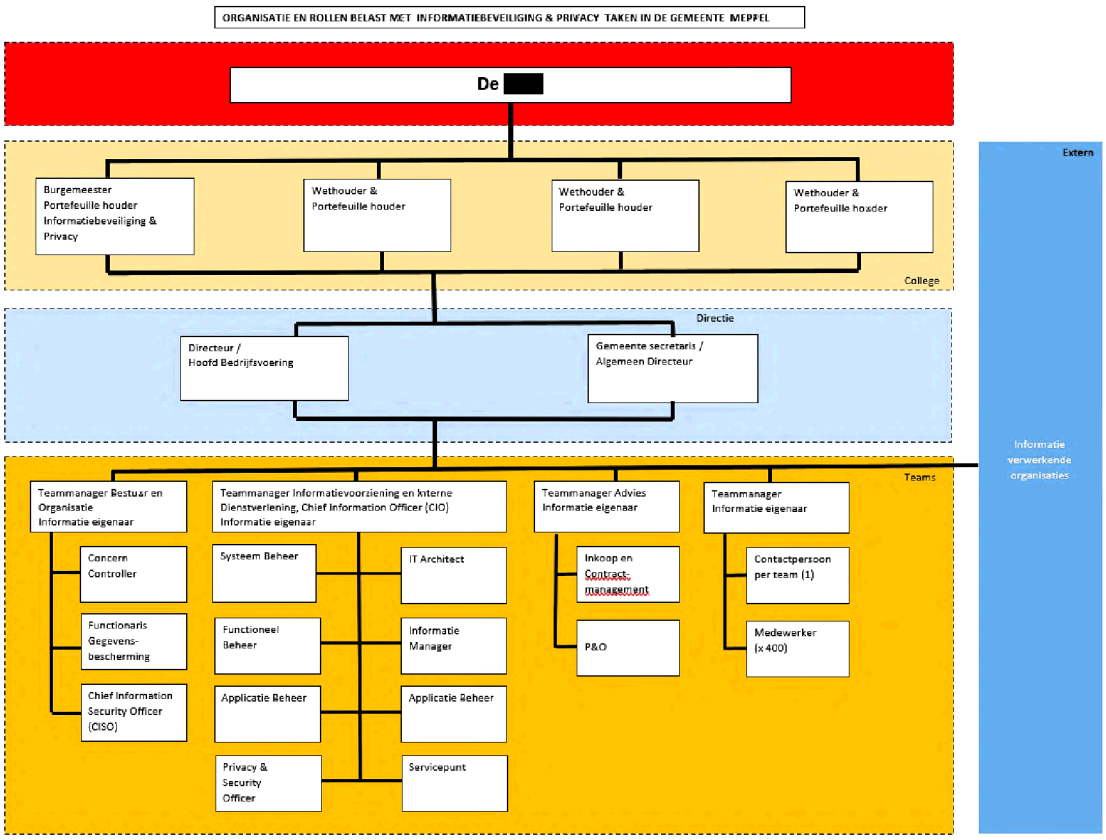
Het gebruik van internet en ICT-middelen is voor (veel van) de werknemers binnen de gemeente noodzakelijk om hun werk goed te kunnen doen. Aan het gebruik hiervan zijn echter risico's verbonden die het stellen van gedragsregels noodzakelijk maken. Deze regels voor aanvaardbaar gebruik worden ook wel een Acceptable Use Policy genoemd (AUP). Tegen de achtergrond van deze risico's mag van de werknemers verantwoord gebruik van internet en ICT worden verwacht. De gemeente Meppel heeft de regels omtrent het gebruik van deze middelen vastgelegd in het personeelshandboek.

3.14 Opleiding (awareness)

Om gebruik te mogen maken van de informatiesystemen moet iedereen die werkzaam is voor de gemeente Meppel, deelnemen aan de verplichte informatiebeveiliging trainingen. Naast bewustwording van risico's in het gebruik van informatiesystemen, worden ook onbedoelde fouten hiermee voorkomen en komt dit de efficiënt gebruik ten goede. Dit kunnen trainingen zijn zoals: Introductieprogramma voor nieuwe medewerkers.

- E-learning genaamd Basiskennis informatieveiligheid en Privacy.
- E-learning (taken) in relatie tot specifieke onderwerpen.
  (Denk hierbij AVG, ondermijning, enzovoorts, deze worden ad-hoc op specifieke momenten op/ of verzoek uitgestuurd via email)
- Micro-learning via e-mail (sir Askalot)
- Maatwerktrainingen zoals bijvoorbeeld voor gebruikers van SUWINET

4. Organisatie, Taken en Rollen (Mens)



Afbeelding 2, Belangrijkste rollen ten aanzien van informatiebeveiliging binnen Meppel.

4.1 De Raad

De raad neemt, als hoogste orgaan binnen de gemeente, kennis van dit informatiebeveiligingsbeleid. Indien gewenst kan de raad voorstellen indienen ter verbetering van dit beleid, zolang deze niet strijdig zijn met enig wet of regelgeving.

