Rekenkameronderzoek informatiebeveiliging

Gemeente Meppel



DMC GROUP
SECURITY MANAGEMENT

Documentbeheer

Opdrachtgever
Rekenkamer Meppel

Versie
v1.1

Datum
21 juni 2026

Auteur(s)
ir. Stijn Hoogervorst CISSP CISM
mr. Alexander Garrelfs CCSP CISSP CISM CIPP/e OTPM/A
Timothy Siebes MSc. GCIH GSEC CISSP
drs. Chris Deben MBA CISM
Mick Deben MSc. CISSP CRISC CGEIT CCSP SSCP AAISM

Distributie
DMC Group distribueert alle versies beveiligd (end-to-end versleuteld) via Tresorit

DMC Group
Postbus 928
6200 AX Maastricht

+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl

KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

DMC GROUP
SECURITY MANAGEMENT

Managementsamenvatting

In opdracht van de personele unie van de rekenkamers van de gemeenten Meppel, Staphorst, Steenwijkerland en Westerveld (MSSW) heeft DMC een onderzoek naar de informatiebeveiliging bij de vier gemeenten uitgevoerd. Voor elke gemeente is een afzonderlijk en zelfstandig onderzoek uitgevoerd. De onderzoeken hebben plaatsgevonden in de periode augustus 2025 - december 2025. In dit rapport zijn uitsluitend de bevindingen van de gemeente Meppel verwerkt en zijn aanbevelingen gedaan ter verbetering van de algehele informatiebeveiliging. De rekenkamer trekt op basis van dit rapport conclusies.

Gemeenten spelen een cruciale rol in de (digitale) samenleving. Zij beheren en verwerken grote hoeveelheden privacygevoelige informatie, zijn sterk afhankelijk van digitale systemen voor hun dienstverlening en werken intensief samen met ketenpartners en leveranciers. De continuïteit, betrouwbaarheid en veiligheid van de informatievoorziening zijn daarmee essentieel voor het vertrouwen van burgers en bedrijven in de gemeente en de kwaliteit van de publieke taken. Tegelijkertijd worden gemeenten geconfronteerd met een groeiend en complexer wordend cyberdreigingslandschap en strengere wet- en regelgeving, zoals de Cyberbeveiligingswet (Cbw).

Belangrijkste bevindingen en aanbevelingen

De belangrijkste bevindingen en aanbevelingen zijn onderverdeeld in de vier domeinen van de BIO2: Organisatorisch, Mensgericht, Fysiek en Technologisch. De vier domeinen zijn complementair en zorgen samen voor een integrale beheersing van informatiebeveiligingsrisico's: bestuurlijk geborgd, menselijk gedragen, fysiek beschermd en technisch afgedwongen.

Organisatorisch

Het organisatorische domein gaat over governance (bestuur), verantwoordelijkheid en sturing op informatiebeveiliging. Het borgt dat bestuur en management duidelijke keuzes maken, risico's afwegen en verantwoording afleggen. Dit is essentieel omdat informatiebeveiliging alleen effectief is als het bestuurlijk is verankerd en actief wordt aangestuurd.

Informatiebeveiliging staat bij Meppel op het netvlies en er wordt aandacht besteed aan de juiste zaken. Informatiebeveiliging is echter informeel en ad-hoc georganiseerd waardoor het lastig(er) is om gemaakte keuzes of verrichte werkzaamheden aantoonbaar te kunnen maken en onderbouwen. De belangrijkste aandachtspunten hebben betrekking op het professionaliseren van het managementsysteem voor informatiebeveiliging, risicobeheer, continuïteitsbeheer en leveranciersmanagement.

Mensgericht

Dit domein richt zich op het gedrag, bewustzijn en de competenties van medewerkers en bestuurders, inclusief screening, opleiding en duidelijke verantwoordelijkheden. Het is cruciaal omdat mensen vaak de doorslaggevende factor zijn in het voorkomen, veroorzaken, detecteren

DMC Group
Postbus 928
6200 AX Maastricht
+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl
KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

en reageren op beveiligingsincidenten; goed geïnformeerde en handelingsbekwame medewerkers verkleinen risico's aanzienlijk.

Er is sprake van continue aandacht voor het stimuleren van veilig gedrag, bijvoorbeeld via de wekelijkse microlearning. Medewerkers zijn zich bewust van hun verantwoordelijkheden en dragen die goed uit. De belangrijkste aandachtspunten zijn het toespitsen van de materialen op de doelgroep, het meten van de effectiviteit van bewustwordingsactiviteiten,

Fysiek

Dit domein richt zich op de beveiliging van gebouwen, werkplekken, datacenters en fysieke toegang tot systemen en informatie. Dit domein is belangrijk omdat digitale beveiliging niet losstaat van fysieke bescherming: onbevoegde fysieke toegang kan technische maatregelen direct ondermijnen.

Meppel heeft compartimentering toegepast en de rechten tot verschillende compartimenten gescheiden op basis van het 'need-to-be' principe. De belangrijkste aandachtspunten hebben betrekking op het opruimen van oude archiefkasten in de openbare ruimte, het adequaat opslaan van handhaving kleding en het verbeteren van sleutelbeheer en cameratoezicht.

Technologisch

Dit domein omvat de technische beveiliging van systemen en netwerken, zoals toegangsbeheer, logging, monitoring, patching en back-ups. Het is essentieel omdat digitale dienstverlening en gegevensbescherming direct afhankelijk zijn van robuuste en actuele Informatietechnologie[1] (IT-) en Operationele Technologie[2] (OT-)beveiliging.

Meppel heeft op technisch vlak diverse maatregelen geïmplementeerd die de weerbaarheid versterken. De belangrijkste aandachtspunten hebben betrekking op het actief monitoren op indicatoren van cyberaanvallen, het goed voorbereid zijn op cyberincidenten en consistentie in het beveiligingsniveau.

Aanbevelingen aan het college van B&W

Bestudeer de bevindingen en aanbevelingen in dit rapport en bepaal of de aanbevelingen worden overgenomen, en zo ja op welke termijn.

Aanbevelingen aan de gemeenteraad

De gemeenteraad heeft een belangrijke rol ten aanzien van de informatieveiligheid binnen Meppel. De VNG[3] benadrukt dat digitale veiligheid een bestuurlijke verantwoordelijkheid is die niet alleen de ambtelijke organisatie betreft, maar een integraal onderdeel moet zijn van het bestuurlijke werk van de raad. Door als raad het onderwerp regelmatig te agenderen,

[1] Informatietechnologie is een term binnen de informatica en behandelt een groot werkveld in de computertechnologie van hardware, software en computernetwerken.

[2] 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. Voorbeelden zijn sluizen en medische apparatuur.

[3] https://vng.nl/artikelen/raadgever-digitale-veiligheid

DMC Group
Postbus 928
6200 AX Maastricht
+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl
KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

kaders te stellen, prioriteiten te bepalen, voldoende middelen beschikbaar te stellen en toezicht te houden op hoe Meppel risico's beheerst en incidenten aanpakt, is de raad in staat haar kaderstellende en controlerende taak goed te vervullen. Het doel is het versterken van de (digitale) veiligheid van de gemeentelijke dienstverlening en de weerbaarheid van de gemeente en haar inwoners en ondernemers.

Neem kennis van de beschikbare hulpmiddelen[4][5] zodat u (beter) in staat bent om de juiste accenten te leggen en het gesprek inhoudelijk aan kunt gaan met het college.

Realiseer u dat de ENSIA-verantwoording een beperkt beeld van de realiteit schetst vanwege zelfevaluaties en beperkte onafhankelijke toetsing. Daarnaast richt ENSIA zich vooralsnog uitsluitend op het voldoen in opzet en bestaan aan de BIO-beheersmaatregelen, en niet op de effectieve werking over een langere periode. Zet het onderwerp informatiebeveiliging daarom regelmatig op de agenda en nodig bijvoorbeeld de CISO uit om de raad hierover bij te praten. Dit biedt de raad tevens ook de mogelijkheid om (technische) vragen te stellen.

De Cybersecurity Raad[6] adviseerde in 2018 al om minimaal 10% van het totale IT-budget voor informatiebeveiliging aan te wenden. Sinds 2018 is het cyberdreigingslandschap verergerd en zijn er meer wettelijke eisen in werking getreden. Het is dan ook niet meer dan logisch dat de kosten voor het onderhouden en aanscherpen van de algehele informatiebeveiliging ook toeneemt. Wees uzelf daarvan bewust bij de totstandkoming van de begroting.

[4] https://vng.nl/sites/default/files/2025-04/raadsleden-en-informatiebeveiliging.pdf
[5] https://vng.nl/sites/default/files/2023-04/checklist-raadsleden-digitale-veiligheid.pdf
[6] https://www.cybersecurityraad.nl/documenten/2018/04/01/csr-meerjarenstrategie-2018-2021

DMC Group
Postbus 928
6200 AX Maastricht
+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl
KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

DMC GROUP
SECURITY MANAGEMENT

Inhoudsopgave

1 Inleiding **7**

1.1 Cyberdreigingsbeeld gemeenten 7

1.2 Cyberbeveiligingswet 8

1.3 Onderzoeksvragen en -aanpak 8

1.4 Disclaimer 9

2 Bevindingen & aanbevelingen **10**

2.1 Organisatorisch 10

2.2 Mensgericht 16

2.3 Fysiek 19

2.4 Technologisch 21

2.5 Aanbevelingen gemeenteraad 25

3 Beantwoording onderzoeksvragen **27**

A Aangeleverde informatie **32**

B Interviews **45**

DMC Group
Postbus 928
6200 AX Maastricht

+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl

KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

DMC GROUP
SECURITY MANAGEMENT

1 Inleiding

Gemeenten spelen een cruciale rol in de (digitale) samenleving. Zij beheren en verwerken grote hoeveelheden privacygevoelige informatie, zijn sterk afhankelijk van digitale systemen voor hun dienstverlening en werken intensief samen met ketenpartners en leveranciers. De continuïteit, betrouwbaarheid en veiligheid van de informatievoorziening zijn daarmee essentieel voor het vertrouwen van burgers en bedrijven in de gemeente en de kwaliteit van de publieke taken. Tegelijkertijd worden gemeenten geconfronteerd met een groeiend en complexer wordend cyberdreigingslandschap en strengere wet- en regelgeving, zoals de Cyberbeveiligingswet (NIS2).

1.1 Cyberdreigingsbeeld gemeenten

Het cyberdreigingsbeeld van de Informatiebeveiligingsdienst voor gemeenten [7] benadrukt dat ransomware[8], datalekken[9] en uitval van processen door incidenten de grootste bedreigingen vormen voor Nederlandse gemeenten. De Informatiebeveiligingsdienst stelt dat gemeenten hun digitale weerbaarheid moeten versterken door basismaatregelen, leveranciersmanagement en intensievere samenwerking met andere gemeenten. De Informatiebeveiligingsdienst concludeert: ”Digitale veiligheid is geen luxe maar een noodzakelijke voorwaarde voor continuïteit en vertrouwen in gemeentelijke dienstverlening. Gemeenten moeten blijven investeren in bewustwording, technologie en samenwerking om huidige én toekomstige dreigingen effectief het hoofd te kunnen bieden. ”In dit licht is het van belang dat gemeenten inzicht hebben in hun huidige volwassenheid ten aanzien van informatiebeveiliging. Oftewel, in hoeverre processen, maatregelen en verantwoordelijkheden zijn ingericht, geborgd en effectief functioneren.

Het Cybersecuritybeeld Nederland[10] onderkent dat het cyberdreigingslandschap divers en onvoorspelbaar is en dat verschillende dreigingsactoren zich richten op Nederlandse doelwitten. Het benoemt dat geopolitieke ontwikkelingen het cyberdreigingslandschap beïnvloeden en dat generatieve AI[11] de schaal en impact van cyberdreigingen vergroot. Ondanks deze ontwikkelingen benadrukt de Algemene Inlichtingen en Veiligheidsdienst (AIVD) dat veel incidenten te voorkomen zijn met goede basismaatregelen en weerbaarheidstrainingen.

[7] https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2025/06/IBD-Dreigingsbeeld-informatiebeveiliging-2025-2026.pdf

[8] Kwaadaardige software waarbij een slachtoffer afgeperst wordt, nadat zijn digitale systeem of de bestanden erop met een code op slot zijn gezet. De aanvaller biedt de code tegen betaling aan, zodat hij er weer bij kan. Maar zelfs dat is niet zeker. Ransomware is een samenvoeging van de woorden ransom (losgeld) en software. Tegenwoordig is de daadwerkelijke software maar een kleine stap in de totale aanval die plaatsvindt. Alle stappen samen vormen de Ransomware Killchain.

[9] Een gangbare term voor een cyberincident, veelal gebruikt in relatie tot persoonsgegevens. In de context van de Algemene Verordening Gegevensbescherming is een datalek een leken-term voor ‘inbreuk in verband met persoonsgegevens’, inhoudende een incident waardoor de integriteit, beschikbaarheid en/of vertrouwelijkheid van persoonsgegevens worden aangetast. Voorbeelden zijn ransomware aanvallen, of een e-mail met alle geadresseerden in het “To” – veld.

[10] https://www.aivd.nl/documenten/publicaties/2025/11/26/cybersecuritybeeld-nederland-2025

[11] Generatieve AI gaat over vormen van kunstmatige intelligentie (AI) die nieuwe content creëren of genereren. Zoals teksten en afbeeldingen die net echt lijken.

