



Strategisch Informatiebeveiliging & Privacy beleid (IB&P Beleid) Gemeente Meppel 2026-2029

Geldig vanaf 01-01-2026

Definitief, op 02 juni 2026 vastgesteld door College B&W Meppel



Inhoudsopgave

Versiebeheer	3
Bijlagen.....	3
Voorwoord	4
1. Algemeen.....	5
1.1. Inleiding	5
1.2 Leeswijzer.....	5
1.3 Ambitie, visie en missie informatiebeveiliging en privacy.....	5
1.4 Privacy en Gegevensbescherming.....	6
1.5 Risicomanagement.....	7
1.6 Pas-toe-of-leg-uit.....	9
1.6 Aansluiting bij wet- en regelgeving.....	9
1.8 Continu verbeteren (PDCA)	10
2. Doelen en uitgangspunten	12
2.1 Inleiding	12
2.2 Strategische doelen.....	12
2.3 Koers	13
2.4 Standaarden informatiebeveiliging	13
2.5 Kaders	14
2.6 Plaats strategisch informatiebeveiliging en privacy beleid	15
2.7 Reikwijdte Informatiebeveiliging en Privacy	15
2.8 Herziening	16
2.9 Werkwijze	16
3. Organisatie, Taken & Verantwoordelijkheden	18
3.1 Governance	18
3.2 Gemeenteraad (Toezicht en kaderstelling)	18
3.4 Directie (Aansturing ambtelijke organisatie).....	20
3.5 Chief Information Officer.....	20
3.5 Teammanagers (Uitvoering, eigenaarschap en afstemming)	21
3.6 De tweede en derde lijn rollen: Controle en verantwoording	22
3.7 Medewerker.....	25
4. Communicatie & Overleg.....	28
Bijlage A: De 10 bestuurlijke principes voor informatiebeveiliging (VNG).....	29
Bijlage B Afkortingen en Begrippenlijst.....	35
Bijlage C: Overzicht van Wet en regelgeving	38



Versiebeheer

Versie	Datum	Door	Wijzigingen
0.3	01-12-2025	CISO	Aanpassingen op eerdere versies doorgevoerd, en voor 2026 -> gebaseerd op de template Strategisch Informatiebeveiliging- en privacy beleid van de VNG
0.4	04-12-2025	CISO	Verbeterpunten van I&ID doorgevoerd, + kleine wijziging in volgorde paragrafen
0.5	07-04-2026	CISO	Tekstuele verbeterpunten doorgevoerd
0.99	23-04-2026	CISO	Verbeterpunten vanuit CIO doorgevoerd

Bijlagen

- Bijlage A De 10 bestuurlijke principes voor informatiebeveiliging (VNG)
- Bijlage B Afkortingen en Begrippenlijst
- Bijlage C Overzicht van Wet en regelgeving
- Bijlage D Grafisch Overzicht (ter indicatie) van tactische documenten



Voorwoord

Het is van groot belang dat inwoners en ondernemers kunnen rekenen op betrouwbare en veilige dienstverlening. Of het nu gaat om een paspoort, een vergunning of ondersteuning bij zorg: achter al deze processen schuilt veel informatie van en over inwoners. Die informatie moet niet alleen beschikbaar zijn, maar vooral goed beschermd worden.

Digitale veiligheid is geen eenmalige inspanning, maar een continu proces. Wetgeving verandert, dreigingen nemen toe en technologie ontwikkelt zich razendsnel. Daarom passen wij ons beleid voortdurend aan. Met dit strategisch informatiebeveiligings- en privacybeleid laten we zien dat we veiligheid en privacy structureel en serieus borgen. We doen er alles aan om risico's te beheersen, incidenten te voorkomen en als er toch een incident plaatsvindt, de gevolgen tot een minimum te beperken.

Onze inzet gaat verder dan voldoen aan wettelijke verplichtingen. Het raakt aan vertrouwen, want als inwoner of ondernemer moeten je erop kunnen rekenen dat jouw gegevens bij ons in veilige handen zijn. Dat vertrouwen is de basis voor goede dienstverlening. Daarom investeren we in digitale weerbaarheid, duidelijke afspraken en een cultuur waarin iedereen zich bewust is van zijn verantwoordelijkheid.

Met dit bijgestelde beleid laat Meppel zien dat informatiebeveiliging en privacy blijvend aandacht krijgt. We blijven leren, verbeteren en anticiperen op nieuwe ontwikkelingen, zodat we samen zorgen voor een veilige en betrouwbare gemeente.

Arjen Maathuis

Burgemeester



1. Algemeen

1.1. Inleiding

Dit document beschrijft het strategisch informatiebeveiligings- en privacy beleid (IB&P-beleid) van de gemeente Meppel vanaf 2026 en presenteert een geactualiseerde versie van het in 2023 vastgestelde beleid. Dit beleid is gebaseerd op de gemeentelijke taken en doelstellingen en vormt het fundament voor de bescherming van diensten, informatie en privacy. Deze verbeterde versie volgt uit nieuwe en bijgestelde wettelijke kaders en richtlijnen, waaronder de Cyberbeveiligingswet (Cbw), de Baseline Informatiebeveiliging Overheid 2.0 (BIO2).

Dit beleid is richtinggevend voor alle informatiebeveiligings- en privacy activiteiten en wordt aangevuld met onderwerp specifieke beleidsdocumenten op tactisch niveau of procedures en standaarden op operationeel niveau. De gehanteerde uitgangspunten zijn gebaseerd op de tien bestuurlijke principes voor informatiebeveiliging van de VNG en de beginselen uit de AVG voor de verwerking van persoonsgegevens. Door de continue verbetering en implementatie van dit beleid en de actualisatie van onderliggende documenten wordt de digitale weerbaarheid van de gemeente duurzaam geborgd.

1.2 Leeswijzer

Dit strategisch informatiebeveiligings- en privacy beleid van de gemeente Meppel is opgebouwd uit vier hoofdstukken en diverse bijlagen die samen het kader vormen voor de periode 2026–2029. Het voorwoord benadrukt het belang van vertrouwen en betrouwbare dienstverlening. Hoofdstuk 1 schetst de algemene uitgangspunten, waaronder ambitie, visie, missie, privacy, risicomanagement en aansluiting op wet- en regelgeving. Hoofdstuk 2 beschrijft de strategische doelen, kaders en standaarden, de plaats van dit beleid binnen de organisatie en de werkwijze voor herziening en communicatie. Hoofdstuk 3 gaat in op Governance en de verdeling van taken en verantwoordelijkheden tussen raad, college, directie, teammanagers en medewerkers. Hoofdstuk 4 behandelt de overlegstructuur en communicatie. De bijlagen bieden verdieping: bestuurlijke principes, begrippenlijst, overzicht van wet- en regelgeving, detailuitwerking van strategische doelen en een grafisch overzicht van onderliggende tactische documenten.

1.3 Ambitie, visie en missie informatiebeveiliging en privacy

De gemeente verwerkt dagelijks privacygevoelige gegevens van inwoners, organisaties en andere partijen. Zij moeten erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze gegevens omgaat. Onvoldoende aandacht voor risico's, rechtmatigheid en ethiek kan tot aanzienlijke schade leiden voor inwoners, politiek, reputatie, financiën en personeel,



maar ook bedrijven kunnen direct de gevolgen ondervinden van ons handelen of nalaten. Dreigingen zoals cybercriminaliteit, geopolitieke spanningen, menselijke fouten, falende technologie en een sterke afhankelijkheid van derde partijen voor digitale dienstverlening maken het noodzakelijk dat wij voorbereid en weerbaar zijn. Deze weerbaarheid omvat niet alleen de bescherming van gegevens, maar ook het structureel waarborgen van de continuïteit van onze dienstverlening. Daarmee draagt de gemeente Meppel bij aan de bredere weerbaarheidsopgave van de overheid: het onder alle omstandigheden kunnen blijven uitvoeren van publieke taken en het behouden van vertrouwen van inwoners, organisaties en partners.

- Ambitie: De gemeente streeft naar een digitaal veilige en weerbare organisatie die het vertrouwen van inwoners, organisaties en partners waarborgt. Deze ambitie wordt gerealiseerd door aantoonbaar te werken volgens de principes en eisen van ISO 27001, waarbij informatiebeveiliging en privacy systematisch, risico gestuurd en controleerbaar wordt ingericht binnen een aantoonbaar werkend managementsysteem.
- Visie: Zoals ook weergegeven in het programma [Koers in actie](#), streeft de gemeente naar betrouwbare en transparante (digitale) dienstverlening, waarbij informatiebeveiliging en privacy structureel en integraal zijn ingebed in alle processen. Door risico's proactief te beheersen, bewustwording te vergroten en te voldoen aan wet- en regelgeving, wordt digitale veiligheid een vanzelfsprekend onderdeel van verantwoord en toekomstgericht werken.
- Missie: De gemeente beschermt privacy en informatieveiligheid door zorgvuldig, veilig en verantwoord met informatie om te gaan. Wij stimuleren medewerkers tot verantwoord handelen en voorbeeldgedrag, waarmee de privacy en informatieveiligheid in gemeentelijke processen wordt gegarandeerd.

1.4 Privacy en Gegevensbescherming

De gemeente werkt met (persoons)gegevens van inwoners, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt de gemeente voor het goed kunnen uitvoeren van de gemeentelijke wettelijke taken en om een efficiënte en effectieve bedrijfsvoering te voeren. Denk hierbij onder andere aan taken in het sociaal domein, openbare orde en veiligheid of voor burgerzaken. Om als gemeente deze taken uit te voeren is de verwerking van persoonsgegevens noodzakelijk.

Bij de omgang met persoonsgegevens van inwoners en personeel hebben gemeenten een grote verantwoordelijkheid. Privacy is een wezenlijk en uitdagend vraagstuk. De complexiteit ervan wordt versterkt door de toenemende digitalisering van samenleving en gemeentelijke dienstverlening, de decentralisatie van overheidstaken, de intensieve gegevensuitwisseling met (keten)partners, de snelle technologische ontwikkelingen en voortdurend veranderende wetgeving. Privacy raakt daarom de hele gemeentelijke organisatie en verdient, samen met



informatiebeveiliging, continu aandacht. De inwoner moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met haar persoonsgegevens omgaat.