4.2 College B&W

Het College van Burgemeester en Wethouders is integraal (politiek) verantwoordelijk voor de beveiliging van informatie en de borging van de privacy binnen de gemeentelijke bedrijfsprocessen. Zij stelt kaders op voor informatiebeveiliging en de bescherming van privacy op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders. Dit stelt het college vast in het informatiebeveiligingsbeleid. Het college mandateert de ambtelijke verantwoordelijkheid op het gebied van informatiebeveiliging en privacy aan de gemeentesecretaris. Vanuit het bovenstaande resulteert dit in volgende verantwoordelijkheden en taken:

- Het College van B&W stelt het informatiebeveiligingsbeleid vast.
- Stelt kaders op voor informatiebeveiliging en de bescherming van privacy op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders.
- Neemt kennis van rapportages op gebied van informatiebeveiliging en informeert hierover de raad.
- Bij politieke wijzigingsvoorstellen, worden deze door het college vooraf getoetst aan het informatiebeveiligingsbeleid.

4.3 Portefeuillehouder

De portefeuillehouder is vanuit het aspect Informatieveiligheid medeverantwoordelijk voor de toegekende portefeuilles en gerelateerde processen. Voor een exact overzicht wie als wethouder gekoppeld is aan de specifieke portefeuilles wordt verwezen naar het coalitieakkoord. Vanuit deze verantwoordelijkheid heeft de portefeuillehouder de volgende taken;

- Verantwoordelijk voor de juiste informatiebeveiligingsmaatregelen, voor toegekende portefeuilles, zoals vastgelegd in het coalitieakkoord.
- Kennis te nemen van informatiebeveiligingsrapportages inzake eigen portefeuilles
- Knelpunten informatiebeveiliging inzake eigen portefeuilles bespreken
- Politieke wijzigingsvoorstellen, vooraf te toetsen aan het informatiebeveiligingsbeleid

4.4 Directie

De directie is de opdrachtnemer van het college. De directie is verantwoordelijk voor het functioneren van de ambtelijke organisatie in al zijn aspecten, waaronder informatiebeveiliging en privacy. Vanuit deze verantwoordelijkheid heeft de directie de volgende taken;

- adviseert het college van B&W over het vast te stellen strategische beleid.
- Ziet toe op de uitvoering en kwaliteit van het informatiebeveiligingsbeleid.
- Zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een teamleider en ziet erop toe dat de teamleiders adequate maatregelen nemen.
- Vasstellen van aanvullende beleid maatregelen op gebied van IB&P
- Neemt kennis van de rapportages op gebied van informatiebeveiliging
- Stuurt de CISO functioneel aan qua taakstelling, prioritering in relatie tot informatie beveiliging vraagstukken.

4.5 De Gemeente Secretaris (tevens Algemeen Directeur)

De Gemeente Secretaris is namens de Burgemeester opdrachtnemer voor het opstellen, toezicht op, en uitvoering van het informatiebeveiligingsbeleid en rapporteert hierover, regelmatig aan het College van B&W. Vanwege functiescheiding is opstelling van het beleid en bijhorende toezichtfunctie belegd bij de CISO. Terwijl de uitvoering van het beleid belegd is bij de respectievelijke teammanagers. Daarnaast heeft de gemeentesecretaris de volgende taken;

- Verantwoordelijk voor de uitvoering van dit beleid.
- Bespreekt informatiebeveiliging regelmatig binnen de directie.
- Neemt kennis van kwartaalrapportages inzake informatieveiligheid.
- Bespreekt informatiebeveiliging in de voortgangsgesprekken met de TM.

4.6 De Directeur

De Directeur is namens de Gemeentesecretaris belast met de uitvoering van het informatiebeveiligingsbeleid binnen zijn of haar deelgebied en rapporteert hierover aan de Gemeentesecretaris. Daarnaast heeft de directeur de volgende taken;

- Ondersteunt de gemeentesecretaris in de uitvoering van dit beleid.
- Neemt kennis van kwartaalrapportages inzake informatieveiligheid.
- Bespreekt informatiebeveiliging in de voortgangsgesprekken met de TM.

4.7 Concern Controller (CC)

De CC is op organisatieniveau tevens adviserend voor het concern belang in relatie tot het informatiebeveiligingsbeleid en werkt hierin nauw samen met de CISO en Functionaris Gegevensbescherming (FG). De belangrijkste taak van de CC in dit beleid is de;

- Toezicht op uitgevoerde controles, informatiebeveiliging en privacy in de kwartaal en jaar rapportages.

4.8 Functionaris Gegevensbescherming (FG)

De FG is conform de algemene verordening gegevensbescherming (AVG) de interne toezichthouder en adviseur binnen de gemeente op de verwerking van persoonsgegevens. In deze werkt de FG nauw samen met de CISO en PO. De belangrijkste taken voor de functionaris gegevensbescherming zijn;

- Eerste aanspreekpunt, vanuit de gemeente Meppel voor de Autoriteit Persoonsgegevens (AP) bij geconstateerde incidenten of overtredingen op de AVG
- Verwerkingsverantwoordelijken, de proceseigenaren en haar medewerkers te informeren en adviseren, over hun verplichtingen op basis van de AVG, andere privacy gerelateerde wetgeving.