DMC Group
Postbus 928
6200 AX Maastricht
+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl
KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

Dit onderstreept het belang voor gemeenten om de BIO2 te implementeren en te onderhouden.

In dit onderzoek is onder andere onderzocht hoe de gemeente Meppel zich verhoudt tot deze actuele dreigingen. Daarbij is gelet op de aanwezigheid en borging van basismaatregelen, het beheer van leveranciers- en ketenrisico's, de voorbereiding op incidenten en calamiteiten en de inrichting van governance en capaciteit. Ook is aandacht besteed aan de manier waarop Meppel inspeelt op opkomende risico's en toekomstige technologische ontwikkelingen. Zo wordt de volwassenheid in context geplaatst van het actuele cyberdreigingsbeeld.

1.2 Cyberbeveiligingswet

De Cyberbeveiligingswet verplicht alle overheidsorganisaties de BIO2 aantoonbaar na te leven en legt de eindverantwoordelijkheid expliciet bij het bestuur. Bestuurders moeten risicogebaseerd passende en evenredige maatregelen voor informatiebeveiliging vaststellen en goedkeuren, toezien op de kwaliteit van de uitvoering en actief sturen op cyberrisico's. Zij moeten zelf over voldoende kennis beschikken en borgen dat medewerkers structureel worden opgeleid. Daarnaast is de gemeente verantwoordelijk voor het tijdig melden van meldplichtige incidenten. De toezichthouder voor overheidsorganisaties is de Rijksinspectie Digitale Infrastructuur (RDI).[12]

1.3 Onderzoeksvragen en -aanpak

De hoofdvraag van dit onderzoek luidt:

Hoe wordt de informatieveiligheid binnen de gemeente georganiseerd, welke maatregelen zijn er genomen om de veiligheid van gevoelige gegevens te waarborgen, en in hoeverre zijn de kritische processen van de gemeente beschermd tegen infiltratie en ongeautoriseerde toegang?

De rekenkamer heeft twintig deelvragen geformuleerd verdeeld over acht categorieën:

1. Algemene informatieveiligheid
2. Beveiliging van kritische systemen
3. Risicoanalyse en dreigingen
4. Testen van infiltratie
5. Opleiding en bewustwording van personeel
6. Beveiliging van gegevens en privacy
7. Incidentmanagement en crisiscommunicatie
8. Kosten beveiligingsmaatregelen

[12] https://www.rdi.nl/

DMC Group
Postbus 928
6200 AX Maastricht
+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl
KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

Om de hoofd- en deelvragen te beantwoorden zijn informatie en documenten opgevraagd, interviews gehouden met verschillende medewerkers en heeft een schouw op locatie plaatsgevonden. De deelvragen zijn in het derde hoofdstuk beantwoord.

1.4 Disclaimer

Dit rapport vormt een momentopname van de huidige volwassenheid ten aanzien van informatiebeveiliging op basis van de beschikbare informatie ten tijde van het onderzoek. De bevindingen zijn gebaseerd op steekproeven, interviews en documentreview binnen de beperkte doorlooptijd en het beschikbare budget. Hierdoor kan niet worden uitgesloten dat er aanvullende risico's, kwetsbaarheden of verbeterpunten bestaan die buiten de reikwijdte van dit onderzoek vallen. De bevindingen en aanbevelingen dienen daarom te worden geïnterpreteerd als een indicatief beeld en niet als een volledige of uitputtende beoordeling van de informatiebeveiliging.

DMC Group
Postbus 928
6200 AX Maastricht

+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl

KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

DMC GROUP
SECURITY MANAGEMENT

2 Bevindingen & aanbevelingen

De bevindingen en aanbevelingen zijn onderverdeeld in de vier domeinen die aansluiten op de structuur van de Baseline Informatiebeveiliging Overheid (BIO) 2:

- Organisatorisch als het betrekking heeft op organisatorische aspecten;
- Mensgericht als het betrekking heeft op individuele personen;
- Fysiek als het betrekking heeft op fysieke objecten;
- Technologisch als het betrekking heeft op technologie.

De aanbevelingen in paragrafen 2.1 tot en met 2.4 zijn gericht aan het college van B&W. De aanbevelingen in paragraaf 2.5 zijn gericht aan de gemeenteraad.

2.1 Organisatorisch

Het organisatorische domein gaat over governance, verantwoordelijkheid en sturing op informatiebeveiliging. Het borgt dat bestuur en management duidelijke keuzes maken, risico's afwegen en verantwoording afleggen. Dit is essentieel omdat informatiebeveiliging alleen effectief is als het bestuurlijk is verankerd en actief wordt aangestuurd.

Het managementsysteem voor informatiebeveiliging (Information Security Management Systeem, ook wel ISMS) is een werkwijze om informatiebeveiliging op een gestructureerde manier toe te passen in de gemeente. Zo wordt de gemeente, en een bestuurder in het bijzonder, in staat gesteld om de juiste afwegingen te maken.

Om een veelvoorkomend misverstand te voorkomen: een managementsysteem is géén applicatie. Een applicatie kan wel ondersteunen bij het toepassen van een managementsysteem.

De BIO schrijft voor dat het managementsysteem van een organisatie voldoet aan NEN-EN-ISO/IEC 27001. Bij het bepalen van de reikwijdte van het managementsysteem moet een organisatie minimaal de bedrijfsprocessen en informatiesystemen opnemen die kritisch zijn voor haar dienstverlening, waarbij aantasting van de beschikbaarheid, integriteit of vertrouwelijkheid zou leiden tot onacceptabele impact.

Het managementsysteem voor informatiebeveiliging borgt de beschikbaarheid, integriteit en vertrouwelijkheid van informatie door een risicomanagementproces toe te passen. Dit geeft belanghebbenden het vertrouwen dat risico's adequaat worden beheerd.

Het is belangrijk dat het managementsysteem voor informatiebeveiliging deel uitmaakt van en geïntegreerd is met de procedures van de gemeente en met de algehele managementstructuur, en dat informatiebeveiliging in aanmerking wordt genomen bij het ontwerpen van processen, informatiesystemen en beheersmaatregelen.

DMC Group
Postbus 928
6200 AX Maastricht
+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl
KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

2.1.1 Bevindingen

1. De Chief Information Security Officer (CISO) heeft feitelijk 0.5 fte voor deze rol.
2. De CISO heeft een directe lijn naar de directie en het college en is gepositioneerd onder Bestuur en Organisatie.
3. Meppel huurt een Functionaris Gegevensbescherming (FG) in voor 0.2 fte. Achtervang van de FG is via het externe bureau afgedekt.
4. Meppel heeft haar kritieke processen en systemen vastgesteld.
5. Meppel heeft binnen het team Informatie & Interne Dienstverlening (I&ID) een Information Security Officer (ISO) aangesteld die tevens ook Privacy Officer (PO) is. De voorganger van de PO is beschikbaar als achtervang voor de huidige PO. De ISO is achtervang voor de CISO en vice versa.
6. De verantwoordelijkheden ten aanzien van informatiebeveiliging zijn formeel vastgesteld in het informatiebeveiligingsbeleid.
7. De teammanagers hebben de opdracht gekregen om continuïteitsplannen te maken voor de kritieke processen. Op de wiki heeft Meppel een overzicht van alle leveranciers inclusief contactpersonen. Het overkoepelende continuïteitsplan moet geactualiseerd worden.
8. De overlegstructuren zoals vastgesteld in het informatiebeveiligingsbeleid wijken af van de werkelijkheid, zoals bijvoorbeeld de jaarlijkse risico-inventarisatie en het directie-overleg.
9. Informatiebeveiliging en privacybescherming staan niet structureel op de agenda van het managementoverleg en directieteam. Er wordt vanuit het management en bestuur niet gevraagd naar sturingsinformatie ten aanzien van informatiebeveiliging.
10. Bij de totstandkoming van informatiebeveiligingsbeleid wordt input gevraagd en draagvlak gecreëerd door interactie met stakeholders, zoals medewerkers, teammanagers en de directie. Strategisch informatiebeveiligingsbeleid wordt door het college vastgesteld.
11. De CISO spreekt alle teammanagers afzonderlijk iedere twee maanden om relevante aspecten van informatiebeveiliging te bespreken, zoals bewustwording en de beschikbaarheid van systemen.
12. De jaarlijkse informatiebeveiligings- en toezichtsplannen worden voorafgaand afgestemd met de teammanagers. Beiden plannen worden tot aan het directieteam behandeld.
13. Meppel heeft geen formeel managementsysteem voor informatiebeveiliging en ondersteunende Governance, Risk & Compliance (GRC) tooling. Er loopt een aanbesteding voor GRC-tooling.

DMC Group
Postbus 928
6200 AX Maastricht
+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl
KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

14. Meppel heeft Business Impact Analyses (BIA) uitgevoerd om de te beschermen belangen ('kroonjuwelen') te bepalen. Hierbij zijn de beschikbaarheidseisen bepaald (tenzij dit wettelijk is bepaald)[13][14]. Dit heeft geresulteerd in 57 kroonjuwelen en wordt in Excel bijgehouden.

15. Risicobeheer is informeel georganiseerd en er is geen centraal overzicht van informatiebeveiligingsrisico's inclusief hun eigenschappen en status. Het kunnen aantonen van gemaakte keuzes rondom risicobehandeling is uitdagend vanwege het decentrale karakter (mailboxen, ticketingsysteem, gespreksverslagen, etc.). Risico-acceptatie vinden plaats door de systeem- en proceseigenaren (eerste lijn).

16. Een deel van de applicaties is niet via Single-Sign-On (SSO) gekoppeld, waardoor men lokale accounts en verschillende inloggegevens moet gebruiken.

17. Er is geen vastgesteld herstelplan voor cyberincidenten en -crises. Hier wordt aan gewerkt door Meppel. Meppel heeft een post van 3,5 miljoen euro gereserveerd voor noodgevallen door een cybercrisis en heeft geen retainer afgesloten met een gespecialiseerde partij. Een Digital Forensics & Incident Response (DFIR) retainer biedt garantie en voorrang op ondersteuning bij cybercrises.

18. Voor het herstellen van informatie en configuraties is er wel een herstelplan (backups).

19. Het informatiebeveiligingsplan wordt door de directie vastgesteld, hier is echter geen gedocumenteerd bewijs van aangeleverd.

20. Meppel verricht periodiek autorisatiecontroles op haar kritieke applicaties en systemen (deze lijst is breder dan hetgeen wettelijk verplicht is). De controles worden verricht door de functioneel beheerders en de ISO controleert deze. De CISO controleert op zijn beurt of de ISO zijn controles juist heeft uitgevoerd. Van dit laatste is geen gedocumenteerd bewijs aangeleverd.

21. Meppel heeft een cybercrisisoefening gehouden, geëvalueerd en heeft daar lering uit getrokken, zoals het aanscherpen van procedures.

22. Het onderwerp informatiebeveiliging leeft beperkt bij het college van B&W.

23. Informatiebeveiliging is structureel onderdeel van de paragraaf bedrijfsvoering in de rapportage van de Planning & Control cyclus.

24. Informatiebeveiliging staat bij de directie 2 á 3 maal formeel op de agenda waarin zij gebriefd wordt over de stand van zaken en relevante ontwikkelingen. Daarnaast staat het onderwerp ad-hoc op de agenda als daar aanleiding voor is.

25. De afhankelijkheid van de CISO is hoog en Meppel is zich daarvan bewust. Meppel stuurt aan op het beleggen van verantwoordelijkheden op rollen in plaats van individuen.

26. Het structureel uitvoeren en vastleggen van risicoanalyses is niet aan de orde, de CISO of controleurs moeten Meppel hierop aanjagen.

[13] Recovery Point Objective betekent herstelpuntdoestelling
[14] Recovery Time Objective betekent hersteltijddoelstelling

DMC Group
Postbus 928
6200 AX Maastricht
+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl
KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

27. Goed voorbeeldgedrag wordt belangrijk geacht, dit blijkt bijvoorbeeld uit het wekelijks beantwoorden van de awareness vragen en het aanjagen van teammanagers op dit onderwerp.
28. Meppel heeft de raad gevraagd om een investering om een programma op te tuigen voor het verbeteren van datamanagement.
29. Het verkrijgen van structureel voldoende middelen om de bedrijfsvoering op orde te brengen en te houden wordt als uitdagend beschouwd. Incidentele budgetten worden aangewend ter compensatie daarvan.
30. Autorisatiecontroles worden niet regelmatig uitgevoerd (HRM).
31. Gebruikersaccounts handmatig verwijderen of blokkeren is deels aan de orde.
32. De digitale toegang is niet ingericht op basis van rollen (Role Based Access Control).
33. HRM heeft geen overzicht van uitgegeven rechten en middelen aan medewerkers, zoals telefoons, laptops, sleutels, toegangspassen, etc.
34. Vast personeel ontvangt een laptop van Meppel, inhuur mag met eigen apparatuur inloggen op de virtuele werkplek (Bring Your Own Device).
35. Het vier-ogen principe (functiescheiding) wordt niet consequent toegepast door de salarisadministratie.
36. Er zijn geen (formele) afspraken gemaakt met de gemeente Steenwijkerland over de beveiliging van het datacenter. Meppel gaf aan dat er ooit een intentieverklaring is afgegeven, maar deze is niet aangeleverd.
37. Het verwerkingsregister (Excel) is eind 2023 voor het laatst vastgesteld en sindsdien niet actief bijgehouden. Het register wordt reactief bijgewerkt zodra er wijzigingen in verwerkingen geconstateerd worden. Bestaande verwerkingen worden niet gecontroleerd. Meppel is voornemens om het register in een Governance, Risk en Compliance (GRC) tool onder te brengen.
38. Meppel loopt achter qua AVG-compliance.
39. De bewaartermijnen voor persoonsgegevens zijn voor ongeveer 75% van de belangrijkste systemen technisch afgedwongen. Meppel neemt dit bij aanbesteding op als eis.
40. Dossiers rondom inzageverzoeken worden in het zaaksysteem geregistreerd.
41. Overeengekomen afspraken met leveranciers die in opdracht van Meppel persoonsgegevens verwerken (verwerkersovereenkomsten) worden niet periodiek door Meppel gecontroleerd.
42. Meppel voert pre-DPIA's uit om te bepalen of het uitvoeren van een DPIA noodzakelijk is. Het is voor medewerkers niet duidelijk wanneer een DPIA uitgevoerd moet worden, ondersteuning en aansturing vanuit de PO en FG is noodzakelijk.