De gemeente sluit aan bij de privacy-aanpak van de Informatiebeveiligingsdienst (IBD) van de Vereniging van Nederlandse Gemeenten (VNG). Door hierbij aan te sluiten kan de gemeente gebruikmaken van de door de IBD gedeelde risicoanalyses voor gegevensbescherming. Deze risicoanalyses zijn in vaktermen bekend als de Data Protection Impact Assessment (DPIA). Ook Meppel deelt haar eigen DPIA's met de IBD. Zo versterken we gezamenlijk de kennisbasis en de bescherming van (persoons)gegevens.

1.5 Risicomanagement

Risicomanagement is het belangrijkste uitgangspunt binnen het gemeentelijke beleid voor Informatiebeveiliging en Privacy. en is belangrijk voor een evenwichtige afweging te maken tussen beveiliging, gebruiksgemak en doelmatigheid. Een volledig dichtgetimmerde informatievoorziening is niet wenselijk; het streven is een passende beveiliging gebaseerd op de aard en omvang van risico's

Binnen dit beleid wordt uitgegaan van een systematische en herhaalbare aanpak voor het identificeren, analyseren, beoordelen en behandelen van risico's die de Beschikbaarheid, Integriteit en Vertrouwelijkheid van informatie kunnen beïnvloeden. Deze aanpak sluit aan bij de landelijk hiervoor geaccepteerde norm en voldoet daarmee aan de verplichtingen die voortvloeien uit relevante wet- en regelgeving, waaronder de Cbw en de BIO2.

1.5.1 Kaders voor risicomanagement

Het risicomanagement binnen informatiebeveiliging en privacy omvat in ieder geval het:

- Structureel in kaart brengen en beoordelen van risico's bij nieuwe of gewijzigde processen, systemen en gegevensverwerkingen.
- Uitvoeren van een Data Protection Impact Assessment (DPIA) wanneer sprake is van verwerkingen van persoonsgegevens met een verhoogd privacy risico.
- Afstemmen van beveiligingsmaatregelen op de aard en omvang van de geïdentificeerde risico's, waarbij kritieke informatie en systemen prioriteit krijgen.
- Toepassen van een vastgestelde risicomanagementmethodiek die zorgt voor consistentie en herhaalbaarheid.
- Centraal vastleggen en periodiek actualiseren van risico's, incidenten en getroffen maatregelen om de betrouwbaarheid en actualiteit van informatie te waarborgen.

1.5.2 Beleidsuitgangspunten voor risicomanagement

Op basis hiervan gelden de volgende uitgangspunten:

- Beveiligingsmaatregelen worden afgestemd op de risico's die de organisatie loopt.
- Risico's worden structureel, herhaalbaar en aantoonbaar in kaart gebracht en beoordeeld.



- DPIA's worden uitgevoerd wanneer de verwerking een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen.
- Risico's, incidenten en maatregelen worden centraal geregistreerd en periodiek geactualiseerd.
- Risicomanagement is een continu proces dat gericht is op voortdurende verbetering van informatiebeveiliging en privacybescherming.

1.5.3 ISO/IEC 27005 – Risicomanagement voor informatiebeveiliging als methodiek voor risicomanagement op het gebied van IB&P binnen Meppel

De jaarlijkse rechtmatigheidsverklaring (RMV) vereist dat de gemeente beschikt over een aantoonbaar en consistent ingericht risicomanagementproces, waaronder het risicomanagement voor informatiebeveiliging en privacy. Risicomanagement vormt daarmee een structureel onderdeel van de gemeentelijke sturing en verantwoording. De gemeente hanteert hiervoor als basis een generieke risicomanagementmethodiek, deze basismethodiek is vastgelegd in de Nota Risicomanagement.

Voor risicomanagement gericht op Informatiebeveiliging en Privacy sluit de gemeente qua werkwijze aan bij de internationale normen ISO/IEC 27005. De ISO/IEC 27005 norm is het belangrijkste kader voor het systematisch identificeren, analyseren en behandelen van risico's die de beschikbaarheid, integriteit en vertrouwelijkheid van informatie kunnen aantasten.

De ISO/IEC 27005 schrijft geen vaste set risico's voor, maar biedt een raamwerk waarmee organisaties op een systematische en herhaalbare wijze alle relevante risico's voor informatiebeveiliging kunnen identificeren, analyseren en beoordelen. Vanuit een generiek strategisch perspectief toetst de gemeente daarom ten minste de belangrijkste risicodomeinen die de beschikbaarheid, integriteit en vertrouwelijkheid van informatie kunnen beïnvloeden. Deze strategische risicocategorieën vormen de basis voor het bepalen van proportionele beveiligingsmaatregelen en voor het borgen van een consistent en aantoonbaar risicobeheer binnen informatiebeveiliging en privacy.

De strategische te beoordelen risicocategorieën omvatten in ieder geval:

1.5.3.1 Beschikbaarheid

- Uitval of verstoring van kritieke systemen en infrastructuur.
- Afhankelijkheid van leveranciers, clouddiensten en ketenpartners.
- Ontoereikende continuïteits- en herstelvoorzieningen.

1.5.3.2. Integriteit

- Ongeautoriseerde of onbedoelde wijziging van gegevens.
- Fouten in geautomatiseerde processen of gegevensverwerking.
- Manipulatie of vervalsing van informatie.

1.5.3.3. Vertrouwelijkheid



- Ongeautoriseerde toegang tot persoonsgegevens of vertrouwelijke informatie.
- Datalekken door menselijk handelen, technische tekortkomingen of externe aanvallen.
- Onvoldoende toegangsbeveiliging of segmentatie.

1.5.3.4. Externe dreigingen

- Cyberaanvallen zoals Phishing, Ransomware en DDoS.
- Verstoringen door geopolitieke of maatschappelijke ontwikkelingen.
- Kwetsbaarheden in de keten of bij leveranciers.

1.5.3.5. Organisatorische en procesmatige factoren

- Ontoereikend beleid, procedures of naleving.
- Onvoldoende bewustwording en veilig gedrag.
- Gebrekkige monitoring, logging en rapportage.

1.5.3.6. Technologische ontwikkelingen

- Verouderde systemen zijn kwetsbaar.
- Risico's door nieuwe technologieën zoals AI, IoT of Cloud-oplossingen.
- Kwetsbaarheden in software, hardware of configuraties.

1.5.3.7. Privacy en gegevensbescherming

- Verwerkingen met verhoogde privacy risico's.
- Onvoldoende waarborgen voor rechtmatigheid, transparantie en dataminimalisatie.
- Risico's die aanleiding geven tot een DPIA.

1.6 Pas-toe-of-leg-uit

De gemeente hanteert de verplichte standaarden voor informatiebeveiliging, zoals vastgelegd in de BIO2 en de daarbij van toepassing zijnde normen. De BIO2 beschrijft hoe organisaties hun informatie veilig en betrouwbaar moeten beheren. Afwijkingen zijn alleen toegestaan als uit de vastgelegde risicobeoordeling blijkt dat maatregelen niet noodzakelijk zijn of geaccepteerd worden ('pas toe of leg uit').

1.6 Aansluiting bij wet- en regelgeving

Dit beleid sluit aan bij de AVG en andere relevante wet- en regelgeving op het gebied van informatiebeveiliging en privacy. De BIO2 vormt het uniforme basisnormenkader voor informatiebeveiliging binnen de overheid, waarin een risicogestuurde aanpak centraal staat. Daarnaast is de Europese NIS2-richtlijn van toepassing, die organisaties verplicht tot het versterken van hun digitale weerbaarheid, het treffen van passende beveiligingsmaatregelen en het melden van significante cyberincidenten. De Nederlandse implementatie van deze richtlijn is vastgelegd in de Cyberbeveiligingswet (CBW), waarmee de BIO2 een wettelijke verplichting wordt voor overheidsorganisaties. Uit een nog te publiceren onderzoek van de

Rekenkamer de basis op orde heeft en dat het belang van informatiebeveiliging & Privacy breed wordt onderkend binnen de organisatie. Waar processen of gegevensverwerkingen onder sectorspecifieke wetgeving vallen, zoals de Wet politiegegevens (Wpg), worden aanvullend de specifieke beveiligingsvereisten uit deze wet toegepast. Hiermee sluit dit beleid volledig aan op het geldende normatieve en wettelijke kader voor informatiebeveiliging en privacy.

1.7 Samenwerking en Standaardisering

De gemeente Meppel sluit waar mogelijk aan bij de landelijke initiatieven van de Vereniging van Nederlandse Gemeenten (VNG) gericht op gezamenlijke inkoop, uitvoering en standaardisering binnen het domein van informatiebeveiliging en digitale weerbaarheid. Door aan te sluiten bij deze gezamenlijke aanpak kan Meppel profiteren van schaalvoordelen, kwaliteitsverbetering en actuele landelijke kennisontwikkeling. Daarnaast staat de gemeente open voor samenwerking in de uitvoering met andere overheidsorganisaties en, waar dit toegevoegde waarde biedt, met publiek-private partners. Deze samenwerkingsvormen dragen bij aan een toekomstbestendige, kostenefficiënte en professionele inrichting van onze informatiebeveiliging.

1.8 Continu verbeteren (PDCA)

Informatiebeveiliging en privacy binnen de gemeente Meppel wordt ingericht en beheerd volgens de PDCA-cyclus (plannen, uitvoeren, controleren en bijstellen). Deze cyclus vormt de basis voor het Information Security Management System (ISMS), waarmee de gemeente de beveiliging van informatie structureel, aantoonbaar en risico gestuurd organiseert.



Binnen het ISMS wordt het strategisch informatiebeveiligingsbeleid vertaald naar tactisch en operationeel beleid. Jaarlijks wordt het tactische en operationele beleid geactualiseerd in de vorm van een informatiebeveiligingsplan. Deze actualisatie is gebaseerd op dit strategisch beleid, de jaarlijkse uitkomsten van de ENSIA-verantwoording, overige relevante audits en het actuele dreigingsbeeld voor gemeenten in combinatie met periodieke risicoanalyses. Deze bronnen vormen aanvullende input voor de PDCA-cyclus van het ISMS, waarin de structurele bijstelling van beleid, maatregelen en processen daarmee wordt geborgd.