4.9 Chief Information Security Officer (CISO)

De CISO definieert het informatiebeveiligingsbeleid, namens de gemeentesecretaris en organiseert en ziet toe op uitvoering van de informatiebeveiligingstaken van de organisatie, overeenkomstig de behoeften en risicobereidheid. De belangrijkste taken voor de CISO zijn;

- Opstellen en bijstellen van het informatiebeveiligingsbeleid in lijn met de gebruikelijke PDCA-cyclussen van de gemeente.
- Het coördineren en adviseren bij afhandelen van beveiligingsincidenten.
- De afstemming van informatiebeveiliging met belanghebbenden.
- Het toezien op naleving van de eisen voor informatiebeveiliging.
- Het bevorderen van het informatiebeveiligingsbewustzijn
- De voorbereiding op toekomstige informatiebeveiligingsrisico's en ICT-beveiligingsrisico's o.b.v. het dreigingsbeeld Nederlandse Gemeenten

4.10 Teammanager I&ID

Het uitvoeren en toepassen maar vooral ook technische beheer aspecten of maatregelen van het Informatiebeveiligingsbeleid, vallen specifiek onder de verantwoordelijkheid van de teammanager I&ID. Om deze verantwoordelijkheid te kunnen uitvoeren worden deze ondersteund hierin door de Concern controller, de CISO en de FG. Hierbij is de teammanager I&ID specifiek vooral verantwoordelijk voor;

- Het in gesprek gaan en blijven met de Directie, Portefeuillehouders en het lijnmanagement over technische en functionele invalshoeken voor maatschappelijke opgaven, zodat het informatiebeveiligingsbeleid uitvoerbaar blijft.
- Het ondersteunen en laten vaststellen van het juiste beveiligingsniveau voor bedrijfsprocessen, informatiesystemen en applicaties, vanuit een informatie-eigenaar[1] perspectief, in lijn met geldende wetgeving en gemeentelijke beleid.
- Het vaststellen van kritieke gemeentelijke processen binnen zijn domein.
- Het opstellen, afstemmen en vaststellen van een teamcontinuïteitplan (BCP) voor de kritieke processen.
- Het vaststellen van de juiste autorisaties, van medewerkers binnen het team

- Het toekennen van de juiste autorisaties binnen informatiesystemen waarvoor de TM als informatie-eigenaar is gedefinieerd.
- Het vergroten van informatieveiligheidsbewustzijn van medewerkers .
- Uit laten voeren van risicoanalyses, bijvoorbeeld bij het aantrekken nieuw personeel, nieuwe systemen, nieuwe verwerkingen.
- Het evalueren van veiligheidsincidenten en datalekken, naast meldplicht aan de PO, collegiaal delen als dit bij kan dragen aan het voorkomen van soortgelijke incidenten, elders in de gemeente,
- Het laten uitvoeren van noodzakelijke controles [2] op gebied van informatiebeveiliging binnen het domein.
- Minimaal 3-maandelijks rapporteren aan de Directie, omtrent het aantal geconstateerde datalekken, veiligheidsincidenten, uitgevoerde controles en niveau van informatiebeveiligingsbewustzijn.
- Voert regelmatig functioneel (horizontaal) overleg met de CISO en FG.

4.11 Teammanager (TM)

Het uitvoeren en toepassen van het Informatiebeveiligingsbeleid valt onder de verantwoordelijkheid van de teammanager. Om deze verantwoordelijkheid te kunnen uitvoeren worden zij ondersteund door een of meerdere teamcontactpersonen, de CISO en de PO/SO van I&ID. Hierbij is de teammanager vooral verantwoordelijk voor;

- Het vaststellen van het juiste beveiligingsniveau voor informatiesystemen en applicaties, vanuit een informatie-eigenaar[1] perspectief, in lijn met wetgeving en gemeentelijke beleid.
- Het vaststellen van kritieke gemeentelijke processen binnen zijn domein.
- Het opstellen, afstemmen en vaststellen van een teamcontinuïteitplan (BCP) voor de kritieke processen.
- Het vaststellen van de juiste autorisaties, van medewerkers binnen het team
- Het toekennen van de juiste autorisaties binnen informatiesystemen waarvoor de TM als informatie-eigenaar is gedefinieerd.
- Het vergroten van informatieveiligheidsbewustzijn van medewerkers
- Uit laten voeren van risicoanalyses, bijvoorbeeld bij het aantrekken nieuw personeel, nieuwe systemen, nieuwe verwerkingen.
- Het evalueren van veiligheidsincidenten en datalekken, naast meldplicht aan de PO, collegiaal delen als dit bij kan dragen aan het voorkomen van soortgelijke incidenten, elders in de gemeente,
- Het laten uitvoeren van noodzakelijke controles [2] op gebied van informatiebeveiliging binnen het domein.
- Minimaal 3-maandelijks rapporteren aan de Directie, omtrent het aantal geconstateerde datalekken, veiligheidsincidenten, uitgevoerde controles en niveau van informatiebeveiligingsbewustzijn.