DMC Group
Postbus 928
6200 AX Maastricht

+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl

KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

43. Vanuit het bestuur is onvoldoende opvolging gegeven aan de resultaten van een nulmeting in 2022-2023 ten aanzien van privacybescherming.
44. In het jaarverslag wordt verantwoording afgelegd over privacybescherming. De opvolging daarvan is beperkt en niet aantoonbaar.
45. Belangrijke aanbevelingen zoals het uitbreiden van de capaciteit ten aanzien van privacybescherming bereiken het college niet.
46. Meppel hanteert als uitgangspunt dat bij datalekken de betrokkenen altijd geïnformeerd worden.
47. Plaatsgevonden datalekken worden als voorbeeld gebruikt in bewustwordingsactiviteiten.
48. De FG verricht ieder jaarlijks toezichtsacties (4x) en rapporteert daarover aan de betrokken teammanagers en de directie. De FG bepaalt wat de toezichtsacties zijn en hoe die uitgevoerd worden.
49. De interactie met de gemeenteraad ten aanzien van privacybescherming is beperkt alsook de reactie op de adviezen van de FG.
50. Meppel is zich bewust van haar beperkte capaciteit en probeert achtervang te organiseren door bijvoorbeeld het aanwijzen van buddy's en het documenteren van kennis in een wiki.

2.1.2 Aanbevelingen

1. Ga door met het verder uitwerken van de continuïteitsplannen en betrek de gemeente Steenwijkerland voor wat betreft de technische uitwijkmogelijkheid.
2. Zorg ervoor dat de overlegstructuren ten aanzien van informatiebeveiliging in lijn zijn met hetgeen is vastgesteld in het beleid (of pas het beleid aan).
3. Zet het onderwerp informatiebeveiliging en privacybescherming regelmatig, bijvoorbeeld maandelijks, op de agenda van het managementteam en directie. Zo dwingt Meppel zichzelf het onderwerp regelmatig te behandelen en toont het leiderschap en betrokkenheid.
4. Vertaal de doelstellingen uit het informatiebeveiligingsbeleid naar meetbare indicatoren en rapporteer daar periodiek over aan het MT/DT. Begin klein met elementen die voor Meppel belangrijk zijn zoals bijvoorbeeld de dekkingsgraad van essentiële maatregelen zoals MFA of het aantal nodige verwerkersovereenkomsten versus het daadwerkelijk overeengekomen aantal verwerkersovereenkomsten.
5. Professionaliseer risicobeheer en zorg ervoor dat de aantoonbaarheid toeneemt. Het informele handelen kan nadelig uitpakken voor Meppel wanneer zich een incident of calamiteit voordoet. Zorg voor een centraal risicoregister, een vaste maar pragmatische methodiek voor risicobeheer en monitor (rest)risico's regelmatig.

DMC Group
Postbus 928
6200 AX Maastricht
+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl
KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

6. Zorg ervoor dat de jaarlijkse informatiebeveiligings- en toezichtsplannen tenminste ter kennisname gedeeld worden met het college van B&W en de gemeenteraad, zodat zij op de hoogte zijn van de grootste informatiebeveiligingsrisico's van Meppel én de manier waarop zij deze gaat adresseren.

7. Richt het managementsysteem voor informatiebeveiliging aantoonbaar in conform de ISO 27001 zoals de BIO dit vereist. Maak hierbij dankbaar gebruik van de handreikingen en voorbeelddocumenten van de Informatiebeveiligingsdienst. Zorg ervoor dat de governance dusdanig wordt ingericht zodat het college van B&W en de gemeenteraad regelmatig worden geïnformeerd en geconsulteerd.

8. Faciliteer een wachtwoordmanager voor alle medewerkers zodat zij, indien nodig, sterke en unieke logingegevens kunnen genereren, bewaren en eventueel synchroniseren naar verschillende apparaten. Dit draagt bij aan het (her)gebruiken van zwakke logingegevens die mogelijkerwijs makkelijk te raden of te kraken zijn.

9. Inventariseer en leg centraal vast welke applicaties en systemen niet via SSO gekoppeld zijn én identificeer de daaraan verbonden risico's. Bepaal op basis van een risico-afweging of en welke compenserende maatregelen nodig zijn.

10. Ga door met het uitwerken van een herstelplan voor cyberincidenten en -crises. Zorg ervoor dat dit plan voor of na formalisatie getest wordt om vast te stellen of dit plan goed (genoeg) werkt. Tijdens dergelijke testen wordt soms duidelijk dat bepaalde invalshoeken over het hoofd gezien zijn of dat de volgordelijkheid van activiteiten anders moet. Het plan is geen eenmalige exercitie, maar een continu proces waarin telkens verbeteringen worden aangebracht op basis van interne en externe ontwikkelingen en bevindingen van uitgevoerde testen.

11. Zorg ervoor dat er een centraal overzicht is van alle bedrijfsmiddelen die zijn toegekend aan individuen, zoals sleutels, mobiele apparaten en toegangspassen. Dit kan bijvoorbeeld gekoppeld worden aan persoonlijke dossiers bij HRM.

12. Bepaal op basis van een risico-afweging voor welke processen het 4-ogen principe afgedwongen moet worden en richt dit vervolgens zodanig in.

13. Stel formeel afspraken met de gemeente Steenwijkerland vast over de beveiliging van het datacenter, bijvoorbeeld in een Dossier Afspraken en Procedures (DAP). Controleer vervolgens regelmatig om de overeengekomen afspraken adequaat worden nageleefd.

14. Zorg ervoor dat het verwerkingsregister actief bijgehouden wordt, bijvoorbeeld door ieder kwartaal de verantwoordelijken een overzicht te sturen van de bekende verwerkingen met de vraag of dit overzicht juist en compleet is. Zorg voor een feedback-loop op de uitvraag en werk het register continu bij op basis van de ontvangen feedback. Controleer steekproefgewijs de bestaande verwerkingen, tenminste voor de meest gevoelige verwerkingen.

15. Stel vast voor welke informatiesystemen het automatisch afdwingen van de bewaartermijnen van persoonsgegevens niet is afgedwongen en probeer dit alsnog technisch af te

DMC Group
Postbus 928
6200 AX Maastricht
+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl
KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

dwingen. Daar waar dit niet mogelijk is, wordt geadviseerd om dit mee te nemen in de periodieke toezichtsacties.

16. Zorg er tenminste voor dat de afspraken met leveranciers die de belangrijkste verwerkingen van persoonsgegevens uitvoeren regelmatig gecontroleerd worden. Daar waar dit niet lukt vanwege bijvoorbeeld capaciteitsgebrek, wordt geadviseerd om de samenwerking binnen de sector op te zoeken.

17. Stem de toezichtsacties af met Meppel zodat deze aansluiten op de grootste risico's en doelstellingen van Meppel.

2.2 Mensgericht

Dit domein richt zich op het gedrag, bewustzijn en de competenties van medewerkers en bestuurders, inclusief screening, opleiding en duidelijke verantwoordelijkheden. Het is cruciaal omdat mensen vaak de doorslaggevende factor zijn in het voorkomen, veroorzaken, detecteren en reageren op beveiligingsincidenten; goed geïnformeerde en handelingsbekwame medewerkers verkleinen risico's aanzienlijk.

2.2.1 Bevindingen

1. Communicatie over informatiebeveiliging richting medewerkers vindt hoofdzakelijk via intranet plaats.

2. Onderdeel van het indiensttredingsproces is het volgen van een introductiecursus waar informatiebeveiliging een onderdeel van uitmaakt. Binnen drie maanden na indiensttreding moet verplicht aan de basistraining deelgenomen worden. Een score van 55% of hoger wordt als voldoende beschouwd.

3. Gedurende het dienstverband worden medewerkers continu (wekelijks) getraind ten aanzien van informatiebeveiliging (Sir Askalot). Er wordt gerapporteerd over deelname aan de wekelijkse vragen en teammanagers hebben een dashboard voor hun eigen team. Monitoring op individuele medewerkers door de ISO/CISO vindt niet plaats. Medewerkers geven aan deze trainingen niet serieus te nemen en dat ze (te) generiek van aard zijn.

4. Er is geen SMART geformuleerd plan voor het structureel verbeteren van veilig gedrag. De effectiviteit van awareness activiteiten wordt niet gemeten en er zijn geen concrete doelstellingen geformuleerd (KPI/KRI[15]).

5. Medewerkers kunnen integriteitsschendingen (anoniem) aankaarten (conform integriteitsbeleid).

6. Er is geen sprake van een afrekencultuur, men mag fouten maken en voelt zich niet bezwaard om een melding te maken.

[15] Key Performance Indicator / Key Risk Indicator

DMC Group
Postbus 928
6200 AX Maastricht
+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl
KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

7. Meppel onderkent digitale soevereiniteit als risico vanwege de sterke afhankelijk van Microsoft en acteert daarop.
8. Door de hoeveelheid aan WOO-verzoeken, en daarmee de druk op de capaciteit, is merkbaar dat men ervoor kiest om bepaalde zaken niet te documenteren en vast te leggen in het zaaksysteem. Kennis over bepaalde zaken dreigt daarmee onvoldoende gewaarborgd te zijn wanneer iemand bijvoorbeeld vertrekt.
9. Medewerkers laten regelmatig spullen onbeheerd op hun werkplek liggen.
10. Tijdens de introductiedagen voor nieuwe medewerkers is informatiebeveiliging een van de onderwerpen.
11. Alle medewerkers dienen een geldige Verklaring Omtrent het Gedrag (VOG) te overleggen. Jeugdconsulenten en BOA's worden aanvullend gescreend. Het vereiste screeningsniveau is niet per rol of functie uitgewerkt of vastgelegd.
12. Referentiecontroles bij kandidaten worden sporadisch uitgevoerd.
13. Informatiebeveiliging is geen structureel onderwerp in functioneringsgesprekken.
14. Sommige medewerkers spreken elkaar aan op onveilig gedrag, zoals het laten liggen van printjes bij de printer of bij het vergeten te vergrendelen van de werkplek.
15. Sommige medewerkers geven aan dat het melden van incidenten laagdrempeliger zou mogen.
16. Medewerkers zijn zich bewust van hetgeen er van hen verwacht wordt ten aanzien van informatiebeveiliging.
17. Medewerkers ontvangen niet altijd een terugkoppeling op incidenten die zijn gemeld.
18. Medewerkers merken op dat schermen niet altijd vergrendeld worden bij het verlaten van de werkplek.
19. Door Meppel gefaciliteerde systemen sluiten soms minder goed aan op de werkvloer waardoor gewenste of noodzakelijke functionaliteiten beperkt worden en controle achteraf wordt bemoeilijkt. Medewerkers geven aan zich niet gehoord te voelen wanneer issues bij hoger management worden aangekaart.
20. Medewerkers geven aan dat zij onvoldoende getraind worden in het goed kunnen gebruiken van bijvoorbeeld Teams en OneDrive.
21. Medewerkers geven aan dat zij om processen en systemen heenwerken omdat ze niet voldoen aan de behoefte of aanvullende complexiteit introduceren.

DMC Group
Postbus 928
6200 AX Maastricht
+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl
KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

2.2.2 Aanbevelingen

1. Stel een SMART plan of programma vast voor het structureel verbeteren van veilig gedrag, bijvoorbeeld met behulp van Cybersafe Yourself[16]. Bepaal het gewenste doelgedrag en werk dit uit naar meetbare (sub)doelen en bepaal hoe, door wie en wanneer die gemeten moeten worden (KPI/KRI). Verwerk de resultaten van de metingen in verantwoordingsrapportages en stuur daarop.

2. Spits de awareness materialen toe op de beleveniswereld van de doelgroep zodat de herkenbaarheid, bruikbaarheid en adoptie toenemen. Verricht korte evaluatiecycli, bijvoorbeeld iedere 90 dagen, om te bepalen of de beoogde doelstellingen bereikt worden, in welke mate de materialen aansluiten bij de doelgroep én welke verbetermogelijkheden er zijn.