Het ISMS omvat ook een periodieke herijking van het strategisch informatiebeveiliging en privacy beleid. Maar aanpassing van dit beleid vindt alleen plaats wanneer ontwikkelingen in wet- en regelgeving, technologische veranderingen, nieuwe risico's of structurele bevindingen uit audits en ENSIA daartoe aanleiding geven. Hiermee wordt geborgd dat het strategisch beleid actueel blijft en aansluit op de gemeentelijke opgaven en risico's.



Binnen de PDCA-cyclus worden vaste rapportagemomenten gehanteerd op strategisch, tactisch en operationeel niveau. Strategisch wordt jaarlijks gerapporteerd over de voortgang, risico's en noodzakelijke beleidsaanpassingen. Tactisch wordt periodiek gerapporteerd over de uitvoering van het informatiebeveiligingsplan en de voortgang van verbetermaatregelen. Operationeel wordt structureel inzicht gegeven in incidenten, risico's en de status van beheersmaatregelen. Hiermee wordt geborgd dat het ISMS continu wordt verbeterd en aantoonbaar aansluit op de gemeentelijke planning- en control cyclus.



2. Doelen en uitgangspunten

2.1 Inleiding

Dit document heeft tot doel het Strategisch Informatiebeveiligings- en Privacy kader voor de jaren 2026–2029 vast te leggen en daarmee de borging van IB&P binnen de gemeente Meppel te verzekeren. De uitwerking van dit beleid in concrete maatregelen en activiteiten vindt plaats in het jaarlijks bij te stellen Informatiebeveiligings- en privacy plan (IB&P-Plan). Dit IB&P beleid geeft richting en biedt ondersteuning aan alle lagen van de organisatie bij het plannen, uitvoeren, beheren en controleren van informatieveiligheid en privacy.

2.2 Strategische doelen

Om richting te geven aan de informatiebeveiliging en privacy binnen de gemeente zijn en viertal strategische hoofddoelen geformuleerd:

- Het zorg dragen voor de beschikbaarheid, integriteit en vertrouwelijkheid van onze informatievoorziening, omdat deze aspecten essentieel zijn voor de continuïteit van onze dienstverlening.
- Het beschermen van onze bedrijfsmiddelen en beheerde (persoons)gegevens tegen onrechtmatige toegang, misbruik en/of manipulatie;
- Het managen van de informatiebeveiliging(risico's), het minimaliseren van (cyber)risico's en het verhogen van de weerbaarheid daartegen;
- Het adequaat kunnen reageren op cyberincidenten en zo snel als mogelijk voorkomen of beperken van schade.

We realiseren deze doelen door risico gestuurd te werken, zoals uitgewerkt in het risicomanagementkader, beschreven in paragraaf 1.5. informatie- of proceseigenaren geven hieraan invulling door risico's structureel te identificeren, te beoordelen en te behandelen binnen hun processen en gegevensverwerkingen. Zij passen privacy--by--design toe, laten waar nodig risicoanalyses uitvoeren en dragen er zorg voor dat risico's, incidenten en maatregelen centraal worden vastgelegd en geactualiseerd. De PDCA-cyclus binnen het Informatie Security Management Systeem (ISMS)-cyclus ondersteunt dit proces en maakt de voortgang aantoonbaar. De gemeente monitort hiermee de uitvoering en past doelen en maatregelen aan wanneer nieuwe dreigingen, risico's of wijzigingen in wet-- en regelgeving daartoe aanleiding geven.



2.3 Koers

Informatiebeveiliging en privacy zijn onlosmakelijk onderdeel van de manier waarop de gemeentelijke organisatie Meppel werkt. Ze ondersteunen onze opdracht om betrouwbaar, zorgvuldig en transparant te handelen. Door de bedoeling van het vraagstuk centraal te stellen, verwerken we gegevens van inwoners en partners op een veilige en rechtmatige manier.

Betrouwbaarheid is hierin leidend. Daarom borgen we beveiliging en privacy structureel in processen, maken we afspraken toetsbaar en handelen we volgens het principe we zeggen wat we doen, en we doen wat we zeggen. Dit vraagt om duidelijke verantwoordelijkheden en een consistente uitvoering.

Zo dragen informatiebeveiliging en privacy bij aan een voorspelbare, zorgvuldige en toekomstbestendige organisatie.

2.4 Standaarden informatiebeveiliging

Onderstaand een overzicht van de normen en kaders die richtinggevend zijn voor de inrichting van informatiebeveiliging en privacy binnen de gemeente Meppel. Het maakt zichtbaar welke standaarden per onderwerp van toepassing zijn en welke ondersteuning hiervoor beschikbaar is.

Onderwerp	Norm/Kader	Toelichting
Organisatie en organisatie op Informatiebeveiliging	NEN-EN-ISO/IEC 27001:2023	Gaat over het management van informatiebeveiliging.
Maatregelen	NEN-EN-ISO/IEC 27002:2022 + BIO2	Best practices en overheidsmaatregelen
Risicomanagement voor IB&P	NEN-EN-ISO/IEC 27005	Expliciet gericht op IB&P onderwerpen.
Operationele Technologie (OT)	IBD OT-aanpak (CSIR)	Bescherming van gebouwen, verkeer, bruggen, gemalen
Zorginformatie	NEN7510	Specifiek voor verwerking van zorggegevens
WPG	Normenkader Wpg (Ministerie van JenV)	Dit is het verplichte toetsingskader voor beveiliging van politiegegevens. Het is strenger en specifiek dan de BIO



Forum Standaardisatie	'Pas-toe-of-leg-uit-lijst'	Forum Standaardisatie adviseert de publieke sector om gebruik te maken van ICT-standaarden. De standaarden van de 'Pas toe of leg uit'-lijst zijn verplicht voor overheidsorganisaties.
Kennisproducten Informatie Beveiliging Dienst (IBD) van de VNG	Samenwerkingsaspect	Kennisproducten, handvatten of templates gericht op de BIO

2.5 Kaders

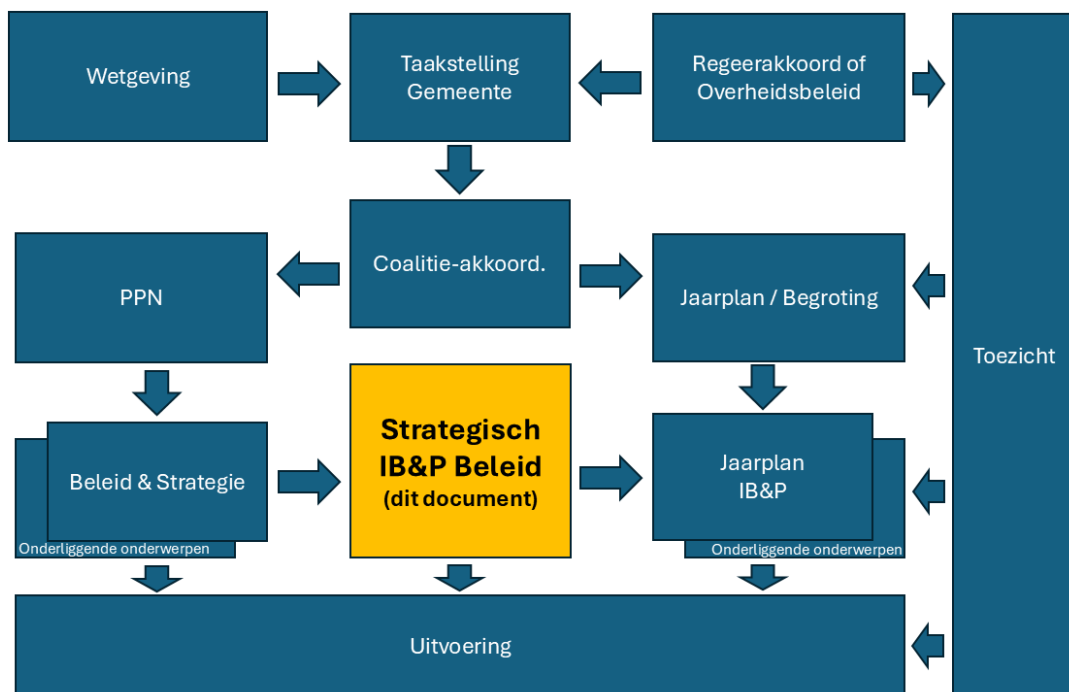
De belangrijkste kaders, wetgeving en ontwikkelingen die van belang zijn voor de handhaving en actualisering van het IB&P beleid zijn de volgende:

- De BIO2: Is een actualisatie van de BIO1.04 richtlijn en is nu een bindend normenkader met een wettelijke grondslag voor informatiebeveiliging bij de overheid. Dit kader richt zich op risicobeheersing en hanteert risicomanagement als uitgangspunt voor noodzakelijke maatregelen op basis van internationale normen.
- NIS2 en Cyberbeveiligingswet (Cbw): NIS2 is een Europese richtlijn die als doel heeft om cybersecurity binnen de EU te verhogen. De Nederlandse uitwerking van NIS2 is de Cbw. Gemeenten zijn aangewezen als essentiële entiteiten en moeten voldoen aan strenge beveiligingsnormen en meldingsvereisten ten opzichte van incidenten.
- De AVG en privacy normenkader: Nieuwe technologische ontwikkelingen en een steeds digitaler wordende overheid maken het omgaan met persoonsgegevens complexer en noodzakelijker. De gemeente wil aangeven hoe zij invulling geeft aan nationale en Europese wet- en regelgeving op het gebied van privacy.
- De Wet politiegegevens (Wpg): Binnen de gemeente verwerken BOA's gegevens die onder de Wpg vallen. De naleving van de BIO2 en de AVG vormt hiervoor de basis. Voor de specifieke Wpg-gegevens gelden aanvullende verplichtingen, zoals aanvullende maatregelen en extra toezicht op toegangsrechten, autorisaties, dataclassificatie, risico-inschatting, registratie en logging, en meld- en documentatieplicht.
- De 10 bestuurlijke principes voor informatiebeveiliging: Deze principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging in de gemeentelijke organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement en het nemen van een voorbeeldrol. De principes zijn in detail uitgeschreven in bijlage A.
- Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten: Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten geeft een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst en helpt bij het actualiseren van beleid en plannen.