4.12 Contactpersoon informatiebeveiliging & privacy (CIP)

Per team, kan een medewerker gemandateerd worden (naast de eigen taken) voor Informatieveiligheid & Privacy aspecten. Deze functionaris, de contactpersoon Informatiebeveiliging en Privacy (CIP) voert deze taken dan uit namens de teammanager. Deze taken, en het bijbehorende mandaat moeten, vanuit een (extern) audit perspectief, schriftelijk door de teammanager worden vastgelegd. Voorbeelden van direct te delegeren taken kunnen zijn:

- De 3-maandelijkse controle van autorisaties.
- De Jaarlijks Actualisatie van continuitsplannen.
- Het vergroten van het veiligheidsbewustzijn
- Het voorbereiden van kwartaalrapportages.

- Enzovoorts.

4.13 Privacy en Security Officer (PO/SO)

De PO/SO is het eerste aanspreekpunt binnen de gemeente op de verwerking van persoonsgegevens. Als SO adviseert en ziet hij daarnaast toe of alle maatregelen conform het informatiebeveiligingsbeleid worden toegepast en uitgevoerd. De PO/SO heeft een functionele relatie met zowel de CISO en FG. De belangrijkste taken van de PO/SO zijn;

- Het ondersteunen van de organisatie om aan de wettelijke verantwoordelijkheid inzake privacyregelgeving te voldoen,
- Het melden van datalekken aan de AP met informatieplicht aan Directie, verantwoordelijk Teammanager, FG en CISO
- Het uitvoeren van risico-inventarisaties:
    - Voor de PO zijn dat DPIA's
    - Voor de SO zijn dat RI&E's
- Het opstellen en herijken van beleidsstukken inzake IB&P
- Het bijhouden van verwerkingsregisters.
- Verplicht deelnemen aan het overleg van de wijzigingsadviescommissie.
- Stimuleren van informatieveiligheid

4.14 Inkoop Adviseur

Binnen het team Advies is het cluster Inkoop medeverantwoordelijk voor een aantal specifieke aspecten in relatie tot informatiebeveiliging. De belangrijkste taken en aandachtspunten voor inkoop zijn;

- Het alleen inkopen op basis GIBIT-voorwaarden van de VNG, GIBIT staat voor Gemeentelijke Inkoop bij IT Toolbox.
- Het voor aanschaf toezien op de uitvoering van een (pre-)DPIA bij verwerking van persoonsgegevens door derden
- Het voor aanschaf toezien op het opstellen en ondertekenen van een verwerkersovereenkomst
- Het opnemen van een Exit clausule binnen de overeenkomst, waarbij gemeentelijke data in een open format verplicht, beveiligd moeten worden aangeleverd aan de gemeente voordat de overeenkomst ten einde komt.
- Het toezien dat TPM's onderdeel zijn van nieuwe, of te verlengen contracten zodat er geen verborgen kosten zijn, indien deze t.b.v. audits later moeten worden aangeleverd.
- Het opstellen van een goed leesbare en interpreteerbare Service Level Agreement inclusief het vooraf definiëren van het basis beveiligingsniveau (dataclassificatie)
- Het toezien dat nieuwe applicaties of systemen in lijn zijn met de informatie- en ICT-architecturen en de BIO. Hierop mag alleen door de directie worden afgeweken.

4.15 Contract Managers

Leveranciersmanagement en toezicht houden op lopende contracten is een zeer belangrijk aspect, mede ter voorkoming van oneindig doorlopende contracten (rechtmatigheid) of het overschrijden van (Europese) regelgeving. Dit beleid is generiek dus voor diensten en producten. De belangrijkste taken van de contract manager zijn;

- Het bewaken van de contractafspraken op basis SLA en rapportages.

- Het bewaken en toezien op geldigheid van TPM en ISO-certificaten bij de leveranciers (monitoren actualiteit en geldigheid).
- Het bewaken en toezien op eventuele Escrow overeenkomsten.
- Het bewaken van de contractduur en verlenging.
- Het periodiek toetsen en actualiseren van de vastgelegde GIBIT-voorwaarden, (pre-)DPIA's, Verwerkersovereenkomsten en SLA's.

4.16 P&O adviseur

Binnen het team Advies is de personeelsafdeling verantwoordelijk voor werven en aannemen van veilig personeel. De belangrijkste taken voor de personeelsadviseur zijn;

- Het uitvoeren van een risicoanalyse in relatie tot nieuwe functies en bevoegdheden
- Het uitvoering geven aan het screeningsbeleid, bij in- en doorstroom
- Het uitvoering geven aan het uitstroombeleid
- Het beschikbaar stellen van budget voor Awareness trainingen
- Het periodiek uitvoeren van risicoanalyses in relatie tot functies en bevoegdheden

4.17 IT Architect (IA)

Gezien vanuit de term "basis op orde" is een goede informatiebeveiliging alleen mogelijk als veiligheid, het uitgangspunt is voor de bestaande en toekomstige ICT-infrastructuur. De belangrijkste taken van de IT Architect zijn;

- Het Security by Design (BIO, ISO27001, ISO27002) toe te passen als uitgangspunten voor de architectuurkeuze.
- Het gevraagd en ongevraagd, opstellen van of adviseren over de toepassing van de architectuurkaders, met betrekking tot informatiebeveiliging.
- Het ondersteunen van functionarissen bij hun verantwoordelijkheden in het kader van informatiebeveiliging.