3. Besteed ook aandacht aan de zaken die men moet documenteren en registreren in het zaaksysteem. Maak duidelijk dat het achterwege blijven van documentatie en registratie voor problemen kan zorgen wanneer iemand vertrekt of (externe) verantwoording nodig is.

4. Blijf aandacht schenken aan clean desk en clear screen, met name in ruimten waar bezoekers mogen komen.

5. Overweeg om voor bepaalde functies of rollen aanvullende (pre-employment) screening toe te passen en het periodiek herhalen daarvan. Denk hierbij aan functies of rollen van IT-beheerders en bestuurders, die over het algemeen meer rechten of toegang hebben tot bepaalde middelen. Justis heeft in een brochure uitgewerkt[17] welke integriteitsrisico's er zijn en welke vormen van screening daarbij passen. Maak risicogebaseerd een afweging en pas dit beleid vervolgens consistent toe voor zowel vaste medewerkers als inhuur. Een Verklaring omtrent het gedrag (VOG) heeft een beperkte blik op de historie van een individu, het is daarom raadzaam om dit proces regelmatig te herhalen.

6. Besteed in functioneringsgesprekken ook aandacht aan informatiebeveiliging. Neem hierin bijvoorbeeld de verantwoordelijkheid ten aanzien van informatiebeveiliging, geldende regels en afspraken en eventuele knelpunten die worden ervaren, bewustwording (deelname Sir Askalot en overige activiteiten), leren en ontwikkelen (indien van toepassing) en aanspreekbaarheid. Elke interactie met medewerkers is een kans om het onderwerp onder de aandacht te brengen.

7. Verricht een onderzoek, bijvoorbeeld via een enquête, naar de laagdrempeligheid van de incidentprocedure en stel op basis daarvan vast waar en hoe dit laagdrempeliger kan. Denk bijvoorbeeld een aan meldknop in de e-mail client of op intranet.

8. Zorg ervoor dat melders van incidenten altijd een terugkoppeling ontvangen over de afhandeling van een incidentmelding. Het gaat hierbij niet alleen om de bevestiging dat een melding succesvol is ontvangen en in behandeling werd genomen, maar met name

[16] https://cybersaveyourself.nl/
[17] https://justis.nl/justis/screening-van-personeel

DMC Group
Postbus 928
6200 AX Maastricht
+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl
KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

wat ermee gedaan is en de melders persoonlijk bedanken. Door het uitblijven van een terugkoppeling daalt de meldingsbereidheid.

9. Zorg ervoor dat er regelmatig gesprekken plaatsvinden met de verschillende teams en afdelingen over informatiebeveiliging. Hoe ervaren de medewerkers de beveiligingsmaatregelen of systemen waarmee ze moeten werken? Werkt het naar behoren, zien zij risico's of veranderd het hun gedrag door bepaalde maatregelen of systemen? Het doel is het begrijpen van de behoeften en beleveniswereld van medewerkers. Hierdoor is Meppel (beter) in staat om beveiligingsmaatregelen effectief daarop toe te passen.
10. Train medewerkers in het gebruik van Teams en OneDrive zodat zij in staat zijn deze systemen goed en veilig te gebruiken.

2.3 Fysiek

Dit domein richt zich op de beveiliging van gebouwen, werkplekken, datacenters en fysieke toegang tot systemen en informatie. Dit domein is belangrijk omdat digitale beveiliging niet losstaat van fysieke bescherming: onbevoegde fysieke toegang kan technische maatregelen direct ondermijnen.

2.3.1 Bevindingen

1. Meppel heeft onderzoek laten uitvoeren naar de weerbaarheid tegen fysieke binnendringers (mystery guest).
2. Meppel heeft in haar gemeentehuis noodstroomvoorziening (niet no-break).
3. Meppel gaat het gemeentehuis herinrichten en neemt fysieke (toegangs)beveiliging vanaf de start daarin mee.
4. In de openbare ruimte van het gemeentehuis staan oude archiefkasten en dozen met daarin allerlei informatie. Het is onduidelijk of daar vertrouwelijke en/of privacygevoelige informatie tussen zit. Tijdens de steekproeven werd dit niet als dusdanig geconstateerd.
5. De bezoekersprocedure is ontoereikend.
6. Het gemeentehuis heeft veel grote ramen waardoor het over de schouder meekijken op schermen van medewerkers bij de receptie en burgerzaken mogelijk is ('shoulder surfing').
7. Het cameratoezicht in het gemeentehuis is ontoereikend.
8. Het gemeentehuis is opgedeeld in compartimenten waarvoor autorisatie is vereist om het afgeschermde deel te bereiken (toegangspas).
9. Voor het bedienen van de lift in de openbare ruimte is autorisatie vereist.

DMC Group
Postbus 928
6200 AX Maastricht
+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl
KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

10. Op de tweede en derde verdieping is na kantoortijd compartimentering aangebracht om te voorkomen dat raadsleden toegang hebben tot de afdelingen van de ambtenaren.
11. Voor gevoelige ruimten zoals MER/SER[18] zijn speciale sleutels nodig.
12. Het toegangscontrolesysteem gaat vervangen worden door Salto DESFire waardoor het niet meer vatbaar is voor RFID klonen[19]).
13. Het beheer van fysieke sleutels vindt plaats op de gemeentewerf. Er is geen sleutelplan waaruit blijkt wie welke sleutel heeft (of mag hebben) en hoe daarop gecontroleerd wordt. Er is geen protocol voor verloren of gestolen sleutels.
14. Tijdens de rondleiding werden een aantal keer onbekende sleutels aangetroffen, zoals een sleutel voor een sleutelkluis. Later bleek dat deze sleutel noodzakelijk was voor het Servicepunt wanneer de batterij van een bepaald systeem uitvalt.
15. Tijdens de rondleiding waren op één na alle ruimten die afgesloten zouden moeten zijn, ook afgesloten.
16. In de kelder werden zakken en dozen aangetroffen met daarin kleding voor handhavers. Al het personeel heeft toegang tot de kelder.
17. Tijdens de rondleiding is veilig gedrag geobserveerd, werkplekken waren vergrendeld, er lag geen (gevoelige) informatie bij de printers of op bureaus, niemand liet onbekenden met zich mee lopen, etc.
18. Er zijn geen bakken voor het veilig deponeren van vertrouwelijke informatie, er is wel een rode bak voor papier op de begane grond.

2.3.2 Aanbevelingen

1. Controleer de oude archiefkasten en dozen in de openbare ruimte op vertrouwelijke en/of privacygevoelige informatie en zorg ervoor dat deze informatie wordt opgeruimd of vernietigd.
2. Scherp de procedures rondom bezoekers aan. Verplicht het vooraf aanmelden van bezoek zodat de receptionisten dagelijks een overzicht hebben van het te verwachten bezoek, inclusief wie daar intern voor verantwoordelijk is. Zorg ervoor dat bezoekers gecontroleerd worden op hun identiteit (alleen tonen van officiële identiteitsbewijzen) voordat zij een bezoekersbadge, sleutel of ander toegangsmiddel ontvangen. Zorg ervoor dat bezoekers duidelijk herkenbaar zijn, bezoekersmiddelen nergens toegang tot verlenen en dat bezoekers opgehaald en weggebracht moeten worden door de verantwoordelijke medewerker.

[18] Main Equipment Room / Secondary Equipment Room
[19] Radio-Frequency identification klonen is het kopiëren van de informatie die op een RFID token staat naar een andere token, waardoor een kopie met dezelfde identificatie en rechten ontstaat

DMC Group
Postbus 928
6200 AX Maastricht
+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl
KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

3. Positioneer de bureaus en computerschermen dusdanig dat het over de schouder meekijken onmogelijk of lastig is voor derden. Een alternatieve oplossing kan het plaatsen van privacy screens zijn, waardoor het scherm alleen vanuit een beperkte kijkhoek te zien is.
4. Vernieuw het systeem voor cameratoezicht en verbeter de positionering van de camera's. Zorg ervoor dat er geen blinde vlekken zijn en dat alle in- en uitgangen zijn afgedekt.
5. Overweeg het plaatsen van stevige objecten zoals plantenbakken of paaltjes aan de buitenzijde van de hoofdingang (langs de grote ramen) om te voorkomen dat voertuigen eenvoudig, al dan niet onbewust, naar binnen kunnen rijden.
6. Scherp de procedures rondom het beheer van fysieke sleutels aan. Zorg ervoor dat er een overzicht is van alle sleutels inclusief waar deze voor dienen, waar deze opgeslagen worden, wie ze mag hebben op basis van functie of rol en de uitgifte status. Controleer regelmatig of dit overzicht juist is en of er geen sleutels ontbreken. Overweeg het minimaliseren van het gebruik van fysieke sleutels omdat deze nagemaakt kunnen worden met 3D-printers.
7. Sla de kleding van handhavers afgesloten op omdat dergelijke kleding misbruikt of verkocht kan worden voor criminele doeleinden.
8. Zorg ervoor dat op iedere verdieping tenminste één bak of shredder voor het veilig deponeren van vertrouwelijke papier is.

2.4 Technologisch

Dit domein omvat de technische beveiliging van systemen en netwerken, zoals toegangsbeheer, logging, monitoring, patching en back-ups. Het is essentieel omdat digitale dienstverlening en gegevensbescherming direct afhankelijk zijn van robuuste en actuele IT- en OT-beveiliging.

2.4.1 Bevindingen

1. Security monitoring is intern informeel georganiseerd. Meppel heeft geavanceerde monitoring (SIEM/SOC) ingericht De opvolging van beveiligingsmeldingen buiten kantoortijden is niet formeel georganiseerd.
2. Beveiligingsmeldingen van de Informatiebeveiligingsdienst (IBD)[20] worden automatisch als calls aangemaakt in de IT Service Management (ITSM) oplossing.
3. Meppel monitort niet actief naar uitgelekte inloggegevens, maar ontvangt deze in sommige gevallen via de IBD.
4. Alle slimme apparaten (Internet of Things) zijn gesegmenteerd van de rest van de systemen.

[20] Het sectorale Computer Emergency Response Team (CERT)

DMC Group
Postbus 928
6200 AX Maastricht
+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl
KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

5. Het bijhouden en registreren van technische bedrijfsmiddelen (assets), inclusief eigenschappen zoals locatie, IP-adres, MAC-adres, etc., vindt op verschillende plekken plaats. G-facility wordt gebruikt voor laptops, iPad's en mobiele telefoons en de rest, zoals printers, wordt in een afgeschermde wiki omgeving bijgehouden. Meppel is een transitie naar Microsoft Intune aan het maken. Telefoons worden bijvoorbeeld nog met Airwatch (Workspace One UEM)[21] beheert.
6. Meppel monitort met Icinga[22] haar netwerk op verbonden assets en de beschikbaarheid daarvan.
7. Meppel heeft geen beleid ten aanzien van open source software en hardware, maar geeft aan hier wel rekening mee te houden tijdens inkoop- en aanbestedingstrajecten. Bijvoorbeeld door het onderschrijven van de Common Ground principes[23][24].
8. Meppel heeft geen applicatielijst met alle versienummers beschikbaar.
9. Meppel ondersteunt Bring-Your-Own-Devices (BYOD) en is aan het testen met Mobile Application Management (MAM).
10. Meppel maakt gebruik van Purview[25] om vertrouwelijke en privacygevoelige informatie te identificeren en in de toekomst automatisch te classificeren.
11. Meppel maakt gebruik van SmartLockr[26] voor het veilig uitwisselen van informatie met derden.
12. Meppel heeft een transitie naar de Microsoft Azure cloud gemaakt.
13. De firewall regels zijn niet gekoppeld aan ticketnummers in G-facility, hierdoor is het lastig om te zien waarom bepaalde regels geconfigureerd zijn.
14. Er is geen beleid ten aanzien van firewall regels, in de praktijk worden best practices gevolgd.
15. Meppel hanteert een standaard (CIS benchmark[27]) voor hardening[28] in de Azure omgeving. Een externe partij heeft in het verleden geholpen bij de veilige inrichting van de omgeving. Voor overige systemen en applicaties worden geen hardeningsrichtlijnen toegepast.
16. Meppel heeft op twee locaties een inventarisatie van Operational Technology (OT) gemaakt.

[21] https://www.omnissa.com/products/workspace-one-unified-endpoint-management/
[22] https://icinga.com/
[23] https://commonground.nl/
[24] https://vng.nl/artikelen/common-ground
[25] https://www.microsoft.com/nl-nl/security/business/microsoft-purview
[26] https://www.smartlockr.io/nl/
[27] https://www.cisecurity.org/cis-benchmarks
[28] Niet gebruikte functies in hardware en software uitzetten of weghalen en de rechten van andere functies waar mogelijk beperken. Zo verkleint men het aanvalsoppervlak en daarmee het risico van aanvallen.