- **Artificial Intelligence (AI):** De inzet van AI binnen de gemeente valt onder de Europese AI-verordening (AI Act), die vanaf 2025 gefaseerd van kracht wordt. Deze wet verbiedt toepassingen met onaanvaardbaar risico en stelt strikte eisen aan hoog-risico systemen. Daarnaast gelden de AVG en BIO2 als basis voor gegevensbescherming en informatiebeveiliging. AI mag alleen worden toegepast wanneer risico's inzichtelijk zijn en continuïteit van dienstverlening is geborgd.

2.6 Plaats strategisch informatiebeveiliging en privacy beleid

Het IB&P beleid vormt de basis voor tactische beleidsplannen en geeft richting aan de verdere invulling van informatiebeveiliging en privacy op tactisch en operationeel niveau. De uitvoering van dit beleid wordt vertaald in een plan. Dit plan is het jaarlijks bij te stellen Informatiebeveiliging- en privacy plan (IB&P-plan). De verbanden tussen de diverse documenten is weergegeven in onderstaande afbeelding.



Afbeelding 2: Positionering van het strategisch informatiebeveiligingsbeleid t.o.v. de omgeving.

Noot: In bijlage E is overzicht opgenomen van onderliggende stukken gerelateerd aan het IB&P jaarplan.

2.7 Reikwijdte Informatiebeveiliging en Privacy

De reikwijdte van dit informatiebeveiligings- en privacybeleid omvat alle gemeentelijke processen, informatiesystemen, procesautomatisering, informatie en gegevens die binnen de organisatie worden verwerkt, evenals de fysieke beveiliging van locaties, middelen en voorzieningen die nodig zijn om deze informatie te beschermen. Dit betreft zowel interne



gegevens als gegevens van externe partijen, voor zover deze onderdeel zijn van de gemeentelijke taakuitvoering. De nadruk ligt op de bescherming van informatie (vertrouwelijkheid, integriteit en beschikbaarheid) en de naleving van privacyregels waardoor kritieke gemeentelijke processen en de continuïteit van de dienstverlening worden geborgd.

2.8 Herziening

BIO2 5.01.02 schrijft het volgende voor: 'Het informatiebeveiligingsbeleid wordt minimaal jaarlijks en in aansluiting bij de (bestaande) bestuurs- en Planning & Control (P&C)-cycli en externe ontwikkelingen beoordeeld en zo nodig bijgesteld.

2.9 Werkwijze

Het bestuur, de directie en het management spelen een belangrijke rol bij de totstandkoming van dit beleid. Het management beoordeelt in eerste instantie welke onderdelen van de informatievoorziening van belang zijn voor de gemeente, welke risico's zich voordoen en welke risico's te groot zijn. De directie bewaakt de samenhang en prioritering van deze beoordelingen, vertaalt bestuurlijke kaders naar de organisatie en zorgt dat de voorgestelde maatregelen aansluiten bij de strategische koers van de gemeente. Het College van B&W beoordeelt vervolgens of de risico's en voorgestelde maatregelen aanvaardbaar zijn, zoals ook beschreven in de Cbw.

Op basis van de risicoanalyses en kaders stelt de CISO, in zijn beleidsadviesrol als behandeld ambtenaar, een voorstel voor het strategisch beleid op. Het College van B&W stelt dit beleid vast. De directie draagt zorg voor de implementatie en borging binnen de organisatie. Tactisch beleid en werkinstructies is een verantwoordelijkheid van de teams, proces of informatie-eigenaren, waarbij zij gebruikmaken van hun eigen inhoudelijke expertise maar ook van de centrale advies en ondersteuningsrollen zoals bedrijfsvoering maar ook IT, informatievoorziening, financiën, contractmanagement of juridische ondersteuning. Ook de CISO of de Privacy en Security Officer en de Functionaris Gegevensbescherming leveren hierbij richtinggevende kaders en advies. De totstandkoming van tactisch beleid en operationele werkinstructies is daarmee een gezamenlijke opgave, maar de integrale verantwoordelijkheid voor de inhoud en toepassing binnen het eigen domein ligt bij de teams zelf.

Bestuur, directie en management geven duidelijke richting aan informatiebeveiliging en privacy en laten in hun voorbeeldgedrag zien dat dit een prioriteit is. Dit vraagt niet alleen om bestuurlijke aandacht, maar ook om het vrijmaken van tijd, capaciteit en middelen. De benodigde inzet wordt uitgewerkt in de daarvoor bestemde plannen, in samenhang met de bestuurlijke ambitie die de gemeente Meppel vaststelt.

Het vrijmaken van tijd, capaciteit en middelen voor informatiebeveiliging en privacy wordt planmatig geborgd. De benodigde inzet wordt niet alleen bestuurlijk



vastgesteld, maar ook uitgewerkt in de daarvoor bestemde uitvoeringsplannen. In deze plannen wordt geconcretiseerd welke capaciteit, expertise en middelen nodig zijn om de gestelde doelen te realiseren. Voorbeelden hiervan zijn het jaarlijkse Informatiebeveiligings- en Privacy plan, het verbeterplan voor de Wpg, maar ook meer algemeen in aanbestedingen en projecten.

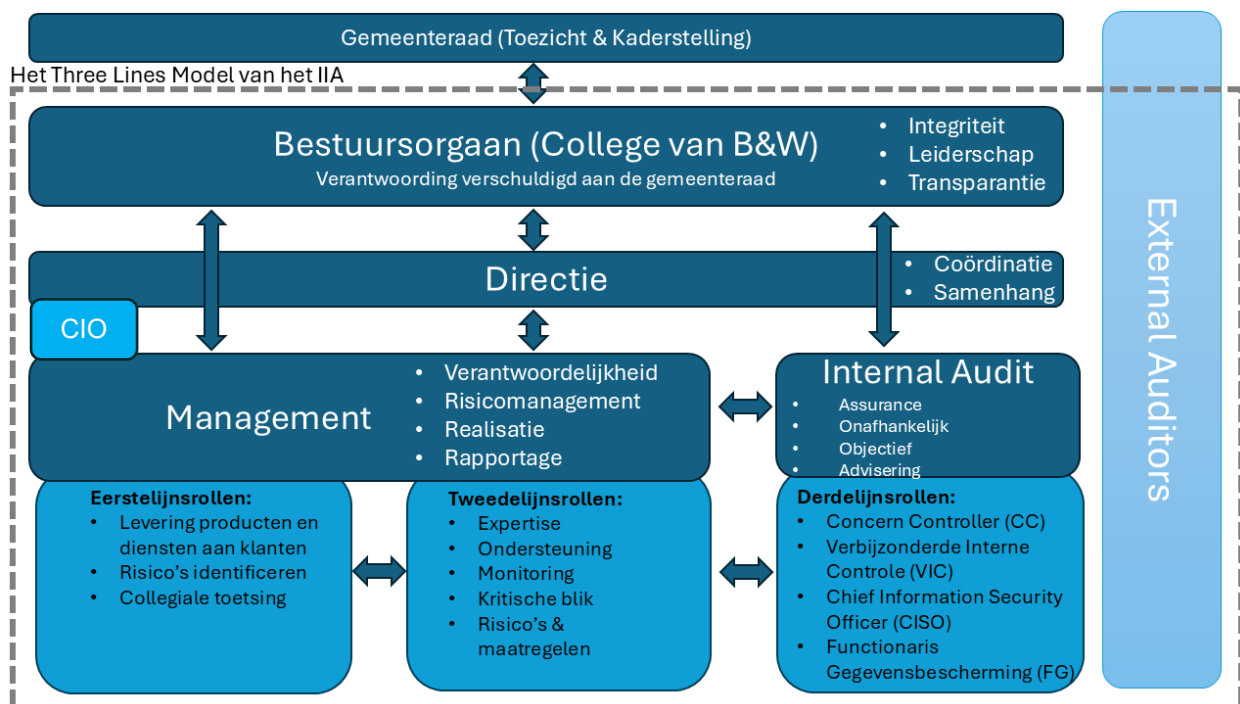
3. Organisatie, Taken & Verantwoordelijkheden

3.1 Governance

Governance vormt de basis voor goed bestuur en legt de samenhang vast tussen sturing, toezicht en borging. Het bepaalt hoe verantwoordelijkheden zijn verdeeld, hoe toezicht wordt georganiseerd en hoe dit duurzaam wordt verankerd in beleid en uitvoering.

Binnen de gemeente Meppel is de bedrijfsvoering, inclusief informatiebeveiliging en privacy, structureel ingericht op basis van het *Three Lines Model* van het Institute of Internal Auditors (IIA), eerder bekend als het *Three Lines of Defense*. Deze inrichting sluit aan bij de in 2020 door de concerncontroller geformuleerde gemeentelijke visie op control, waarin het belang van heldere verantwoordelijkheden, transparantie en een integrale benadering van risicomanagement centraal staat.

Onderstaande afbeelding toont hoe dit model binnen de gemeente Meppel is toegepast.



Afbeelding 3: Samenhang tussen sturing, toezicht en borging in Meppel.

3.2 Gemeenteraad (Toezicht en kaderstelling)

De gemeenteraad vervult de kaderstellende en controlerende rol ten aanzien van het IB&P-beleid. De raad stelt de beleidsmatige en financiële kaders vast, ziet toe op een rechtmatige en veilige uitvoering door het college en beoordeelt de verantwoording over



risico's, incidenten en naleving van wet- en regelgeving. Hiermee borgt de raad dat digitale veiligheid en privacy aansluiten bij de belangen van inwoners en dat besluitvorming transparant en uitlegbaar blijft.

3.3 College Van B&W (Bestuursorgaan)

Het College van B&W is het bestuursorgaan van de gemeente Meppel en stelt daarmee als eindverantwoordelijke dit beleid vast.