4.18 Informatie Manager (IM)

De informatiemanager focust op wettelijke en maatschappelijke ontwikkelingen en geeft richting aan de doorontwikkeling van het informatielandschap. Vanuit een informatiebeveiligingsoogpunt is het zeer belangrijk dat het landschap en daarmee taken, verantwoordelijkheden en bevoegdheden goed zijn ingericht in relatie tot uit te voeren informatieprocessen. De belangrijkste taken van de Informatiemanager zijn;

- Het adviseren over processen die ten grondslag liggen aan informatiebeveiliging door duidelijk te maken, welke taken, verantwoordelijkheden en bevoegdheden, ingericht moeten worden.
- Adviseren over informatie- en applicatielandschap, in lijn met het informatiebeveiligingsbeleid en gedefinieerde ICT-architectuur
- Bijdragen aan bewustwording rond informatieveiligheid.
- Adviseren bij nieuwe of te wijzigen informatieprocessen zodat deze in lijn blijven, of met het informatiebeveiligingsbeleid.

4.19 Functioneel en Applicatie beheer

Het uitvoeren van functioneel en applicatie beheertaken voor systemen en applicaties is een van de allerbelangrijkste aspecten in relatie tot een goede informatiebeveiliging. Hierbij richt de functioneel beheerder zich vooral op het beheer van functionaliteiten, rolscheiding en autorisaties (vertrouwelijkheid),

terwijl de applicatie beheerder focust op aspecten als beschikbaarheid en Integriteit. Omdat beide taken in Meppel met elkaar verweven zijn is ervoor gekozen, deze in het beleid als één te beschrijven. De belangrijkste taken van de Functionele en Applicatie beheerders zijn;

- Inrichting, uitvoering en controle autorisaties en functiescheiding
- Invoeren van functionele normen en eisen (metagegevens)
- Melden van veiligheid incidenten en datalekken
- In voorkomend geval, zelfstandig extra beveiligingsmaatregelen treffen, mits direct noodzakelijk, met meldplicht achteraf

4.20 Technisch beheerder

Als de basis niet op orde is, ontstaan er grote risico's op het gebied van informatieveiligheid en privacy. Inrichting van de netwerkinfrastructuur, segmentering, interne en externe koppelingen, basiswerkplek, servers, back-ups, maar ook firewalls, indringerdetectie, zijn allemaal taken van de systeembeheerders. De systeembeheerder heeft daarom een zeer grote verantwoordelijkheid op het gebied van informatieveiligheid. De belangrijkste taken van de systeembeheerder zijn;

- Het zorgdragen voor de technische beveiliging van de gehele infrastructuur, op basis alle maatregelen zoals benoemd in bijlage A, conform de BIO
- Het zorgdragen voor d e technische uitvoering in relatie tot dataclassificatie beleid
- De inrichting, uitvoering en controle van generieke autorisaties en functiescheiding in relatie tot de basiswerkplek.
- Het invoeren van functionele normen en eisen (metagegevens)
- Het melden van risico's op gebeid van veiligheidsincidenten en datalekken
- Het dagelijks en periodiek monitoren van de infrastructuur
- Het zelfstandig extra beveiligingsmaatregelen treffen, mits direct noodzakelijk, met meldplicht achteraf

4.21 Het Servicepunt

Het servicepunt is het eerste aanspreekpunt in de organisatie voor het;

- Het aannemen en registreren van meldingen.
- Het houden van toezicht op de voortgang van meldingen.
- Het actief informeren van de SO/PO en CISO, wanneer er een inschatting is dat er sprake is van een ernstig of risicovol beveiligingsincident.
- Het houden van toezicht en controle op de uitvoering van de back-up.
- De uitvoering van het Configuratie Managementproces

4.22 Iedere Medewerker

Onbewust menselijk handelen is de belangrijkste bedreiging voor de gemeentelijke informatievoorziening. Onbewuste acties van medewerkers blijken een groter risico voor de privacy van burgers en de veiligheid van informatie dan bewuste en gerichte aanvallen door criminelen en medewerkers zijn dan ook de alles bepalende factor voor de informatieveiligheid. Gezien vanuit dat gezichtspunt heeft iedere medewerker de taak;

- Om uitvoering te geven aan dit beleid.
- Tot het volgen van aangeboden informatiebeveiliging trainingen.
- Om beveiligingsincidenten en datalekken direct te melden.
- Om verbeteringen of tekortkomingen in dit beleid te melden.

- Om hulp te vragen, bij twijfels over Informatieveiligheid & Privacy.
- Om collega's te attenderen en adviseren over informatiebeveiliging.