DMC Group
Postbus 928
6200 AX Maastricht
+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl
KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

17. Meppel maakt reservekopieën (backup) van de virtuele machines, Centric applicatie en alle Teams omgevingen naar Azure en vervolgens naar ImpossibleCloud. De backups naar Azure zijn incrementeel en vinden dagelijks plaats. Daarnaast worden backups gemaakt van de on-premise infrastructuur naar het datacenter in het gemeentehuis Steenwijkerland. Meppel ziet toe op het slagen en falen van backups en heeft in 2024 een hersteltest uitgevoerd.
18. Meppel heeft specifieke apparaten gecompartimenteerd in virtuele segmenten (VLAN).
19. Meppel heeft poort-gebaseerde Network Access Control (NAC)[29] geïmplementeerd.
20. Het gebruik van een virtueel privaat netwerk (VPN) is alleen op beheerde apparaten mogelijk en dit betreft geen always-on VPN.
21. Kennisoverdracht is ad-hoc gedreven door de waan van de dag, maar Meppel probeert zo goed mogelijk de technische documentatie op de wiki bij te houden en twee beheerders te betrekken bij gesprekken met de leverancier.
22. Meppel heeft scheiding aangebracht tussen reguliere- en beheeraccounts. Meppel heeft de logingegevens van het break-the-glass account veilig in een kluis opgeborgen.
23. De IT-beheerders maken gebruik van een gedeelde wachtwoordkluis waarvan het wachtwoord bekend is bij de beheerders. Dit wachtwoord wordt niet direct geroteerd bij functiewijzigingen of uitdiensttreding.
24. Het gebruik van een Remote Management oplossing vanaf het internet is toegestaan.
25. Gebruikers hebben geen beheerrechten op hun laptop (local admin).
26. De effectiviteit van beveiligingsmaatregelen wordt niet structureel geëvalueerd.
27. Vanuit incidentmanagement wordt met behulp van Power-BI zicht gehouden op het aantal meldingen, doorlooptijden, reactietijden, enzovoort. Het daadwerkelijk rapporteren daarover is beperkt, mede door een gebrek aan details in G-facility.
28. Meppel kan onvoldoende invulling geven aan het realiseren van de gewenste of vastgestelde hersteltijden (RTO). In de jaarlijkse hersteltest wordt vastgesteld wat haalbaar is.
29. De internetverbinding van Meppel is niet redundant uitgevoerd.
30. Het technisch afdwingen van meervoudige authenticatie (MFA) voor vanaf het internet benaderbare applicaties is inconsistent.
31. Meppel faciliteert geen wachtwoordmanagers waardoor men privé wachtwoordmanagers, browser-gebaseerde wachtwoordmanagers of notities gebruikt.

[29] Manier om het een netwerk beter te beveiligen. Dit gebeurt door alleen bekende en geautoriseerde apparaten op het netwerk toe te laten.

DMC Group
Postbus 928
6200 AX Maastricht
+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl
KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

2.4.2 Aanbevelingen

1. Neem een MDR dienst af zodat niet alleen pro-actief gemonitord wordt, maar vooral ook (geautomatiseerd) buiten kantoortijden ingegrepen kan worden op verdacht of ongewenst gedrag. Overweeg aanvullend het plaatsen van een netwerksensor of appliance zodat het (draadloze) netwerkverkeer binnen de reikwijdte van de MDR dienstverlening komt te vallen.
2. Overweeg een subscriptie bij Have I Been Pwned[30] voor in ieder geval het hoofddomein van Meppel, zodat Meppel snel op de hoogte gebracht wordt van nieuw uitgelekte (login)gegevens.
3. Ga door met het centraliseren van het overzicht van assets in Intune zodat er één single point of truth ontstaat. Houdt ook rekening met cloud assets, zoals Azure, en neem deze ook op in Intune.
4. Zorg ervoor dat alle geïnstalleerde applicaties, browser-extensies en Office plugins in kaart gebracht zijn (inclusief versienummers) en gemonitord worden. Zo ontstaat er een actueel overzicht van alle aanwezige software en kan Meppel snel schakelen bij kwetsbaarheden en gericht remediëren.
5. Ga door met het testen rondom MAM, met name vanwege de opkomst van functionaliteiten zoals Microsoft Recall[31] waardoor gevoelige informatie toch uit beveiligde omgevingen kan lekken. Bepaal daarom op basis van een risico-afweging welke informatie(systemen) wel of niet toegankelijk mogen zijn vanaf onbeheerde apparaten.
6. Zorg ervoor dat wijzigingen aan firewall regels onderbouwd, goedgekeurd en centraal gedocumenteerd zijn zodat altijd duidelijk is waar een regel voor dient. Dit kan bijvoorbeeld door het realiseren van een koppeling tussen firewall regels en ticketnummers in G-facility. Controleer (audit) de firewall regels regelmatig om de noodzaak te verifiëren en ongeautoriseerde wijzigingen te detecteren.
7. Controleer tenminste netwerkapparatuur op verbetermogelijkheden om het aanvalsoppervlak verder te verkleinen en voer daar waar mogelijk verbeteringen door[32]. Het is raadzaam om dit regelmatig te controleren omdat updates en upgrades ertoe kunnen leiden dat zaken wijzigen en opnieuw aangepast moeten worden. Pas deze werkwijze risicogebaseerd toe op kritieke hard- en software, zoals servers en laptops. Denk ook aan Powershell.[33]
8. Breng OT-systemen op alle gemeentelijke locaties in kaart, ook als deze niet direct onder de verantwoordelijkheid van IT vallen.

[30] https://haveibeenpwned.com/

[31] Recall is een AI-applicatie die regelmatig screenshots maakt van het systeem, vervolgens worden deze screenshots geanalyseerd en is de content doorzoekbaar. Een eindgebruiker kan vervolgens een zoekopdracht uitvoeren naar iets wat ze eerder hebben gezien, en Recall kan dan laten zien in welke applicatie, bestand of website dat was.

[32] https://ncp.nist.gov/repository

[33] https://learn.microsoft.com/en-us/powershell/scripting/security/overview?view=powershell-7.5

DMC Group
Postbus 928
6200 AX Maastricht
+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl
KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

9. Richt identiteits- en toegangsbeheer (IAM) rolgebaseerd in, verricht regelmatig controles of de autorisaties gekoppeld aan rollen (nog) juist zijn toebedeeld. Probeer daarnaast applicaties te koppelen aan de centrale identiteit provider (Entra ID) met Single-Sign-On (SSO), zodat de toegang geautomatiseerd ingetrokken wordt. Dit verkleint de kans op menselijke fouten waarbij accounts niet (tijdig) opgeruimd of geblokkeerd worden én zorgt voor één centraal overzicht van de digitale toegang tot (informatie)systemen.
10. Pas daar waar mogelijk client isolatie of host isolatie toe zodat apparaten in (virtuele) segmenten niet met andere machines in hetzelfde segment kunnen communiceren (tenzij expliciet toegestaan). Dit bemoeilijkt laterale beweging.
11. Zorg ervoor dat testomgevingen niet direct aan het internet worden ontsloten, tenzij dit noodzakelijk is. Beperk dan in ieder geval de toegang daartoe door bijvoorbeeld geofencing of IP-allowlisting. Testomgevingen kunnen gevoelige informatie bevatten en hebben soms een lager beveiligingsniveau dan productie-omgevingen. Door het verkleinen van het aanvalsoppervlak wordt de kans op misbruik gereduceerd.
12. Blijf aandacht houden voor het bijwerken van technische documentatie zodat de afhankelijkheid van individuen gereduceerd wordt. Reserveer bijvoorbeeld maandelijks ruimte binnen het team om de documentatie bij te werken en stel geautomatiseerde taken in via G-facility.
13. Zorg ervoor dat het wachtwoord van de gedeelde wachtwoordkluis direct geroteerd wordt bij functiewijzigingen of uitdiensttreding van direct betrokken medewerkers.
14. Sta RDP niet direct vanaf het internet toe, aangezien dit een veelvoorkomende aanvalsvector is.
15. Evalueer risicogebaseerd de effectiviteit en dekkingsgraad van beveiligingsmaatregelen, bijvoorbeeld een periodieke controle op de dekkingsgraad van MFA of eindpuntbeveiliging.
16. Dwing MFA voor iBabs af.
17. Zorg ervoor dat er consensus bereikt wordt over de balans tussen gewenste en realiseerbare hersteltijden (RTO). Beoefen regelmatig of de gestelde doeltermijn bereikt kan worden.
18. Overweeg het redundant uitvoeren van de internetverbinding.
19. Overweeg het beschikbaar stellen van wachtwoordmanagers aan alle medewerkers, bijvoorbeeld KeePass of Bitwarden (gratis en open source). Dit helpt medewerkers het genereren van sterke en unieke logingegevens.

2.5 Aanbevelingen gemeenteraad

De gemeenteraad heeft een belangrijke rol ten aanzien van de informatieveiligheid binnen Meppel. De VNG[34] benadrukt dat digitale veiligheid een bestuurlijke verantwoordelijkheid is

[34] https://vng.nl/artikelen/raadgever-digitale-veiligheid

DMC Group
Postbus 928
6200 AX Maastricht
+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl
KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

die niet alleen de ambtelijke organisatie betreft, maar een integraal onderdeel moet zijn van het bestuurlijke werk van de raad. Door als raad het onderwerp regelmatig te agenderen, kaders te stellen, prioriteiten te bepalen, voldoende middelen beschikbaar te stellen en toezicht te houden op hoe Meppel risico's beheerst en incidenten aanpakt, is de raad in staat haar kaderstellende en controlerende taak goed te vervullen. Het doel is het versterken van de (digitale) veiligheid van de gemeentelijke dienstverlening en de weerbaarheid van de gemeente en haar inwoners en ondernemers.

Neem kennis van de beschikbare hulpmiddelen[35][36] zodat u (beter) in staat bent om de juiste accenten te leggen en het gesprek inhoudelijk aan kunt gaan met het college.

Realiseer u dat de ENSIA-verantwoording een beperkt beeld van de realiteit schetst vanwege zelfevaluaties en beperkte onafhankelijke toetsing. Daarnaast richt ENSIA zich vooralsnog uitsluitend op het voldoen in opzet en bestaan aan de BIO-beheersmaatregelen, en niet op de effectieve werking over een langere periode. Zet het onderwerp informatiebeveiliging daarom regelmatig op de agenda en nodig bijvoorbeeld de CISO uit om de raad hierover bij te praten. Dit biedt de raad tevens ook de mogelijkheid om (technische) vragen te stellen.

De Cybersecurity Raad[37] adviseerde in 2018 al om minimaal 10% van het totale IT-budget voor informatiebeveiliging aan te wenden. Sinds 2018 is het cyberdreigingslandschap verergerd en zijn er meer wettelijke eisen in werking getreden. Het is dan ook niet meer dan logisch dat de kosten voor het onderhouden en aanscherpen van de algehele informatiebeveiliging ook toeneemt. Wees uzelf daarvan bewust bij de totstandkoming van de begroting.

[35] https://vng.nl/sites/default/files/2025-04/raadsleden-en-informatiebeveiliging.pdf
[36] https://vng.nl/sites/default/files/2023-04/checklist-raadsleden-digitale-veiligheid.pdf
[37] https://www.cybersecurityraad.nl/documenten/2018/04/01/csr-meerjarenstrategie-2018-2021

DMC Group
Postbus 928
6200 AX Maastricht
+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl
KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

3 Beantwoording onderzoeksvragen

1. Algemene informatieveiligheid

Heeft de gemeente op het gebied van informatieveiligheid de risico's voldoende in kaart gebracht en op basis daarvan beleid geformuleerd?

Meppel heeft stappen ondernomen om risico's op het gebied van informatiebeveiliging in kaart te brengen. Hoewel er een basis gelegd is door het identificeren van kritieke processen en het uitvoeren van Business Impact Analyses, ontbreekt het aan een systematische en volledig geïntegreerde aanpak. Er is sprake van fragmentatie waarbij risicobeheer informeel is georganiseerd en er geen centraal overzicht bestaat van geïdentificeerde risico's, hun eigenschappen en status.

Dit gebrek aan formalisering en integratie heeft consequenties voor de dekkingsgraad en effectiviteit van het beleid en risicobeheersing. Hoewel er een informatiebeveiligingsbeleid is, is niet duidelijk in hoeverre dit beleid expliciet is gebaseerd op een grondige risicoanalyse en of het de geïdentificeerde risico's adequaat adresseert. Daarnaast ontbreekt het aan een systematische controle op verwerkingsactiviteiten en overeenkomsten met leveranciers, wat extra risico's met zich mee kan brengen.

Er is behoefte aan een pro-actieve risicogestuurde aanpak, inclusief een centraal risicoregister, regelmatige risicoanalyses en een duidelijke koppeling tussen geïdentificeerde risico's en het gevoerde beleid. Vanwege de beperkte capaciteit van de security functionarissen is het noodzakelijk dat de primaire verantwoordelijkheid bij de eerste lijn gelegd wordt én dat daar actief op gemonitord en gestuurd wordt door het management.

Hoe wordt de informatieveiligheid binnen de gemeente georganiseerd en welke maatregelen zijn er genomen om de veiligheid van gevoelige gegevens te waarborgen?

Het managementsysteem voor informatiebeveiliging is niet volledig ingericht conform de ISO 27001 en er zijn discrepanties waargenomen tussen het vastgestelde beleid en de werkelijkheid, bijvoorbeeld ten aanzien van de overlegstructuren. Er heerst een informeel karakter waarbij vastlegging en formalisatie achterwege blijven op de werkelijkheid. Met name de 'check' en 'act' fasen van het managementsysteem behoeven een meer systematische aanpak om risico's daadwerkelijk effectief te kunnen beheersen.