Als bestuursorgaan draagt het bestuur zorg voor de:

- **Strategische Sturing en besluitvorming:** Het bestuur stelt de strategische richting van het IB&P-beleid vast, neemt de benodigde besluiten en borgt dat het beleid aansluit bij de organisatievisie, bijdraagt aan het voorkomen van incidenten, de bescherming van informatie en persoonsgegevens, en voldoet aan alle relevante wet- en regelgeving.
- **Risicomanagement:** Het bestuur ziet erop toe dat er een adequaat risicomanagementproces op organisatieniveau is ingericht en dat de belangrijkste risico's bestuurlijk worden afgewogen en geadresseerd. Het College van B&W beoordeelt of de geïdentificeerde risico's en voorgestelde maatregelen aanvaardbaar zijn.
- **Governance en compliance:** Het bestuur waarborgt de naleving van alle relevante wet- en regelgeving op strategisch niveau, waaronder de AVG, de Cbw, de BIO2 en andere normen. Ze stelt het kader voor compliance vast en zorgt voor de naleving ervan.
- **Resources en budget:** Toewijzen van de nodige middelen en budget voor de implementatie van het beleid en het bereiken van de doelstellingen. Dit omvat het vrijmaken van middelen voor trainingen, risicobeheer, en technologie-investeringen.
- **Verantwoordelijkheid voor rapportage:** Het bestuur is verantwoordelijk voor het ontvangen van periodieke rapportages over de voortgang van de strategische doelstellingen, inclusief auditresultaten en risicoanalyses en deelt deze informatie met de gemeenteraad



3.4 Directie (Aansturing ambtelijke organisatie)

Het directieteam vormt de verbinding tussen het bestuursorgaan en het management en is daarmee verantwoordelijk voor het formuleren, adviseren en ambtelijk goedkeuren van de strategische doelstellingen van het IB&P-beleid, waaronder het voorkomen van incidenten, de bescherming van bedrijfsmiddelen en persoonsgegevens en de naleving van wet- en regelgeving. Daarnaast draagt de directie zorg voor de strategische en tactische borging van informatiebeveiliging en privacy binnen de organisatie. Hun rol kan als volgt worden omschreven:

- **Vertaling van beleid naar organisatie:** De directie vertaalt de door het College vastgestelde strategische doelstellingen naar concrete kaders en richtlijnen voor de teammanagers.
- **Uitvoering & Toezicht:** Stelt jaarlijks het uitvoeringsplan (IB&P-plan) en toezichtplan Meppel vast. Ontvangt rapportages van teammanagers en interne audit. Beoordeelt of de uitvoering van het beleid voldoet aan doelstellingen, richtlijnen en kaders, in combinatie met risicoafwegingen en kwaliteitsnormen. Op basis hiervan neemt het gerichte bijsturingsmaatregelen om continuïteit en kwaliteit van IB&P borgen.
- **Prioritering & Coördinatie:** Stelt prioriteiten en bewaakt de coördinatie tussen teams en processen, zodat IB&P niet versnipperd wordt uitgevoerd maar integraal onderdeel is van de bedrijfsvoering.
- **Escalatie en besluitvoorbereiding:** Brengt majeure risico's, incidenten of knelpunten onder de aandacht van het College en adviseert over bestuurlijke keuzes.
- **Resource- en prioriteitsstelling:** Zorgt dat de benodigde middelen, capaciteit en prioriteit beschikbaar zijn om het beleid effectief uit te voeren.
- **Cultuur en bewustwording:** Stimuleert een organisatie brede cultuur van informatiebewustzijn en privacy, en borgt dat dit thema structureel op de agenda staat.

3.5 Chief Information Officer

De Chief Information Officer (CIO) heeft een strategische en adviserende rol richting de Directie. Waar Teammanagers verantwoordelijk zijn voor de tactische en operationele uitvoering van informatiebeveiliging en privacy, richt de CIO zich op de strategische sturing, integrale advisering en besluitvorming rondom informatievoorziening en digitalisering.

Om aan het bovenstaande invulling te geven draagt deze persoon zorg voor:

- De Formulering van strategische doelen voor informatievoorziening afgestemd op organisatiedoelen.
- Creëert meerwaarde door inzet van informatievoorziening voor alle organisatieonderdelen.



- Adviseert over strategische doelen voor informatievoorziening en processen om de dienstverlening te verbeteren.
- Fungeert als opdrachtnemer van de directie voor het IM-projectportfolio en heeft mandaat voor noodzakelijke afstemming prioritering in behoeftes en projecten met een Informatie-component.
- Geeft richting en stuurt aan op innovatie en digitalisering van business processen in combinatie met een optimale informatievoorziening.
- Faciliteert Governance in het ICT landschap door middel van afstemming via overlegstructuren zoals SIO en de behoeftetafel.

Noot: In 2023 is door Directie besloten dat de rol van CIO binnen Meppel ingevuld wordt door de TM I&ID. Op deze wijze wordt al gewerkt, in afwachting van een aanpassing op het organisatiebesluit.

3.5 Teammanagers (Uitvoering, eigenaarschap en afstemming)

De uitvoering van informatiebeveiliging en privacy ligt bij de teammanagers. Zij zijn verantwoordelijk voor de kwaliteit, veiligheid en rechtmatigheid van de processen en gegevens binnen hun domein. Deze verantwoordelijkheid kan niet worden gedelegeerd; de uitvoering van werkzaamheden wel. Om deze verantwoordelijkheid waar te maken, worden teammanagers ondersteund door de Directie.

Alle processen, systemen, applicaties en (persoons)gegevens hebben een toegewezen eigenaar. Dit is doorgaans de manager die verantwoordelijk is voor het procesresultaat. Dit eigenaarschap is noodzakelijk om risico's, beveiligingsmaatregelen en naleving van wet- en regelgeving te kunnen borgen.

Teammanagers stemmen periodiek met de directie af over de voortgang, risico's en knelpunten op het gebied van informatiebeveiliging en privacy. Deze structurele afstemming borgt dat de uitvoering aansluit bij de strategische doelen en dat tijdig kan worden bijgestuurd waar nodig. Daarnaast vindt organisatie brede afstemming plaats binnen de reguliere overlegstructuren, zodat samenhang en consistentie in de uitvoering worden geborgd. Om aan het bovenstaande invulling te geven dragen zij zorg voor:

- **Implementatie van het beleid:** De teammanagers zijn verantwoordelijk voor de uitvoering van het IB&P-beleid binnen hun teams en zorgen ervoor dat de doelstellingen op operationeel niveau behaald worden. Zij werken samen met informatiemanagers, privacyfunctionarissen en beveiligingsprofessionals om risico's te beoordelen en behandelen
- **Zorgdragen voor risicobeheer:** Het identificeren van afdelingsspecifieke risico's en het implementeren van de nodige risicobeheersmaatregelen. Dit kan door middel van de uitvoering van risicobeoordelingen en het nemen van passende actie. Ze houden



hierbij rekening met factoren zoals prioriteit, beschikbare middelen en de capaciteit om maatregelen effectief uit te voeren.

- **Opleidingen en bewustwording:** Het organiseren en faciliteren van trainingen en bewustwordingscampagnes in afstemming met HR, CISO, PO en FG voor medewerkers binnen hun eigen team, specifiek gericht op risico's, beveiliging, en compliance binnen de eigen werkprocessen. Dit draagt bij aan de vermindering van menselijke fouten en incidenten. Naast het begeleiden en aanspreken van medewerkers op de al verplicht generieke bewustwording programma's van de gemeente Meppel, kunnen teammanagers ook bijsturen via dashboard informatie . beschikbaar voor teammanagers via de site meppel.recourse.nl.
- **Verantwoordelijkheid voor toegangscontrole:** Teammanagers zijn verantwoordelijk voor het borgen dat toegangsbeheer en de beveiliging van bedrijfsmiddelen en (persoons)gegevens binnen hun domein op een juiste en veilige manier zijn ingericht. De technische uitvoering hiervan ligt bij ICT en/of functioneel beheer. Teammanagers zorgen ervoor dat de juiste autorisaties worden aangevraagd, periodiek worden beoordeeld en waar nodig tijdig worden aangepast.
- **Rapportage aan het directieteam:** Teammanagers zijn verantwoordelijk voor het tijdig en volledig rapporteren over de voortgang en de uitvoering van het IB&P-beleid binnen hun Team. Zij rapporteren over specifieke team gerelateerde incidenten, risico's en de status van naleving en opvolging hiervan aan het directieteam. Bij het opstellen van deze rapportages kunnen teammanagers worden ondersteund door centrale en decentrale functies zoals CISO, FG of PO/SO, zonder dat dit iets afdoet aan hun eigen verantwoordelijkheid voor de inhoud.
- **Verantwoordelijkheid voor incidentrespons:** In geval van een incident binnen hun afdeling zijn zij verantwoordelijk voor de implementatie van het incidentresponsplan en het coördineren van de eerste reactie.

3.6 De tweede en derde lijn rollen: Controle en verantwoording

3.6.1 Tweede lijn (toezicht en ondersteuning)

De tweede lijn vervult een onafhankelijke, adviserende en ondersteunende rol richting het lijnmanagement. Hun doel is om te zorgen dat informatiebeveiliging en privacy consistent, juist en toetsbaar worden ingericht en uitgevoerd. De tweede lijn biedt expertise, stelt kaders op, geeft ondersteuning, en houdt systematisch toezicht op de naleving door de eerste lijn.

Tot de tweede lijn behoren onder meer de kwaliteitsmedewerkers, beleidsadviseurs, business consultants, de Privacy Officer (PO), de Security Officer (SO) en op onderdelen ook de Chief Information Security Officer (CISO). Samen vormen zij de functie die organisaties helpt om risico's te begrijpen, maatregelen te kiezen en de uitvoering te versterken.

Hun rol omvat, gevraagd en ongevraagd:



Expertise & Kaders

- Vertalen van wet- en regelgeving en organisatiedoelstellingen naar helder en integraal informatiebeveiligings- en privacybeleid.
- Opstellen en onderhouden van kaders, richtlijnen, standaarden en handreikingen die de eerste lijn ondersteunen bij een juiste uitvoering.

Ondersteuning & Risico & Maatregelen

- Ondersteunen van het lijnmanagement bij de tactische en operationele toepassing van informatiebeveiliging en privacy.
- Bieden van advies, praktische formats, best practices en duiding van risico's, inclusief het helpen kiezen van passende maatregelen.

Monitoring & Kritische Blik

- Monitoren en onafhankelijk rapporteren over de naleving en uitvoering door de eerste lijn.
- Signaleren van risico's, tekortkomingen en verbeterpunten, en deze objectief onder de aandacht brengen.
- Bevorderen van bewustwording en kennisdeling door trainingen, workshops en hulpmiddelen om de eerste lijn te versterken.

Met deze combinatie van **expertise, ondersteuning, monitoring, kritische blik en focus op risico & maatregelen** zorgt de tweede lijn voor een stabiele basis waarin de eerste lijn veilig, verantwoord en controleerbaar kan opereren.