5. Processen

5.1 Crisismanagement

Crisismanagement in relatie tot informatiebeveiliging is noodzakelijk, als er een ontwrichtende verstoring of langdurige uitval (>48 uur) plaats vindt van gemeentelijke informatiesystemen, waarbij de gemeentelijke dienstverlening, de privacy van burgers, of openbare orde en veiligheid in gevaar komt. Indien zo een verstoring plaats vindt, moet een team geformeerd worden, wat bestaat uit minimaal de navolgende functionarissen:

Rol	Wie
Voorzitter	Burgemeester of Gemeentesecretaris
Secretaris	Bestuur of Management ondersteuning
Crisis verantwoordelijke	Meest betrokken proceseigenaren
OOV	Indien noodzakelijk
Informatievoorziening	Hoofd I&ID of zijn plaatsvervanger
Adviseur informatiebeveiliging	CISO of PO/SEC OFF I&ID
Communicatieadviseur	Team advies, cluster communicatie
Externe adviseur	Indien noodzakelijk (IBD, Politie, forensisch)

5.2 Incidentenbeheer

Zoals gedefinieerd in pararagraaf 2.8 is er is sprake van informatiebeveiligingsincident als de beschikbaarheid, vertrouwelijkheid of integriteit van informatiesystemen in gevaar komt. Het gaat hierbij dus niet alleen om malware op het netwerk, maar ook om andere ICT gerelateerde storingen, het ontbreken (of fout lopen) van een back-up, het verlies van gegevensdragers (USB/Laptop) of het achterlaten van een documenten bij een printer. De verplichting voor het melden van een incident is belegd bij elke persoon in de organisatie. Het proces incidentbeheer is vastgelegd en opgenomen in het maatregelenoverzicht van hoofdstuk 6.

5.3 Datalekken

Datalekken zijn gedefinieerd in pararagraaf 2.9, wat met zich meebrengt dat er een meldplicht is op het gebied van datalekken door de veroorzakende organisatie (zowel bedrijven als overheden) en hiervan binnen 72 uur een melding te doen bij de Autoriteit Persoonsgegevens (AP). Eenieder die een datalek veroorzaakt, of vermoedt, moet hiervan melding maken. Na het doen van de melding moet direct (telefonisch/email) de teammanager, maar ook privacy officer direct geïnformeerd worden (deze informeert de AP). Het proces omtrent de afhandeling van datalekken is vastgelegd en opgenomen in het maatregelenoverzicht van hoofdstuk 6.

5.4 Wijzigingen

Wijzigingen op de ICT-infrastructuur zijn onderhevig aan risico's. Autorisaties, of invoeren of inhoudelijke wijzigen van informatiesystemen, maar ook bijvoorbeeld het verhelpen van kwetsbaarheden en technische of functionele updates en zelfs uit faseren van systemen kunnen grote gevolgen hebben. Om die reden moeten alle aanvragen van wijzigingen aangevraagd worden via het selfservicesysteem. Hierna moeten deze geautoriseerd worden door de informatiesysteem eigenaar en via het proces wijzigingenbeheer verwerkt

worden. In principe kan iedereen een wijziging aanvragen. De exacte procedure Het proces wijzigingenbeheer is vastgelegd en opgenomen in het maatregelenoverzicht van hoofdstuk 6.

5.5 Kwetsbaarhedenbeheer

Met kwetsbaarheidsbeheer of Patchmanagement worden softwareproblemen en verkeerde configuraties geïdentificeerd en wordt de juiste prioritijd hieraan toegekend om deze problemen te verhelpen. Cybercriminelen, dus aanvallers gebruiken (bekende) problemen om misbruik te maken van gevoelige gegevens en/of bedrijfsactiviteiten te verstoren. De taak voor het uitvoeren van kwetsbaarheden beheer is belegd bij het Team I&ID. Het proces kwetsbaarhedenbeheer is vastgelegd en opgenomen in het maatregelenoverzicht van hoofdstuk 6.

5.6 Dataclassificatie

Het toekennen van classificatieniveaus aan data en/of informatiesystemen is van groot belang, omdat daarmee het (vereiste) beveiligingsniveau toegepast kan worden. Aan de hand hiervan kan worden bepaald welke beveiligingseisen gelden en welke maatregelen moeten worden genomen. De classificatie dient door of namens de eigenaar van het betreffende informatiesysteem te worden uitgevoerd en bepaald. Bij de uitvoering van het classificatieproces wordt de eigenaar ondersteund door de Chief Information Security Officer (CISO), de Functionaris voor de Gegevensbescherming (FG), functioneel beheerder of applicatiebeheerder, business consultant en technisch beheerder. Het proces dataclassificatie is vastgelegd en opgenomen in het maatregelenoverzicht van hoofdstuk 6.

5.7 Autorisatie

Het toekennen, bijstellen, intrekken maar ook controleren van autorisaties is een verantwoordelijkheid die enkel en alleen ligt bij de eigenaar van een informatiesysteem, of een gemandateerd functionaris en wordt altijd schriftelijk of digitaal vastgelegd. Het proces omtrent autorisatiebeheer is vastgelegd en opgenomen in het maatregelenoverzicht van hoofdstuk 6.