Meppel heeft een CISO aangesteld voor 0.5 fte. Daarnaast is er binnen het team I&ID een ISO aangesteld die tevens Privacy Officer (PO) is. De CISO en ISO kunnen elkaars taken overnemen bij verlof of ziekte. De voorgaande PO is beschikbaar als achtervang voor de huidige PO mocht dat nodig zijn. De FG is extern ingehuurd waardoor achtervang via het extern bureau is georganiseerd. In de praktijk valt en staat het managementsysteem met de inzet van de security functionarissen, terwijl zij feitelijk ondersteunend en controlerend dienen te zijn.

Meppel heeft allerlei maatregelen getroffen om de veiligheid van gevoelige gegevens te waarborgen. De relatie tussen risico's en beheersmaatregelen kan explicieter gemaakt worden zodat het controleren en sturen daarop efficiënter en effectiever gemaakt kan worden. Het implementeren van een GRC-tool kan helpen om dit inzichtelijker te maken voor het

DMC Group
Postbus 928
6200 AX Maastricht
+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl
KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

management, maar zou ook zonder een dergelijke tool aan de orde moeten zijn.

Op welke wijze wordt de gemeenteraad geïnformeerd over de risico's en maatregelen? En wat is wenselijk in het delen van dergelijke informatie?

De informatievoorziening aan de gemeenteraad ten aanzien van informatiebeveiliging is niet gedefinieerd. De interactie met de raad is ad-hoc gedreven en de informatievoorziening is beperkt tot jaarverslagen en de ENSIA-verantwoording.

Noot: DMC heeft geen leden van de gemeenteraad gesproken hierover waardoor een eenzijdig beeld geschetst wordt.

In hoeverre voldoet de informatieveiligheid van de gemeente aan de relevante wet- en regelgeving, zoals de Algemene verordening gegevensbescherming (AVG) en de Wet beveiliging netwerk- en informatiesystemen (Wbni)?

Meppel voldoet niet volledig (aantoonbaar) aan de AVG, Cyberbeveiligingswet eisen. Dit wil niet zeggen dat Meppel haar zaken niet op orde heeft of niet goed bezig is. In tegendeel, we hebben goede dingen waargenomen, maar het waarborgen van onderbouwing en bewijslast is uitdagend gebleken. De opvolging van eerdere bevindingen waaruit bleek dat Meppel niet voldeed aan wet- en regelgeving was onvoldoende.

Ten aanzien van de Cyberbeveiligingswet heeft Meppel voornamelijk stappen te zetten op het gebied van risicobeheer en in het algemeen vastlegging en onderbouwing van gemaakte keuzes. Zonder dit is (externe) verantwoording lastig en afhankelijk van individuen.

Welke procedures en beleidsmaatregelen zijn er voor het beheer van gebruiksrechten en toegangscontrole tot kritieke informatiesystemen?

Procedures voor gebruiksrechten en toegangscontrole zijn aanwezig, maar de effectiviteit is onduidelijk. Het is mogelijk dat rechten niet altijd correct zijn toegekend en dat er onbevoegde toegang tot systemen en data is. Regelmatige controles en audits zijn nodig om de effectiviteit van de toegangscontrole te waarborgen. Deze lijken nu voornamelijk te worden uitgevoerd op de systemen waarvoor dit wettelijk vereist is. Daarnaast is de toegang ingericht op basis van attributen en niet op rollen, waardoor de noodzakelijke toegang niet (altijd) eenduidig gedefinieerd en controleerbaar is.

2. Beveiliging van kritische systemen

Welke informatiesystemen worden als 'kritisch' beschouwd voor de werking van de gemeente, en hoe wordt de beveiliging van deze systemen gewaarborgd?

Meppel heeft door het uitvoeren van BIA's bepaalt welke systemen kritisch zijn voor de dienstverlening en continuïteit. Meppel heeft geen beheersmaatregelen gekoppeld aan de classificatieniveaus. Meppel heeft in alle domeinen maatregelen getroffen die gezamenlijk zorgen voor een gelaagde beveiliging. Aan de hand van penetratietesten en mystery guest onderzoeken worden kwetsbaarheden in de beveiliging geïdentificeerd en geremedieerd.

Welke risico's worden er gelopen als de kritische systemen door ongeautoriseerde beïnvloeding van buitenaf uitvallen?

DMC Group
Postbus 928
6200 AX Maastricht
+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl
KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

De teamleiders hebben de opdracht gekregen om continuïteitsplannen op te stellen waarin dit één van de aandachtspunten is. De afhankelijkheden van systemen dienen bepaald te worden met een BIA en vervolgens dient gekeken te worden of de beheersmaatregelen voldoende weerstand bieden tegen uitval door externe beïnvloeding. De hieraan verbonden risico's zijn momenteel niet inzichtelijk, maar dit maakt onderdeel uit van de continuïteitsplannen.

Wat zijn de kwetsbaarheden in de bestaande informatiesystemen die het mogelijk maken om in te breken of ongeautoriseerde toegang te verkrijgen?

In het externe aanvalsoppervlak zijn door de Informatiebeveiligingsdienst regelmatig kwetsbaarheden geconstateerd. Er is geen overzicht van alle technische kwetsbaarheden bekend bij de onderzoekers, maar Meppel laat gespecialiseerde partijen penetratietesten uitvoeren om kwetsbaarheden en aanvalspaden te identificeren. Meppel adresseert de kwetsbaarheden.

Hoe worden de systemen gemonitord op potentiële veiligheidsincidenten en welke mechanismen zijn er voor incidentdetectie en -respons?

Monitoring is onvoldoende en de incidentrespons is niet optimaal en reactief. Dit betekent dat er mogelijk niet tijdig wordt opgemerkt dat er een beveiligingsincident plaatsvindt en dat de schade niet effectief kan worden beperkt.

3. Risicoanalyse en dreigingen

Welke interne en externe dreigingen worden momenteel geanalyseerd en beheerd om inbreuken in informatiesystemen te voorkomen?

Meppel wordt door de Informatiebeveiligingsdienst (IBD) actief geïnformeerd over externe cyberdreigingen en risico's, bijvoorbeeld in het externe aanvalsoppervlak. Intern houdt Meppel toezicht op operationele cyberdreigingen via Microsoft Defender en de incident meldprocedure.

In hoeverre worden risico's zoals social engineering, phishing-aanvallen, malware-infecties en andere vormen van cyberaanvallen in kaart gebracht en tegengegaan?

De risico's van social engineering, phishing en malware worden erkend, maar de bescherming is niet voldoende. Medewerkers zijn mogelijk niet voldoende getraind om deze dreigingen te herkennen en te vermijden. Er is mogelijk behoefte aan aanvullende beveiligingssoftware en procedures om deze dreigingen te bestrijden.

4. Testen van infiltratie

Is er een periodieke penetratietest of red-teaming uitgevoerd om de kwetsbaarheden van de informatiesystemen te identificeren en de effectiviteit van de beveiliging te testen?

Meppel laat gespecialiseerde partijen penetratietesten uitvoeren om kwetsbaarheden en aanvalspaden te identificeren. Meppel adresseert de kwetsbaarheden. Meppel heeft echter geen plan waarin concreet uitgewerkt is wat wanneer op welke wijze door wie gecontroleerd moet worden.

Welke incidenten of beveiligingslekken zijn er in de afgelopen jaren geconstateerd, en

DMC Group
Postbus 928
6200 AX Maastricht
+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl
KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

hoe zijn deze opgelost? Hoe wordt er bijvoorbeeld bij een datalek gecommuniceerd met de mogelijk betrokkenen binnen en buiten de gemeentehuizen?

De afgelopen jaren zijn 93 incidenten waargenomen, waaronder social engineering aanvallen zoals phishing, kwetsbaarheden in hard- en software (via IBD), verloren toegangspassen, schermen niet afgesloten, verstoringen en deuren open laten staan. De technische incidenten zoals malware, poortscans of bruteforce pogingen zijn niet bijgehouden in hetzelfde overzicht. Hierdoor ontstaat een vertekend beeld van de werkelijkheid.

Dit jaar zijn 25 datalekken geregistreerd waarvan het merendeel door menselijk handelen is veroorzaakt. Meppel communiceert datalekken altijd aan betrokkenen, ook wanneer dit niet wettelijk verplicht is. Datalekken worden in G-facility geregistreerd.

5. Opleiding en bewustwording van personeel

Hoe worden medewerkers van de gemeenten opgeleid in het herkennen van beveiligingsrisico's, zoals phishing en social engineering-aanvallen?

Medewerkers worden bewust gemaakt door microlearning, maar de effectiviteit is onduidelijk en wordt niet gemeten (alleen deelname wordt gemeten). De trainingen zijn generiek van aard en worden niet door iedereen even goed ervaren en/of serieus genomen.

Wat is de frequentie en effectiviteit van de trainingen die medewerkers ontvangen met betrekking tot informatieveiligheid?

De frequentie van de bewustwordingsberichten is wekelijks. Regelmatige en interactieve trainingen zijn nodig om de bewustwording van medewerkers te verhogen en hen in staat te stellen om beveiligingsrisico's te herkennen en te vermijden.

6. Beveiliging van gegevens en privacy

Hoe wordt de privacy van persoonsgegevens gewaarborgd binnen de informatiesystemen van de gemeenten?

Het waarborgen van de privacy van personen wordt gewaarborgd door een combinatie van organisatorische-, mensgerichte- en technische maatregelen. Meppel sluit bijvoorbeeld verwerkersovereenkomsten met leveranciers af, voert (pre-)DPIA's uit, houdt toezichtsacties, verricht oorzaakanalyses bij datalekken en past verbeteringen toe naar aanleiding daarvan. Aandachtspunten zijn het bijhouden van het verwerkingsregister, het technisch afdwingen van wettelijke bewaartermijnen, het uitvoeren van DPIA's (al dan niet in samenwerking binnen de sector) en het adequaat opvolgen van eerdere tekortkomingen.

Zijn er gegevensversleuteling en veilige communicatiekanalen voor het uitwisselen van gevoelige informatie?

Meppel past encryptie tijdens transport toe om gevoelige informatie veilig uit te wisselen. Meppel maakt gebruik van een veilig mailen oplossing zodat het veilig kan communiceren met externen.

DMC Group
Postbus 928
6200 AX Maastricht
+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl
KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

7. Incidentmanagement en crisiscommunicatie

Hoe is het incidentmangementproces ingericht voor het geval van een datalek of cyberaanval?

Er is een generiek incidentmanagementproces, maar het ontbreekt aan uitgewerkte incident response plannen voor specifieke incidenten zoals ransomware. Meppel heeft geen retainer afgesloten met een gespecialiseerde derde partij, maar heeft wel financiële middelen gereserveerd voor calamiteiten.

Welke procedures zijn er voor crisiscommunicatie en hoe snel kunnen kwetsbaarheden worden geadresseerd?

Er is een concept crisisplan en sinds drie jaar vinden er crisisoefeningen plaats. Het plan wordt getest op effectieve werking en daar waar nodig bijgesteld. De continuïteitsplannen van de verschillende teams moeten hier ook aan gaan bijdragen, maar die zijn in de maak zoals eerder benoemd.

8. Kosten beveiligingsmaatregelen

Welke eenmalige en structurele kosten worden er gemaakt voor het beheren van risico's op gebied van informatieveiligheid en bescherming kritische processen en hoe verhouden zich die onderling en tot soortgelijke gemeenten?

Niet expliciet uitgevraagd [wordt nagevraagd].

Hoofdvraag

Hoe wordt de informatieveiligheid binnen de gemeente georganiseerd, welke maatregelen zijn er genomen om de veiligheid van gevoelige gegevens te waarborgen, en in hoeverre zijn de kritische processen van de gemeente beschermd tegen infiltratie en ongeautoriseerde toegang?

Meppel heeft een gelaagde beveiliging gerealiseerd bestaande uit een combinatie van organisatorische-, mensgerichte- en technische maatregelen. Ondanks de beperkte capaciteit voor informatiebeveiliging en het informele karakter heeft Meppel laten zien dat zij risico's onderkent en adresseert. De basismaatregelen zijn op orde.