3.6.2 Derde lijn (onafhankelijke controle)

De derde lijn wordt ingevuld door het audit- en control cluster van Team Bestuur en Organisatie, bestaande uit de Concerncontroller (CC), de Functionaris Gegevensbescherming (FG), de Verbijzonderde Interne Controle (VIC) en de interne auditfunctie. Hun rol is onafhankelijk en gericht op toetsing en verantwoording. Zij zijn verantwoordelijk voor:

- Het opstellen van een jaarlijks integraal toezichtplan.
- Het uitvoeren van audits en evaluaties om de effectiviteit van het IB&P-beleid te toetsen.
- Het monitoren van naleving van beveiligingsmaatregelen, gegevensbescherming en toegangscontrole.
- Het opstellen van rapportages met bevindingen en aanbevelingen, rechtstreeks aan management, directie en bestuur.
- Het initiëren van onderzoeken en verbeterplannen bij ernstige incidenten of nalevingsproblemen.
- Het zorgdragen voor volledige en correcte documentatie van alle compliance- en controleactiviteiten.



3.6.3 ENSIA

ENSIA staat voor Eenduidige Normatiek Single Information Audit. Het is de landelijke verantwoordingssystematiek waarmee gemeenten jaarlijks inzicht geven in hun informatiebeveiliging en privacy, en aantonen dat zij voldoen aan wettelijke normen.

Het ENSIA-proces, waaronder het invullen van vragenlijsten worden uitgevoerd door de verantwoordelijke functionarissen per deelgebied. De aangewezen ENSIA-coördinator zorgt voor de coördinatie, bewaakt de voortgang en ziet toe op de samenhang van de verantwoordingsactiviteiten. In Meppel is de rol van ENSIA-coördinator belegd bij de CISO. Daarmee wordt de samenhang geborgd tussen het ENSIA-proces en de bredere PDCA-cyclus van het gemeentelijke informatiebeveiligingsbeleid, zodat bevindingen structureel worden meegenomen in de beleidsontwikkeling en uitvoering..

De verantwoording over de informatiebeveiliging en privacybescherming komt als eigen verklaring in het jaarverslag tot uitdrukking onder de kop bedrijfsvoering en is gebaseerd op een extract van de collegeverklaring Informatiebeveiliging en privacy. Deze verklaring noemt met ook wel een “In Control verklaring”. Met deze verklaring geeft het college van B en W aan in hoeverre de gemeente voldoet aan de afspraken die gemaakt zijn voor de ENSIA-verantwoording Informatiebeveiliging en wettelijke eisen zoals uit de AVG, Cbw, DigiD-audit en Structuur Uitvoeringsorganisatie Werk en Inkomen (Suwi) wet. Ook worden de eventuele verbetermaatregelen vermeld die de gemeente gaat treffen in het komende jaar. De ingevulde zelfevaluatievragenlijst vormt tevens de basis voor het opstellen van de collegeverklaring aan de raad voor de zogenaamde horizontale verantwoording.

3.6.4 Wpg

De gemeente verwerkt in het kader van haar handhavingstaken politiegegevens als bedoeld in de Wet politiegegevens (Wpg). Op grond van artikel 33 Wpg wordt minimaal eens per drie jaar een onafhankelijke audit uitgevoerd naar de naleving van deze wet en het bijbehorende Besluit politiegegevens.

De audit richt zich op de werking en effectiviteit van de getroffen maatregelen voor beveiliging, rechtmatigheid, logging, bewaartermijnen en toegangsbeheer binnen de processen waarin politiegegevens worden verwerkt. De uitkomsten van de audit worden besproken binnen het College van B&W en vormen input voor het continu verbeteren van de informatiebeveiliging en privacybescherming.

De uitvoering en opvolging van de Wpg-audit vanuit de interne auditfunctie zijn in Meppel belegd bij CISO, zodat bevindingen worden meegenomen in de bredere PDCA-cyclus van het gemeentelijke informatiebeveiligingsbeleid. De resultaten en verbetermaatregelen worden verwerkt in het jaarlijkse informatiebeveiligingsplan.



3.7 Medewerker

Informatiebeveiliging en privacy zijn niet alleen verantwoordelijkheden van bestuur en management, maar vereisen vooral actieve betrokkenheid van iedere medewerker binnen de gemeente. Van medewerkers wordt verwacht dat zij zorgvuldig omgaan met informatie en persoonsgegevens, en dat zij bijdragen aan een veilige en integere werkomgeving. Dit betekent dat informatiebeveiliging en privacy onderdeel zijn van het dagelijks handelen en dat medewerkers verplicht zijn om risico's en incidenten tijdig te signaleren en te melden.

Expliciete verplichtingen voor medewerkers zijn onder andere:

- Melden van incidenten: Iedere medewerker is verplicht beveiligings- of privacy-incidenten direct te melden via de daarvoor vastgestelde procedure.
- Verbetervoorstellen doen: Medewerkers dragen actief bij aan het verbeteren van processen door knelpunten of risico's te signaleren en voorstellen voor verbetering te doen.
- Deelname aan bewustwordingsactiviteiten: Deelname aan trainingen, workshops en campagnes rondom informatiebeveiliging en privacy is verplicht om kennis en bewustzijn op peil te houden.
- Zorgvuldig omgaan met gegevens: Medewerkers hanteren het principe van dataminimalisatie en verwerken persoonsgegevens uitsluitend voor het doel waarvoor ze zijn verzameld.
- Naleving van beleid en procedures: Medewerkers volgen de vastgestelde beleidsstukken, procedures en werkinstructies en passen deze consequent toe in hun werk.

3.8 Externe organisaties en dienstverleners

De gemeente werkt intensief samen met externe organisaties en dienstverleners voor het uitwisselen van informatie en de levering van producten en (cloud)diensten. Om de integriteit, vertrouwelijkheid en beschikbaarheid van gemeentelijke informatie te waarborgen, hanteert de gemeente duidelijke eisen aan deze partijen. Deze eisen zijn onderdeel van onze governance-structuur en vormen een vast onderdeel van contractering, leveranciersmanagement en toezicht.

Normenkaders en Contractuele Afspraken

- Toepassing GIBIT

Voor ICT-diensten hanteert de gemeente de GIBIT (Gemeentelijke Inkoopvoorwaarden bij IT) als uitgangspunt; waar nodig kan hiervan worden afgeweken, mits beide partijen dit expliciet overeenkomen en vastleggen.

- Verwerkingsovereenkomsten (AVG)



Als een partij persoonsgegevens verwerkt ten behoeve van de gemeente, is een verwerkersovereenkomst verplicht. De gemeente Meppel maakt uitsluitend gebruik van de standaard verwerkersovereenkomst van de VNG. Als er afgeweken wordt van deze standaard dan dient dit ter advies voorgelegd te worden aan de FG of PO. Alle afwijkingen moeten in het zaaksysteem vastgelegd worden. Exit- en overdrachtsafspraken. Overeenkomsten voor informatie-uitwisseling

Wanneer geen sprake is van verwerking in opdracht, maar wel van uitwisseling van gegevens, worden aanvullende afspraken gemaakt over doelbinding, beveiligingsniveaus, bewaartermijnen, logging en toegangsbeheer.

- Beveiligingsborging en Certificeringen

De gemeente verwacht dat externe partijen hun beveiligingsniveau aantoonbaar kunnen maken. Afhankelijk van het type dienst en het risico kunnen de volgende bewijzen worden verlangd:

- ISO 27001 certificering of een gelijkwaardig Information Security Management System.
- ISAE 3402 Type II, ISAE 3000, of een vergelijkbaar assurance-rapport voor beheer- of cloudomgeving.
- ENSIA-, BIO- of andere relevante sectorale verantwoordingen, afhankelijk van het werkveld.
- Penetratietest- of auditrapportages op verzoek, mits contractueel overeengekomen.

Wanneer certificering niet haalbaar is, dient de partij alternatieve vormen van onafhankelijke toetsing te leveren (bijv. een third-party review of beveiligingsassessment).

- Inzicht in Incidenten en Continuïteit

Externe partijen moeten op een transparante wijze rapporteren over incidenten, dreigingen en kwetsbaarheden die impact kunnen hebben op gemeentelijke dienstverlening of gegevens. De gemeente verwacht daarom:

- Onmiddellijke melding bij ernstige of kritieke beveiligingsincidenten, datalekken of materiële verstoringen bij de gemeente Meppel;
- Maandelijks of kwartaalrapportages over incidenten, trends en verbetermaatregelen (indien proportioneel bij de dienst);
- Toegang tot relevante loggingsinformatie, voor zover noodzakelijk voor onderzoek en binnen wettelijke kaders;
- Continuïteits- en herstelplannen (BCP/DRP), inclusief periodieke testresultaten.

- Service Level- en Dienstenmanagement



Voor alle diensten en samenwerkingen met een risicokarakter worden meetbare afspraken gemaakt over integriteit, beschikbaarheid en vertrouwelijkheid:

- Service Level Agreements (SLA) met afspraken over beschikbaarheid, responstijden, hersteltermijnen en escalatie.
- Diensten Niveau Overeenkomsten (DNO) bij samenwerking met publieke partners.
- Periodieke prestatie-rapportages, inclusief afwijkingen en uitleg van structurele oorzaken.

Rechten op toezicht en audit, zodat de gemeente toezicht kan houden op de naleving van afspraken.

- Risico gestuurde Toetsing en Leveranciersmonitoring

De gemeente beoordeelt externe partijen risico gestuurd. Dit omvat:

- een toetsing vooraf (due diligence en DPIA wanneer nodig);
- jaarlijkse evaluaties van beveiligings- en privacymaatregelen;
- een risicoklasse per leverancier en de daarbij horende beheersmaatregelen;
- correctieve maatregelen bij tekortkomingen, inclusief het recht om dienstverlening op te schorten of te beëindigen indien risico's onvoldoende worden beheerst.