6. Informatiebeveiliging Maatregelen

Vanuit de BIO, maar ook gesteld door toezichthouders van rijk gerelateerde informatiesystemen zijn een groot aantal (verplichte) maatregelen van kracht. Een overzicht van alle maatregelen is hieronder opgenomen

Noot: Deze pagina is een inlegblad, alle maatregelen maken deel uit van dit informatiebeveiligingsbeleid. Maar de maatregelen moeten soms tussentijds worden bijgesteld, bijvoorbeeld als gevolg van gewijzigde wet-, regelgeving of normering

Maatregel	Omschrijving	Versie	Datum	Eigenaar
1	Business Continuïteit Beleid			GS/DIR
2	Crisisplan en & Crisisbeheer			GS/DIR
3	Screenings beleid	2.0	08-03-2023	HR
4	Huisregels / Fair Use Beleid	Personeelshandboek		HR
5	Toegangsbeleid			I&ID
6	Clear desk / Clear Screen Beleid	1.0	08-02-2023	I&ID
7	Wachtwoord Beleid	2.0	08-03-2023	I&ID
8	Privacy Beleid	1.0	25-02-2020	PO/FG
9	Crypto beleid	1.1	08-02-2023	I&ID
10	Malware Beleid	1.1concept	01-07-2022	I&ID
11	Backup Beleid			I&ID
12	Dataclassificatie Beleid			TM
13	Web Applicatiebeheer			I&ID
14	Kwetsbaarhedenbeheer			I&ID
15	Incidentbeheer	Concept		I&ID
16	Wijzigingen Beheer	28	17-04-2023	I&ID
17	Audit & Controleplan			CC
18	Procedure datalekken	?	18-08-2022	PO/FG
19	Procedure Beveiligingsincidenten			CISO
20	Contactoverzicht en Mandaat	Concept	07-11-2022	GS/DIR
21	Suwinet Beleid en Regelgeving	1.0	12-08-2021	VIC
22	WPG Beleid en Regelgeving			TM
23	Thuis of Telewerken Beleid			HR/I&ID
24	Risico Inventarisatie & Evaluatie			GS
25	Uitvoeringsplan informatiebeveiliging			GS
26	Mobiele Apparaten Beleid			I&ID
27	Web Applicatie Beleid			I&ID
28	Monitoring & Response Beleid			I&ID
29	ISMS			CISO

Laatste stand datum dd 01-07-2023
Vastgesteld door :

Gemeente Secretaris
Sander Kastelein

7. Communicatie & Overleg

7.1 Directie overleg

Op directieniveau wordt jaarlijks beoordeeld of het noodzakelijk is het informatiebeveiligingsbeleid bij te stellen. De basis hiervoor is de jaarlijkse risico-inventarisatie inzake informatieveiligheid, die in December van elk jaar opgesteld wordt door de CISO.

Deelnemers: GS, Directeur, CIO, CISO en FG

7.2 Managementoverleg informatiebeveiliging

Op managementniveau wordt minimaal twee keer per jaar een intern overleg informatiebeveiliging gecombineerd met de standaardmanagement overlegvergaderingen (MO). Het initiatief, qua tijdstip en onderwerpen ligt in principe bij de CISO, maar kan natuurlijk ook bij de teammanager zelf liggen.

Deelnemers: CISO, CIO, Teammanagers

7.3 Generiek overleg informatiebeveiliging

Op uitvoerend niveau wordt minimaal vier keer per jaar een intern overleg informatiebeveiliging georganiseerd. De CISO is voorzitter van het overleg. Bij dit overleg zijn aanwezig:

Deelnemers: CISO, PO/SO, FG, IA/IM, CC, CIP (namens de TM)

7.4 Overleg informatiebeveiliging en Privacy

Maandelijks overleggen de CISO, de FG en de Privacy Officer over tactische en operationele zaken. Regelmatig zal ook de Concern Controller hier op uitnodiging aan deelnemen, indien dit nodig is.

Deelnemers: CISO, PO/SO, FG

8. Rapportages & Verantwoording

8.1 Interne rapportage

Interne rapportages zijn een vereiste (mede vanuit de BIO) om het informatiebeleid tijdig te kunnen bijsturen. Binnen de gemeente Meppel moeten de volgende functionarissen, per kwartaal rapporteren;

- Teammanager, over awareness, autorisatiecontroles en problemen
- CISO, omtrent uitvoering jaarplan informatiebeveiliging
- Privacy Officer, datalekken en afhandeling
- FG, inzake uitgevoerde controles en gedane verbetervorstellen.

Bijlage 1 geeft een voorbeeld van een voor nu handmatige, teamrapportage. Uiteindelijk moet dit soort rapportages automatisch deel uitmaken van een overall Governance Risk en Compliancy (GRC) systeem voor Meppel. Een GRC-systeem is een systeem van geautomatiseerde maatregelen en procedures die organisaties gebruiken om hun belangrijkste risico's te beheersen en om zo te voldoen aan wet- en regelgeving. Het Information Security Management Systeem(ISMS) deel binnen zo een systeem, voorziet, mits op een juiste manier gebruikt, over automatische rapportages op het gebied van informatiebeveiliging.