DMC Group
Postbus 928
6200 AX Maastricht
+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl
KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

DMC GROUP
SECURITY MANAGEMENT

A Aangeleverde informatie

```
+---Beleid en Maatregelen
-   +---00 Baseline Informatiebeveiliging Overheid BIO
-   -   -   bio-versie-104zv_def.pdf
-   -   -
-   -   +---01 NEN
-   -   -       NEN27001.PDF
-   -   -       NEN27002.PDF
-   -   -
-   -   +---02 Wetgeving
-   +---01 Informatiebeveiligingsbeleid
-   -   -   Getekend Informatiebeveiligingsbeleid 2023.pdf
-   -   -
-   -   +---01a Informatiebeveiligingsplan
-   -   +---01b Audit & Controleplan Informatiebeveiliging
-   -   +---Archief
-   -   -       bio-versie-104zv_def.pdf
-   -   -       Informatiebeveiligingsbeleid Meppel vanaf 2023__1779821.docx
-   -   -       Jaarplan informatiebeveiliging 2021-2022.pdf
-   -   -
-   -   +---Concepten
-   -           informatiebeveiligingsbeleid aanpassingen vanuit JURA.msg
-   -           Melding met nummer 3104 Afgesloten_.msg
-   -
-   +---02 Ensia
-   -   +---Normering DIGID
-   -   -       Normen ENSIA 2022.pdf
-   -   -       Normering DigiD.txt
-   -   -
-   -   +---Normering SUWINET
-   -           Notitie normerings aspecten SUWINET.txt
-   -
-   +---03 Privacy Beleid
-   -   +---01 Definitief
-   -   -       Privacy beleid gemeente Meppel__1879582__.pdf
-   -   -
-   -   +---02 Concept
-   -   -       20230608-Template-aanvullend-privacybeleid-BIO-V1.2-definitief.docx
-   -   -       Privacybeleid Gemeente Beek.pdf
-   -   -       Privacybeleid Gemeente Meppel 2023-2026 v0.1 opm L2P.docx
-   -   -       Privacybeleid Gemeente Meppel 2023-2026 v0.1.docx
-   -   -       Privacybeleid Gemeente Meppel 2023-2026 v0.2.docx
```


DMC Group
Postbus 928
6200 AX Maastricht
+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl
KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

```
-   -   -
-   -   +---03 Archive
-   -           Privacy Beleid Gemeente Meppel 2020 2023 - Snelkoppeling.lnk
-   -           Privacy Beleid Gemeente Meppel 2020 2023.pdf
-   -
-   +---04 Screenings Beleid
-   -   +---01 Definitief
-   -   -       Vastgesteld Screening Beleid gemeente Meppel versie 1.82.docx
-   -   -       Vastgesteld Screening Beleid gemeente Meppel versie 1.82.pdf
-   -   -
-   -   +---02 Concept
-   -   +---03 Archive
-   -           Adviesaanvraag Ondernemingsraad.docx
-   -           Screening Beleid gemeente Meppel 1.5 met comments van Tineke.docx
-   -           Screening Beleid gemeente Meppel 1.5.docx
-   -           Screening Beleid gemeente Meppel 1.6.docx
-   -           Screening Beleid gemeente Meppel 1.7.docx
-   -           Screening Beleid gemeente Meppel 1.8.docx
-   -           Screening Beleid gemeente Meppel 1.8.pdf
-   -           Screening Beleid gemeente Meppel 1.81.docx
-   -
-   +---05 Toegangs Beleid
-   -   +---01 Defintief
-   -   -       2025_DT - Advies Toegangsbeveiligingsbeleid.docx
-   -   -       2025_DT - Advies Toegangsbeveiligingsbeleid.pdf
-   -   -       2025_Toegangsbeveiligingsbeleid.docx
-   -   -       2025_Toegangsbeveiligingsbeleid.pdf
-   -   -       Fysiek toegangbeleid Meppel 2023.pdf
-   -   -       Voorblad DT-besluit 2025_Toegangsbeveiligingsbeleid.pdf
-   -   -
-   -   +---02 Concept
-   -   -       2024_Logische toegang V1.0.docx
-   -   -
-   -   +---03 Archive
-   -       -   201903-Handreiking-Toegangsbeleid-v2.01.docx
-   -       -   20230322-bio-thema-uitwerking-toegangsbeveiliging-v22-def.pdf
-   -       -   Adviesnota DT Meppel Toegangsbeleid (leeg).docx
-   -       -   Adviesnota DT Meppel Toegangsbeleid.docx
-   -       -   Autorisatiebeleid gemeente Meppel.pdf
-   -       -   Beleid voor logische toegangsbeveiliging.pdf
-   -       -   BS02 adviesnota paslezers.docx
-   -       -   BS02 Beleid logische toegangsbeveiliging gemeente Meppel.docx
-   -       -   Fysiek toegangbeleid Meppel 2022.pdf
-   -       -   Toegangsbeleid versie 0.2.docx
-   -       -
```


DMC Group
Postbus 928
6200 AX Maastricht

+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl

KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

```
-   -       +---01 Fysiek Toegangsbeleid
-   -       -   -   Fysiek toegangbeleid Meppel 2023.pdf
-   -       -   -
-   -       -   +---01 Bijlagen
-   -       +---02 Logisch Toegangsbeleid
-   -           -   2024_Autorisatiebeheer en -controle.docx
-   -           -   2024_Logische toegang V0.4.docx
-   -           -
-   -           +---03 Archive
-   -           -       Toegangsbeleid versie 0.1.docx
-   -           -
-   -           +---04 Bijlagen
-   +---06 Wachtwoord Beleid
-   -   +---01 Definitief
-   -   -       Vastgesteld Wachtwoord Beleid gemeente Meppel versie 1.2.docx
-   -   -
-   -   +---02 Concept
-   -   +---03 Archive
-   +---07 Clear Desk Clear Screen Beleid
-   -   +---01 Definitief
-   -   +---02 Concept
-   -   +---03 Archive
-   -           55e9c2ae9dd7cc15008b8524.jfif
-   -           Clean desk beleid gemeente Meppel v.3.docx
-   -           Clean desk beleid gemeente Meppel v.4.docx
-   -           clean-desk-policy-employees-communication.htm
-   -           Clear_Screen_Clear_Desk.jpg
-   -           deskrisks_thumb.jpg
-   -
-   +---08 Audit en Controle Plan
-   -   +---01 Definitief
-   -   +---02 Concept
-   -   -       Audit- en controleplan 2022 Meppel.pdf
-   -   -
-   -   +---03 Archive
-   -           Audit- en controleplan 2022 Meppel.docx
-   -
-   +---09 Crypto Beleid
-   -   +---01 Definitief
-   -   +---02 Concept
-   -   +---03 Archive
-   +---10 Malware Beleid
-   -   +---01 Defintief
-   -   +---02 Concept
-   -   -       Anti-malware beleid gemeente Meppel v.1.1 Feedback AU.docx
```


DMC Group
Postbus 928
6200 AX Maastricht

+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl

KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

```
-   -   -
-   -   +---03 Archive
-   -   +---04 Informatie IBD
-   -           202002-Handreiking-Anti-malware-beleid-1.2.02 IBD.docx
-   -
-   +---11 Backup Beleid
-   -   +---01 Definitief
-   -   -       Back-up en recovery beleid.pdf
-   -   -       DT advies_Back-up en recovery beleid.pdf
-   -   -
-   -   +---02 Concept
-   -   -       Back-up en Recovery beleid_V0.9.docx
-   -   -
-   -   +---03 Archive
-   -       -   20240617_Bijlagen backup beleid.docx
-   -       -   Back-up en Recovery beleid_V0.1.docx
-   -       -   Back-up en Recovery beleid_V0.2.docx
-   -       -   Back-up en Recovery beleid_V0.3.docx
-   -       -
-   -       +---Bijlagen
-   -               202012-Handreiking-Back-up-en-recovery-gemeente-v2.21 (1).docx
-   -               Gemeente Meppel IDPA TO-Back-up Oplossing Definitief.pdf
-   -               Rapportage restoretest 20220307.docx
-   -               Restoretestplan.docx
-   -
-   +---12 Classificatie Beleid
-   -   +---01 Definitief
-   -   -       Dataclassificatie Beleid Gemeente Meppel__1844402__.pdf
-   -   -       Dossier 1127 voorblad.pdf
-   -   -
-   -   +---02 Concept
-   -   -       Dataclassificatie Beleid Gemeente Meppel - nieuwe huisstijl.docx
-   -   -
-   -   +---03 Archive
-   -   -       20200831-BBN2plus-maatregelen-tbv-gemeenten-BIO-10.4-1.01.xlsx
-   -   -       Dataclassificatie Beleid Gemeente Meppel.docx
-   -   -       Dossier 1127 voorblad.pdf
-   -   -       DT advies dataclassificatiebeleid__1844403__.docx
-   -   -       Kruisje Ensia.msg
-   -   -
-   -   +---04 Handreiking dataclassificatie VNG
-   +---13 Huisregels (leeg)
-   +---14 Change Management
-   -   -   Proces Changemanagement.pdf
-   -   -
```


DMC Group
Postbus 928
6200 AX Maastricht

+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl

KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

```
-   -   +---01 Beleid (definitief, leeg)
-   -   -       stroomschema incident DEF.jpg
-   -   -       Voorbeelden.jpg
-   -   -       Wijzigingenbeheer.pdf
-   -   -       Wijzigingsverzoekformulier.docx
-   -   -
-   -   +---02 Concept
-   -   +---03 Archive
-   +---15 Thuis of Telewerken Beleid
-   -   +---01 Definitief
-   -   +---02 Concept
-   -   -       201908-Handreiking-Telewerkbeleid-v2.12.docx
-   -   -       Concept Telewerk_Hybryde werken.docx
-   -   -
-   -   +---03 Archive
-   -       +---Handreiking IBD
-   -               201902-Handreiking-Telewerkbeleid-v2.0.pdf
-   -
-   +---16 Mobiele Apparaten Beleid
-   -       2025_Beleid voor beheer mobiele apparaten en applicaties_V0.1.docx
-   -
-   +---17 SUWI Beleid en Regelgeving
-   -   +---01 Defintief
-   -   -       Beveiligingsplan en beheerregels Suwinet 2021 1.0 def.pdf
-   -   -
-   -   +---02 Concept
-   -   -       Beveiligingsplan en beheerregels Suwinet 2021 1.0 def.doc
-   -   -
-   -   +---03 Archive
-   -   -       aanwezigheidslijst 15 mei 2018.pdf
-   -   -       aanwezigheidslijst 2018.docx
-   -   -       aanwezigheidslijst suwi.pdf
-   -   -       Aanwezigheidslijst.xlsx
-   -   -       contactpersonen 2017.pdf
-   -   -       Informatiebeveiligingsplan en beheerregels Suwinet 2018.doc
-   -   -       Informatiebeveiligingsplan en beheerregels Suwinet 2020.doc
-   -   -       suwi contactgegevens 2017.pdf
-   -   -       wijzigingsformulier 2017.pdf
-   -   -
-   -   +---04 Normenkaders
-   -   -       Specifiek Suwinet-normenkader Afnemers.1.01.2017.pdf
-   -   -       specifiek-suwinet-normenkader-01_20160906.pdf
-   -   -
-   -   +---05 Overig
-   -           Adviesnota MT Meppel suwibeleid 2018.docx
```


DMC Group
Postbus 928
6200 AX Maastricht

+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl

KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

```
-   -           Informatiebeveiligingsplan en -regels Suwinet.doc
-   -           suwinet 2018.pptx
-   -
-   +---18 Informatieveiligheid Leveranciers (leeg)
-   +---19 Netwerk Beleid (leeg)
-   +---20 Informatie Transport (leeg)
-   +---21 Informatie Beveiliging Management Systeem (ISMS)
-   +---22 SIEM Functionaliteit (leeg)
-   +---23 SOC Functionaliteit (leeg)
-   +---24 Kwetsbaarheden Beheer
-   -   +---Archive
-   -   +---Concept
-   -   -       202112-Handreiking-Patchmanagement-voor-gemeenten-v2.11.docx
-   -   -
-   -   +---Definitief
-   -           Kwetsbaarhedenbeheer (20-08-2024 15_54_22).docx
-   -
-   +---25 Incident Management
-   -   +---Archive
-   -   +---Concept
-   -   -       Incidentmanagement (4).docx
-   -   -
-   -   +---Definitief
-   -           Incidentmanagement (08_26_2025 11_55_31 AM).pdf
-   -           Incidentmanagement (19-08-2024 13_35_28).docx
-   -
-   +---26 Business Continuity Management (BCM)
-   -   +---BCP I&ID
-   -   -   -   201903-Model-Continuiteitsplan_v2.01.docx
-   -   -   -   Adviesnota DT Meppel (leeg).docx
-   -   -   -   Adviesnota DT Meppel BCP I&ID.docx
-   -   -   -   Adviesnota DT Meppel ICB I&ID.docx
-   -   -   -   ICB v0.9.docx
-   -   -   -   Kritisch processen per afdeling.docx
-   -   -   -   Plan van Aanpak BCP.docx
-   -   -   -   Planning ICB.xlsx
-   -   -   -   Teksten voor ICP.docx
-   -   -   -   Uitgangspunten Brainstormsessie.docx
-   -   -   -   Wettelijke termijnen.docx
-   -   -   -   ~$drijfscontinuiteitplan Meppel v0.3.docx
-   -   -   -   ~$TCP v0.5.docx
-   -   -   -
-   -   -   +---AON BCM presentatie
-   -   -   -       Beter vormgeven BCM.PNG
-   -   -   -       Definitie.PNG
```


DMC Group
Postbus 928
6200 AX Maastricht

+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl

KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

```
-   -   -   -       Impactgebieden.PNG
-   -   -   -       Roadmap.PNG
-   -   -   -       uitdagingen.PNG
-   -   -   -
-   -   -   +---Info IBD
-   -   -   -       VDW-Module-4-Mindmap-BCM.pdf
-   -   -   -
-   -   -   +---Oude versies
-   -   -           BCP incl opm.docx
-   -   -           ContinuÛteitsbeleid (I&ID) v0.3.docx
-   -   -           ContinuÛteitsbeleid (I&ID) v0.4.docx
-   -   -           ContinuÛteitsbeleid (I&ID).docx
-   -   -           ContinuÛteitsbeleid (IID) v0.3 AU.docx
-   -   -           ICB v0.7 Feedback.docx
-   -   -           ICB v0.7.docx
-   -   -           ICB v0.8 Feedback MK.docx
-   -   -           ICB v0.8.docx
-   -   -           ICTCB v0.5.docx
-   -   -           ICTCB v0.6.docx
-   -   -           ICTCB v0.7.docx
-   -   -           ICTCP v0.5.docx
-   -   -
-   -   +---Calamiteitenplan Corona
-   -   +---Concept
-   -   +---Rijk gerelateerd
-   -   +---VNG Producten
-   -           20230406 Kaartje in de Meterkast IBD.docx
-   -
-   +---27 Crisis Management (leeg)
-   +---28 Uitwijk Management
-   -       Meppel Site failure test PRODUCTIECLUSTER DEF.docx
-   -       uitwijktest 2022.docx
-   -       uitwijktesten v.2.docx
-   -
-   +---30 Procedure Datalekken
-   -   +---01 Definitief
-   -   -       procedure Datalekken.pdf
-   -   -
-   -   +---02 Concept
-   -   -       Procedure Melden Datalekken.docx
-   -   -
-   -   +---03 Archive
-   +---31 Wijzigingsbeleid
-   -   +---01 Definitief
-   -   -       Wijzigingenbeheer.pdf
```