4. Communicatie & Overleg

Binnen de gemeente Meppel zijn verschillende overlegstructuren ingericht om de sturing, afstemming en borging van informatiebeveiliging te waarborgen. Deze overleggen vinden regelmatig plaats op strategisch, tactisch en operationeel niveau en zorgen voor continue monitoring, besluitvorming en kennisdeling, zoals:

- Portefeuilleoverleg (PFO): Strategisch overleg tussen Burgemeester en CISO samen met de CIO en FG over informatiebeveiligingsbeleid en privacy in relatie tot beleid, dreigingsbeelden en risicobereidheid vanuit het College.
- Directieoverleg: Tactisch overleg tussen Directie, CIO, CISO, FG en CC over beleidsontwikkeling, incidenten en organisatieontwikkelingen.
- Audit en Control overleg: Horizontaal overleg tussen Concerncontroller, CISO, FG en VIC over rechtmatigheid, interne controles en rapportages.
- Operationeel Overleg Team I&ID met CISO en FG: Overleg over lopende en toekomstige projecten, incidenten en voortgang van het jaarplan.
- Continue communicatie tussen CISO (B&O) en PO/SO-overleg: dagelijks of ad-hoc overleg over incidenten, datalekken, bewustwording en actuele ontwikkelingen.
- Horizontaal overleg tussen Teammanagers en CISO waarbij bewustwording en ontwikkelingen binnen het team centraal staan



Bijlage A: De 10 bestuurlijke principes voor informatiebeveiliging (VNG)

1. Bestuurders bevorderen een veilige cultuur

Menselijk gedrag en cultuur beïnvloeden op significante wijze alle aspecten van risicomanagement op elk niveau en in elk stadium.

Ik ben mij bewust van de voorbeeldfunctie van een bestuurder en ik draag uit dat risicomanagement van iedereen is. Ik zorg daarom voor een cultuur waarin iedereen vrij is om dreigingen waar te nemen en te melden. In eerste instantie bij de verantwoordelijke, maar indien nodig ook bij mij als bestuurder. Ik spoor managers aan om voorwaarden te scheppen zodat iedereen binnen de organisatie deelgenoot wordt van het proces van risicomanagement. Ik zorg ervoor dat fouten besproken kunnen worden en dat daarmee een lerende organisatie ontstaat. Ten slotte geef ik in mijn eigen doen en laten het goede voorbeeld van hoe je verantwoordelijk omgaat met informatie.

Toelichting

Zonder open cultuur waar iedereen vrij is om te spreken is het niet goed mogelijk om risico's te identificeren en als de risico's niet bekend zijn, kunt u ze ook niet adresseren. Als u in uw organisatie een cultuur bevordert waarin mensen zich vrij voelen om risico's te melden en maatregelen voor te stellen, dan kunt u adequaat reageren op dreigingen en samenhangende risico's.

2. Informatiebeveiliging is van iedereen

Passende en tijdige betrokkenheid van belanghebbenden maakt het mogelijk dat hun kennis, opvattingen en percepties in aanmerking worden genomen. Dit resulteert in een verbeterd bewustzijn en goed geïnformeerd risicomanagement.

Ik maak medewerkers bewust van de risico's van het werken met informatie en ik maak risicomanagement onderdeel van het MT-overleg en laat het anderen in vergaderingen agenderen. Ik zorg ervoor dat iedereen risicomanagement toepast en dat het gezien wordt

Duurzaamheid in Gemeente Meppel

Gemeente Meppel staat voor duurzaamheid. Dit document is ontworpen voor online gebruik. Wil je het document toch printen? Print dan in zwart-wit en minimale printkwaliteit.

Kijk voor meer informatie over duurzaamheid in Gemeente Meppel op www.meppel.nl/duurzaam.



als vanzelfsprekend en nuttig. Ik ben transparant naar de raad en zorg ervoor dat hij ook zijn rol kan pakken op dit onderwerp.

Toelichting

Iedereen moet betrokken worden bij risicomanagement, in alle lagen van de organisatie. Maak gebruik van de kennis en verantwoordelijkheid van proces- en systeem eigenaren. Gebruik uw Chief Information Security Officer (CISO), Functionaris Gegevensbescherming (FG) en Controller als onafhankelijke adviseur en laat ze samenwerken in een risicoteam, waar u vanzelfsprekend ook zitting in heeft. Laat uw interne communicatie aandacht besteden aan het verspreiden van de boodschap, het belang en het voordeel van risicomanagement binnen uw organisatie. Goed uitgevoerd risicomanagement creëert waarde voor de organisatie omdat de kwaliteit van besluiten toeneemt en de kans op falen afneemt.

3. Informatiebeveiliging is risicomanagement

Risicomanagement wordt bewust toegepast bij alle organisatie activiteiten.

Ik zorg dat risicomanagement een onderdeel is van het bestuurlijk overleg en dialoog. Daarnaast zal ik het integreren in het risicobewustzijn van alle medewerkers en het onderdeel laten zijn van de samenwerking met partners en ik zorg ervoor dat risicomanagement integraal onderdeel uitmaakt van uitbestedingen en samenwerkingen. Ik zorg ervoor dat risicomanagement geformaliseerd wordt binnen de hele organisatie met een duidelijke verdeling van verantwoordelijkheden en heldere besluitvorming.

Toelichting

Risicomanagement werkt alleen als het geïntegreerd is in alle werkprocessen van de organisatie. Dat kan alleen bereikt worden als risico's regelmatig op de agenda staan en als risico's een plek/paragraaf krijgen in alle bestuurlijke documenten. Maak lijnmanagers verantwoordelijk voor risicomanagement door afspraken met ze te maken over uw risicobereidheid. Lijnmanagers zijn verantwoordelijk voor de maatregelen en rapportage daarover.

4. Risicomanagement is onderdeel van de besluitvorming

Risicomanagement is onderdeel van alle besluiten en risicomanagement is chefsache.



Ik maak medewerkers mede-eigenaar van het risicoproces op het vlak van informatieveiligheid en ik maak informatiebeveiliging onderwerp van alle overlegstructuren. Ik draag er zorg voor dat besluiten ten aanzien van de omgang met risico's expliciet genomen en vastgelegd worden. Ik laat risicomanagement naadloos aansluiten op de strategische en beleidsmatige doelstellingen van de organisatie. Op deze wijze bied ik een duidelijk kader waarbinnen de medewerkers kunnen opereren.

Toelichting

U kunt als bestuurder alleen de juiste richting aangeven als informatie u bereikt. Door dreigingen en risico's mee te nemen in de vragen die u stelt aan uw managers kunt u er in uw beslissingen ook rekening mee houden. Zo kunt u bijsturen voordat risico's manifest worden en escalatie voorkomen.

5. Informatiebeveiliging heeft ook aandacht in (keten)samenwerking

Het risicomanagementproces is aangepast en staat in verhouding tot de externe en interne context van de organisatie die verband houdt met haar doelstellingen.

Ik zorg dat ik de risico's ken die een gevaar vormen voor de informatievoorziening van de bedrijfsvoering van de gemeente en ik anticipeer op risico's die voortkomen uit het werken in ketens en ik houd rekening met de complexiteit, de onzekerheid en ambiguïteit in de samenwerking met anderen. Bij samenwerken of uitbesteden van (delen) van de organisatie of processen zorg ik ervoor dat de risico's in kaart gebracht zijn, verantwoordelijkheden verdeeld en dat de juiste maatregelen getroffen worden.

Toelichting

Het risicomanagementproces moet passen bij de organisatie en ondersteunen aan de organisatiedoelstellingen. De keten is zo sterk als de zwakste schakel. De gemeente dient met ketenpartners en leveranciers regelmatig het gesprek te voeren over risico's en de maatregelen die ervoor zorgen dat de risico's tot een acceptabel niveau worden teruggebracht.



6. Informatiebeveiliging is een proces

Risico's kunnen ontstaan, veranderen of verdwijnen als de externe en interne context van een organisatie verandert. Risicomanagement detecteert en anticipeert op die veranderingen en gebeurtenissen op een gepaste en tijdige manier.

Ik zorg ervoor dat risicomanagement cyclisch is en daarmee kan ik reageren op veranderingen en toekomstgericht sturen. Het staat daarom regelmatig op de agenda.

Toelichting

Risicomanagement moet een cyclisch, iteratief en terugkerend proces zijn, want dreigingen veranderen, doelstellingen veranderen, de omgeving verandert en wetgeving verandert. Indien u in uw risicomanagement geen rekening houdt met een veranderende omgeving, dan zijn uw maatregelen op termijn wellicht niet doeltreffend of doelmatig.

7. Informatiebeveiliging kost geld

Risico's moeten behandeld worden en er zijn vele manieren om veiligheid te realiseren, maar aan alle zijn kosten verbonden.

Ik zorg ervoor dat er voldoende middelen beschikbaar zijn om de onderkende risico's op een adequate manier te behandelen. Als gebleken is dat een risico een bedreiging is voor de organisatiedoelstellingen en er maatregelen genomen moeten worden, dan zorg ik er ook voor dat de middelen beschikbaar zijn om deze maatregelen uit te voeren.

Toelichting

Risico's kunt u ontwijken, mitigeren, overdragen of wegnemen door het nemen van preventieve-, repressieve- en/of correctieve maatregelen. Welke strategie u ook kiest, ze kosten allemaal middelen in termen van tijd en geld. Voor maatregelen kan derhalve een kosten-batenanalyse worden gemaakt.

8. Onzekerheid dient te worden ingecalculeerd

De input voor risicomanagement is gebaseerd op historische en actuele informatie, evenals op toekomstige verwachtingen. Risicomanagement houdt expliciet rekening met eventuele beperkingen en onzekerheden die aan dergelijke informatie en verwachtingen zijn



verbonden. Informatie moet tijdig, duidelijk en beschikbaar zijn voor relevante belanghebbenden.

Risicomanagement is gebaseerd op de best beschikbare informatie vanuit mijn organisatie en vanuit mijn samenwerkingen. Ik zorg ervoor dat alle belanghebbenden op een gestructureerde en voorspelbare wijze informatie delen die bijdraagt aan risicomanagement.

Toelichting

Zonder goede informatie kunt u geen goede risico-inschattingen en besluiten nemen. Zonder goede en tijdige informatie bent u niet bekend met de risico's die uw organisatie loopt.

9. Verbetering komt voort uit leren en ervaring

Risicobeheer wordt voortdurend verbeterd door leren en ervaring.

Door mijn inzet zorg ik ervoor dat risicogestuurd werken doorontwikkeld wordt. Ik reflecteer op ervaringen en ik nodig medewerkers uit tot het delen van ervaringen met betrekking tot de risico's die de informatievoorziening bedreigen. Ik zorg ervoor dat de organisatie kan leren van incidenten en dat de organisatie leert te ontdekken wat wel en wat niet werkt.