8.2 Verantwoording ENSIA

De gemeente Meppel verantwoordt zich jaarlijks over de informatiebeveiliging middels de ENSIA-systematiek. De ENSIA-coördinator zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke teammanagers of bij de hiervoor aangewezen medewerkers van het ENSIA-team. De rol van ENSIA-coördinator is schriftelijk vastgelegd bij de ENSIA-organisatie van de VNG.

8.3 Verantwoording WPG

Eens in de vier jaar moeten werkgevers van buitengewoon opsporingsambtenaren (boa's) een externe audit uit laten voeren. Dit staat in de nieuwe Wet politiegegevens (WPG) die sinds 1 mei 2022 van kracht is. Aan de externe audit gaat altijd een interne audit vooraf. Deze dient één keer jaar te worden gedaan en is binnen Meppel tevens belegd bij de CISO/VIC.

8.4 Verantwoording aan de Raad

Jaarlijkse rapportage over informatiebeveiliging is opgenomen in de paragraaf bedrijfsvoering van jaarverslag van de gemeente Meppel.

8.5 Bijstelling van dit Beleid

Dit maakt deel uit van de jaarlijkse PDCA-cyclus van de gemeente Meppel.

9. Vaststelling beleid

Dit informatiebeveiligingsbeleid is vastgesteld, met terugwerkende kracht vanaf 01-01-2023, door de burgemeester en wethouders van de gemeente Meppel.

Gemeentesecretaris Meppel	Burgemeester Meppel
Sander Kastelein	R.T.A Korteland

Bijlage 1: Rapportage onderwerpen Informatiebeveiliging & Privacy / Team

Aspect	Onderwerp	Interval	Controledatum	Status	Bijzonderheden /actie
1	Constatering van Datalekken	Kwartaal, PRIO 1 direct			
2	Constatering van Veiligheidsincidenten	Kwartaal, PRIO 1 direct			
3	Risico-Inventarisatie IB & P Team	Jaarlijks			
4	Controle Team continuïteit plan	Jaarlijks			
5	Controle IB &P Bewustzijn	Kwartaal			
6	Controle van autorisatie Team medewerkers	Jaarlijks			
7	Controle van autorisatie Team systemen	Kwartaal			
8	Controle autorisaties uitgestroomde medewerkers	Maandelijks			

Team: uitgevoerd door: datum:

Bijlage 2: Lijst van Afkortingen en begrippen

Afkorting of Begrip	Betekenis
IB&P	Informatiebeveiliging en Privacy (begrip)
BIO	Baseline Informatiebeveiliging Overheid (Richtlijn)
NIB2/NIS2	EU Netwerk- en Informatiebeveiligingsrichtlijn
AVG	Algemeen Verordening Gegevensbescherming (Wet)
WPG	Wet Politiegegevens
CC	Concern Controller (Functie)
TM	Teammanager (Functie)
CIP	Contactpersoon Informatiebeveiliging & Privacy (Functie)
PO	Privacy Functionaris (Privacy Officer)
CISO	Hoofd informatiebeveiliging (Chief Information Security Officer)
FG	Functionaris Gegevensbescherming
IA	Informatie Architect (Functie of taak)
IM	Informatiemanager (Functie of taak)
FB	Functioneel Beheer (Functie of taak)
AB	Applicatiebeheer (Functie of taak)
SB	Systeembeheer (Functie of taak)
BIV	Beschikbaarheid, Integriteit, Vertrouwelijkheid (begrip)
ISO	International Standard Organisation (Entiteit)
ISO27001	Informatiebeveiliging Norm (ISMS)
ISO27002	Beheersmaatregelen Informatiebeveiliging (Norm)
ISO9001	Kwaliteit Management Systeem
Dataclassificatie	Vasstellen van het beveiligingsniveau (process)
ITIL	Information Technology Infrastructure Library (Best Practice)
NEN	Nederlandse Norm (afkorting)
ENSIA	Eenduidige Normatiek Single Information Audit (afkorting)
BRP	Basis Registratie Personen (Systeem)
DigiD	Digitale Identiteit (Systeem)
SUWINET	Sociale Uitkeringen, Werk en Inkomen Netwerk
BCP	Bedrijf Continuïteit Plan (Afkorting)
I&ID	(Team) Informatie & Interne dienstverlening
ICT	Informatie en Communicatie Technologie
SLA	Service Level Overeenkomst of Dienst Niveau overeenkomst
ESCROW	Angelsaksische term voor broncodedeponering
TPM	Third party Mededeling, vaak of auditrapport van een systeem
DPIA	Data Protection Impact Assessment
GIBIT	Gemeentelijke Inkoopvoorwaarden bij IT
RI&E	Risico Inventarisatie & Evaluatie
CAB	Change advisory Board (Wijziging advies commissie)
IT	Informatie Technology
ISMS	Information Security Management Systeem
GRC	Governance Risk & Control
PFO	Portefeuille Overleg
OOV	Openbare Orde en Veiligheid