DMC Group
Postbus 928
6200 AX Maastricht

+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl

KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

```
-   -   -
-   -   +---02 Concept
-   -   -       Wijzigingsbeleid versie 0.1.docx
-   -   -       Wijzigingsbeleid versie 0.2 (feedback Margreet).docx
-   -   -
-   -   +---03 Archief
-   -   +---04 Informatie IBD
-   -           201903-Handreiking-proces-wijzigingsbeheer-v2.02.docx
-   -
-   +---32 Handreiking geheimhoudingsverklaring
-   -       202004-Handreiking-Geheimhoudingsverklaringen_v2.04.docx
-   -       integriteitsverklaring externe medewerkers VNG.docx
-   -       Verklaring geheimhouding -algemeen-.doc
-   -
-   +---33 Handreiking Verwerkersoveenkomst
-   -   -   14102021-Standaard-Verwerkersovereenkomst-v2.4.1.docx
-   -   -
-   -   +---Verwerkersovereenkomst
-   -           Verwerkersovereenkomst (VNG).docx
-   -
-   +---34 Penetratietesten
-   -   +---2022 Pentest
-   -   -   +---Aanvraag pentest
-   -   -   -   +---Formulieren
-   -   -   -   +---Instructies
-   -   -   -   +---Offertes
-   -   -   -       +---BDO Advisory
-   -   -   -       +---Protinus IT B.V
-   -   -   +---Pentest Hybride werken
-   -   -   +---Pentest schade door toegang
-   -   -   +---Rapportage
-   -   +---2023 Pentest
-   -       +---Pentest Wi-Fi
-   +---35 Contactoverzicht
-   -   -   Contactenoverzicht 02-06-2025.docx
-   -   -   Contactenoverzicht 03-06-2025.docx
-   -   -
-   -   +---Archive
-   -           Contactoverzicht 2024.docx
-   -           Contactoverzicht met eerste commentaar van Roelard verwerkt.docx
-   -           Contactoverzicht.docx
-   -
-   +---36 Tekstberichtenbeleid
-   -       Tekstberichtenservice beleid gemeente Meppel.pdf
-   -
```


DMC Group
Postbus 928
6200 AX Maastricht

+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl

KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

```
-   +---37 Teams
-   -   +---Achtergronddocumenten
-   -           Public DPIA Teams OneDrive SharePoint and Azure AD 16 Feb 2022.pdf
-   -           Samenvatting NL - DPIA Teams OneDrive Sharepoint 16 Feb 2022.pdf
-   -
-   +---39 WPG
-   -   +---Archive
-   -   +---Concept
-   -   -       Handboek BOA (concept) Domein I - Snelkoppeling.lnk
-   -   -       Handboek BOA (concept) Domein I.docx
-   -   -
-   -   +---Defintief
-   +---40 Coordinated Vulnerability Disclosure (CVD)
-   -   +---CVD
-   -   -   +---1. Definitief
-   -   -   +---2. Concept
-   -   -   -       CVD Acme Corporation.docx
-   -   -   -       CVD Gemeente Meppel.docx
-   -   -   -       CVD IBD.docx
-   -   -   -       Info NCSC.pdf
-   -   -   -
-   -   -   +---3. Archief
-   -   +---Security.txt
-   +---Afvoer van gegevensdragers
-   -       2025_Hergebruik en afvoer van gegevensdragers.docx
-   -
-   +---Patchmanagement
-           2025_Patchmanagement beleid.docx
-           Patchmanagement (12-03-2025 14_05_57).docx
-
+---Beschrijving uitbestede beheer van OT en IT
-       Beheer IT door team Informatie en Interne Dienstverlening.docx
-
+---Beschrijving van de PDCA-cyclus
-       Heel globaal memo over Memo_Informatiebeveiliging_Gemeente_Meppel.pdf
-       visie op audit & control 2020-2024.pdf
-
+---BIO2 Gap-analyse
-   -   20250820_BIO2-Gap-analyse-versie-1.2_Rekenkameronderzoek 2025 Gemeente Meppel.xlsx
-   -
-   +---Overige ondersteunende documenten
-           BIA 2503.xlsx
-
+---CIS controls IG1 GAP-analyse
-       CIS_Controls_Version_8_MSSW.xlsx
```


DMC Group
Postbus 928
6200 AX Maastricht

+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl

KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

```
-
+---ENSIA-verantwoordingsrapportages en onderbouwende documentatie
-   +---ENSIA2022
-   -       Adviesnota ENSIA zelfevaluatie.pdf
-   -       Adviesnota_College_1732861__1732861__.pdf
-   -       Schermafbeelding 2025-08-19 093813.png
-   -       Tekortkomingen en verbeterplan ENSIA 2022.pdf
-   -
-   +---ENSIA2023
-   -       Bijlage 1 Managementrapportage BRP.pdf
-   -       Bijlage 12 ENSIA Rapportage voor het College.pdf
-   -       Bijlage 13 ENSIA Rapportage voor de Raad.pdf
-   -       Bijlage 15 College voorstel ENSIA 2023.pdf
-   -       Bijlage 2 Managementrapportage Reisdocumenten.pdf
-   -       Bijlage 4 Uittreksel BRP.pdf
-   -       Bijlage 5 Uittreksel Reisdocumenten.pdf
-   -       College voorstel ENSIA 2023.pdf
-   -       DT advies ENSIA 2023.pdf
-   -       PFO (opiniÎrend).pdf
-   -       Schermafbeelding 2025-08-19 095332.png
-   -
-   +---ENSIA2024
-           3249918 Bijlage BRP-rapportage.pdf
-           3249918 Bijlage BRP-uittreksel.pdf
-           3249918 Bijlage Rapportage ENSIA 2024 College.pdf
-           3249918 Bijlage Reisdocumenten-rapportage.pdf
-           3249918 Bijlage Reisdocumenten-uittreksel.pdf
-           College voorstel ENSIA 2024.pdf
-           Informatiememo ENSIA 2024.pdf
-           Schermafbeelding 2025-08-19 103721.png
-
+---Informatiebeveiliging behandeld door het college van B&W of de gemeenteraad
-   +---FG Jaarverslag 2022
-   +---FG toezicht 2024
-   -       Memo FG toezicht.pdf
-   -
-   +---IB Beleid
-   -       B&W voorstel.pdf
-   -       DT advies__1784147__.pdf
-   -       PFO (opiniÎrend).pdf
-   -
-   +---Penetratietesten
-           PFO (opiniÎrend).pdf
-
+---Informatiebeveiliging behandeld door MT en directie
```


DMC Group
Postbus 928
6200 AX Maastricht

+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl

KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

```
-   +---Informatiebeveiligingsplan
-   -   +---2022
-   -   +---2024
-   -   -       DT advies.pdf
-   -   -       Schermafbeelding 2025-08-19 123238.png
-   -   -
-   -   +---2025
-   -       +---Informatiebeveiligingsplan 2025
-   -           +---Oud
-   +---Monitoring & Response
-   -       20230216 Regiosessie Monitoring en Response.pdf
-   -       Behandeling CISO voorstel M&R.png
-   -       DT advies.pdf
-   -       Inkoopstrategie MR v1.0 22022023.pdf
-   -       Toelichting Monitoring en Response.pdf
-   -
-   +---NIS2
-   -       DT informatiememo.pdf
-   -       Impactanalyse NIS2.pdf
-   -       Schermafbeelding NIS2 behandeling.png
-   -       voorgesteld besluit.png
-   -
-   +---Oefenen
-   -       DT advies__1783531__.pdf
-   -       FLYER IBD TableTop DEF drukbestand.pdf
-   -       Schermafbeelding 2025-08-20 082058.png
-   -       vng_agenda_digitale_veiligheid_2020-2024_def_0.pdf
-   -
-   +---Overige stukken formeel behandeld
-   -       Cryptografiebeleid.pdf
-   -
-   +---Rapportages
-   -       DT voorblad Informatiebeveiligingsrapportage T2.pdf
-   -       DT voorblad T1.pdf
-   -       DT _rapportage_T2.pdf
-   -       Informatiebeveiligingsrapportage T1 2024.pdf
-   -       PFO (opiniÎrend).pdf
-   -       Schermafbeelding Behandeling T1.png
-   -       Schermafbeelding Behandeling T2.png
-   -       Schermafbeelding besluiten na behandeling in DT.png
-   -
-   +---Toezichtplannen
-       +---2024
-       -   -   DT advies.pdf
-       -   -   Schermafbeelding 2025-08-19 124150.png
```


DMC Group
Postbus 928
6200 AX Maastricht

+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl

KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

```
-       -   -
-       -   +---Uitvoering (diverse werkbestanden)
-       -       +---Q1
-       -           +---10
-       -           -   +---10.10
-       -           -   -   +---10
-       -           -   +---10.11
-       -           -   -   +---10
-       -           -   +---10.12
-       -           -   -   +---10
-       -           -   +---10.13
-       -           -       +---10
-       -           +---2
-       -           -   +---2.11
-       -           -   +---2.12
-       -           -   +---2.13
-       -           -   +---2.9
-       -           +---8
-       -           -   +---8.10
-       -           -   +---8.11
-       -           +---9
-       -               +---9.10
-       -               +---9.11
-       -               +---9.12
-       -               +---9.13
-       +---2025
-           -   B&W voorstel Toezichtplan 2025.pdf
-           -   DT advies (1).pdf
-           -   PFO (opiniÎrend).pdf
-           -   Schermafbeelding 2025-08-19 123930.png
-           -   Toezichtplan 2025.pdf
-           -
-           +---UItvoering Diverse Werkbestanden
+---Overige documentatie
-       BIA 2503.xlsx
-       Dataclassificatie applicaties Meppel (1).xlsx
-       Gemeente Meppel - HLD Azure Landingzone v1.0.pdf
-       ML 2023 - (getekend).pdf
-       ML 2024 - definitief, 1 management.pdf
-       personeelshandboek.htm
-       visie op audit & control 2020-2024.pdf
-
+---Resultaten van technische onderzoeken
-   +---Pentest2023
-   -       Analyse en Advies I&ID over pentest 2022Q4.pdf
```


DMC Group
Postbus 928
6200 AX Maastricht

+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl

KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

```
-   -       PFO (opiniÎrend).pdf
-   -
-   +---Pentest2024
-   -       Gemeente-Meppel-Nieuwe-werplek-concept-RAPPORT.pdf
-   -       Gemeente-Meppel-Nieuwe-werplek-concept-RAPPORT.xlsx
-   -
-   +---Pentest2025
-   -   -   Rapportage Vishing Gemeente Meppel 14 juli 2025.pdf
-   -   -
-   -   +---Publieke Website Meppel.nl
-   -           20250630 DBA-YARD Pentest Meppel v1.0s.pdf
-   -           FW Penetratietest omgevingen Meppel.txt
-   -
-   +---Rapportages Oefeningen
-           20231019 Gemeente Meppel Ext (datum voorblad onjuist).pdf
-           2025_GemeenteMeppel_Cyber Crisis Exercise_v0.9.pdf
-
+---Status van het externe aanvalsoppervlak (Darktrace EASM)

Aanvullende informatie n.a.v. interviews:

Awaretrain bewustwordingstraining printscreen.docx
Bewustwording 2024.xlsx
Bewustwording 2025.xlsx
datalek van paar weken terug.msg
Rapport Datalekken meldformulier_17-4-2025 12.08.05.pdf
rapportage brief (jeugd) verkeerde adres.docx
Screenshot agenda afspraak.docx


__
```


DMC Group
Postbus 928
6200 AX Maastricht

+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl

KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group

DMC GROUP
SECURITY MANAGEMENT

B Interviews

- Teammanager Duurzaam
- Informatie architect
- Directeur bedrijfsvoering
- Applicatiebeheer
- Facilitair/gebouwbeheer
- ICT medewerker
- Sociaal ecograaf
- Functionaris Gegevensbescherming (FG)
- Medewerker
- Medewerker
- Manager I&ID/CIO
- Privacy Officer / Information Security Officer (PO/ISO)
- Chief Information Security Officer (CISO)
- HR-adviseur
- Beleidsadviseur

DMC Group
Postbus 928
6200 AX Maastricht

+31 (0)43 7370077
info@dmcgroup.nl
www.dmcgroup.nl

KvK nr.: 71797475
BTW nr.: NL858853322B01
IBAN: NL84 RABO 0330 2884 90 t.n.v. DMC Group