Toelichting

Risicomanagement gedijt het beste in een organisatie die leert van ervaringen en op basis hiervan verbeteringen doorvoert. Hoe goed u uw informatiehuishouding ook beveiligd, incidenten zullen altijd voorkomen. Door te zoeken naar verbeterpunten en de wil om te leren bouwt u doorlopend aan het verhogen van uw digitale weerbaarheid.

10. Het bestuur controleert en evalueert

Risicomanagement is het controleren en evalueren van resultaten, evenals het nemen van eindverantwoordelijkheid en het doorhakken van lastige knopen.

Ik geef opdracht om de werking van risicomanagement binnen mijn organisatie op effectiviteit en efficiency te (laten) controleren. Naast managementrapportages zijn (externe) controles de manier om te weten te komen of en hoe het beleid in de praktijk uitwerkt. Als bestuurder weeg ik goed geïnformeerd risico's en belangen af en neem ik mijn verantwoordelijkheid om knopen door te hakken.



Toelichting

Controle is belangrijk om goed inzicht te krijgen in de mate waarin het informatiebeveiligingsbeleid en risicomanagement ingebed zijn in de organisatie. Naast verslagen en managementrapportages zijn incidenten, en dan vooral de manier waarop ze afgewikkeld worden, een goede graadmeter om te zien hoe de organisatie omgaat met het onderwerp. Medewerkers kunnen erop vertrouwen dat besluiten op bestuursniveau genomen worden, wanneer de situatie daar om vraagt



Bijlage B Afkortingen en Begrippenlijst

<i>AP</i>	Autoriteit Persoonsgegevens
<i>Baseline</i>	Basisniveau, minimumniveau.
<i>Baseline Informatiebeveiliging Overheid</i>	Het verplichte basisnormenkader voor informatiebeveiliging voor alle overheidslagen.
<i>Beschikbaarheid</i>	Het waarborgen dat geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen (informatiesystemen).
<i>BBN</i>	Basis Beveiliging Niveau
<i>BCM</i>	Bedrijfscontinuïteitsbeheer (Business Continuity Management)
<i>BCP</i>	Zie business continuïteitsplan
<i>BIO</i>	Zie Baseline Informatiebeveiliging Overheid
<i>BIV</i>	Acroniem voor Beschikbaarheid, Integriteit en Vertrouwelijkheid
<i>Business continuïteitsplan</i>	Een business continuïteitsplan beschrijft welke procedures en instructies gevolgd moeten worden om te kunnen blijven opereren tijdens een ongeplande onderbreking van de bedrijfsvoering of dienstverlening. Het plan maakt onderdeel uit van bedrijfscontinuïteitsbeheer.
<i>CISO</i>	Chief Information Security Officer
<i>Cloud</i>	De Cloud bestaat uit computers op afstand die je (meestal) via internet gebruikt voor opslag en programma's.
<i>CPO</i>	Concern Privacy Officer
<i>Datalek</i>	Een beveiligingsincident waarbij persoonsgegevens zijn betrokken.
<i>Eenduidige Normatiek Single Information Audit</i>	Verantwoordingproces dat gemeenten volgen om zich te verantwoorden over informatiebeveiliging aan de gemeenteraad en het Rijk.
<i>ISO</i>	Information Security Officer
<i>ENSIA</i>	Zie Eenduidige Normatiek Single Information Audit
<i>FG</i>	Functionaris voor Gegevensbescherming
<i>IBD</i>	Zie Informatiebeveiligingsdienst
<i>IBP</i>	Informatiebeveiligingsplan



<i>In Control Verklaring</i>		Met een In Control Verklaring (ICV) of In Control Statement (ICS) verklaart de organisatie (of een onderdeel ervan) dat zij voor haar bedrijfsvoering aan de beveiligingseisen voldoet. De ICV geeft inzicht aan welke beveiligingsnormen wordt voldaan en voor welke beveiligingsnormen een uitzondering is gedefinieerd.
<i>Informatiebeveiligingsdienst</i>		De Informatiebeveiligingsdienst is het Computer Emergency Response Team (CERT) voor alle Nederlandse gemeenten en is onderdeel van de Vereniging van Nederlandse Gemeenten.
<i>Informatiebeveiligingsincident</i>		Een gebeurtenis waardoor de vertrouwelijkheid, integriteit of beschikbaarheid van de informatievoorziening of informatie ernstig gevaar loopt of die zich al als zodanig heeft voorgedaan.
<i>Information Management System</i>	<i>Security</i>	Het Information Security Management System is een proces voor informatiebeveiliging dat gebaseerd is op de ISO 27001.
<i>Informatiesysteem</i>		Een samenhangend geheel van gegevensverzamelingen, en de daarbij behorende personen, procedures, processen en programmatuur, alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie.
<i>Informatievoorziening</i>		Een informatievoorziening bestaat uit een verzameling, mogelijk samenhangende, informatiesystemen met elk een duidelijke eigenaar.
<i>Integriteit</i>		Het waarborgen van de juistheid en volledigheid van informatie en de verwerking ervan.
<i>ISMS</i>		Zie Information Security Management System
<i>ISO</i>		Information Security Officer
<i>ISO 27001</i>		ISO 27001 is een internationale informatiebeveiligingsstandaard, die in Nederland is uitgebracht als NEN-ISO/IEC 27001. De ISO 27001 beschrijft het proces van informatiebeveiliging (ISMS) en is daarmee een belangrijke basis voor de BIO. De norm maakt deel uit van Forum Standaardisatie en is daarmee verplicht voor alle overheden.
<i>ISO 27002</i>		ISO 27002 is een internationale informatiebeveiligingsstandaard die in Nederland is uitgebracht als NEN-ISO/IEC 27002. Deze standaard geeft handreikingen voor de implementatie van de ISO 27001-maatregelen (controls) en is verplicht voor alle overheden.
<i>3LoD</i>		Zie Three Lines of Defense
<i>NORA</i>		De Nederlandse Overheid Referentie Architectuur (NORA) is het interoperabiliteitsraamwerk voor de Nederlandse overheid en vertaalt daartoe wetgeving, beleid en standaarden naar architectuurprincipes, beschrijvingen en modellen.



<i>Operational Technology</i>	Operational Technology (OT), ook wel bekend onder de naam Procesautomatisering (PA), is een verzamelnaam voor verschillende systemen die worden gebruikt voor het beheer van operationele processen in de fysieke wereld, zoals het aansturen en monitoren van (industriële) apparatuur.
<i>OT</i>	Zie Operational Technology
<i>PO</i>	Privacy Officer
<i>PPM</i>	Project Portfolio Management
<i>Procesautomatisering (PA)</i>	Zie Operational Technology
<i>Risico</i>	De kans op het optreden van een ongewenste gebeurtenis of situatie vermenigvuldigd met de daaruit voortvloeiende schade (impact)
<i>SUWI</i>	SUWI staat voor Structuur Uitvoeringsorganisatie Werk en Inkomen. Het is het wettelijke kader dat de organisatie en samenwerking regelt tussen instanties zoals UWV, SVB en gemeenten bij de uitvoering van sociale zekerheid en arbeidsvoorziening
<i>Risicomanagement</i>	Het proces van vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van Beschikbaarheid, Integriteit en Vertrouwelijkheid alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.
<i>Three Lines of Defense (3LoD)</i>	Het Three Lines of Defense model is een wereldwijd gebruikt raamwerk voor risicobeheer en compliance en draagt bij aan een effectieve informatiebeveiliging.
<i>VDW</i>	Zie Verhogen Digitale Weerbaarheid
<i>Verhogen Digitale Weerbaarheid</i>	Modules die door de Informatiebeveiligingsdienst worden aangeboden om de basis van informatiebeveiliging op orde te krijgen.
<i>Vertrouwelijkheid</i>	Het waarborgen dat informatie alleen toegankelijk is voor diegenen die hiertoe zijn geautoriseerd.



Bijlage C: Overzicht van Wet en regelgeving

- Cyberbeveiligingswet (Cbw).
- Baseline Informatiebeveiliging 2.0(BIO2).
- Cybersecurity Implementatie Richtlijn (CSIR)
- Algemene Verordening Gegevensbescherming (AVG).
- Wet Politie Gegevens (WPG).
- Wet Basis Registratie personen (BRP).
- Paspoortuitvoeringsregeling Nederland 2001 (PUN).
- Wet Basisregistratie grootschalige topografie (BGT).
- Wet Basisregistratie adressen en Gebouwen (BAG).
- Wet Basisregistratie Ondergrond (BRO).
- Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI).
- Wet Open Overheid (WOO).

Daarnaast zijn er een aantal richtlijnen en programma's die onze aanpak verder ondersteunen en versterken, waaronder:

- Het programma Koers van de gemeente Meppel.
- De optimalisatie op Visie op Control voor Meppel uit 2021.
- Strategisch Informatie Plan Meppel
- Ontwikkeling strategisch Portfolio Board
- Optimalisatie Mandaatregister
- Bijstelling Organisatiebesluit



Bijlage D: Een grafisch Overzicht (momentopname) van diverse onderwerpen op het gebied van Informatiebeveiliging en privacy (IB&P)

Blauw = Aanwezig
Rood = Feitelijk nog niet aanwezig (wel in het RAP, voor een deel)
Oranje = In ontwikkeling of wordt bijgesteld
Wit = Niet Relevant of zeer beperkt van omvang

IB-Plan Jaarlijks	Auditplan Jaarlijks	Toegang	Tele- werken	Malware (Defender)	Tekst- berichten
Personeel Screening	Geheim- houding	Huisregels	Bewust- wording	Clear Desk & Screen	ISMS & PIMS
Logging	SIEM / SOC	Incident Management	Crisis Management	BCM	Contact Overzicht
Privacy	Datalekken proces	Teams gebruik	Classifi- catie	DLP Ingericht	CVD Vulnerabilty
Crypto	Wijzigingen proces	Backup & Restore	Kwetsbaar- heden	Netwerk segmentering	Informatie Transport
SUWI Beheerplan	WPG Beheerplan	Keten- Beheer	Mobiele apparaten	Ontwikke- ling	Proces Automatisering