Rekenkameronderzoek informatiebeveiliging

Gemeente Westerveld

DMC GROUP
SECURITY MANAGEMENT

Documentbeheer

Opdrachtgever
Rekenkamer Westerveld

Versie
v1.0

Datum
21 juni 2026

Auteur(s)
drs. Chris Deben MBA CISM
Youri Lammerts MSc. CISM CISA CISSP CIPM CIPP/e
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 Westerveld 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 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 Westerveld 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. 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.

Westerveld 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.

Westerveld 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. Ken aan elke actie een actiehouder toe en stuur op opvolging.

[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.

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

Aanbevelingen aan de gemeenteraad

De gemeenteraad heeft een belangrijke rol ten aanzien van de informatieveiligheid binnen Westerveld. 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, kaders te stellen, prioriteiten te bepalen, voldoende middelen beschikbaar te stellen en toezicht te houden op hoe Westerveld 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 Westerveld 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[6] 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[7] 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.

[3] https://vng.nl/artikelen/raadgever-digitale-veiligheid
[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://ensia.nl/wat-is-ensia/
[7] 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 18

2.4 Technologisch 20

2.5 Aanbevelingen gemeenteraad 22

3 Beantwoording onderzoeksvragen **24**

A Aangeleverde informatie **29**

B Interviews **33**

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

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 [8] benadrukt dat ransomware[9], datalekken[10] 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[11] 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[12] 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.

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

[9] 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.

[10] 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.

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

[12] 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 Westerveld 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 Westerveld 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 Baseline Informatiebeveiliging Overheid - versie 2 (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).[13]

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 een twintigtal 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

[13] 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 is informatie en zijn 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

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. Westerveld heeft een fulltime Chief Information Security Officer (CISO) aangesteld. Er zijn geen (Technical) Information Security Officers ((T)ISO), waardoor de CISO werkzaamheden op strategisch, tactisch en operationeel niveau uitvoert. Westerveld is voornemens om de ISO en CISO rollen uit elkaar te trekken. De CISO vervult aanvullend de rollen ENSIA-coördinator[14] en Security Officer Suwinet.
2. Er is geen structureel overleg tussen de CISO en domeinen zoals HRM en Facilitair.
3. De CISO-rol is vastgelegd in een functieprofiel. De CISO heeft het mandaat om indien nodig in te grijpen bij incidenten.
4. Westerveld heeft 0.7 fte Privacy Officer (PO) aangesteld en de Functionaris Gegevensbescherming (FG) is ingehuurd.
5. De CISO, PO en FG zijn hiërarchisch gepositioneerd onder de concern controller maar hebben een directie lijn naar de directeur.
6. Voor informatiebeveiliging en privacybescherming is een jaarplan vastgesteld. Over de voortgang wordt niet tussentijds gerapporteerd.
7. Voor privacybescherming worden ieder kwartaal toezichtsacties uitgevoerd.
8. Westerveld heeft een achterstand opgebouwd ten aanzien van het uitvoeren van gegevenseffectbeoordeling (DPIA's) en verwerkersovereenkomsten.[15]
9. Er zijn in 2025 20 datalekken en incidenten geregistreerd, waarvan een beperkt deel aan de Autoriteit Persoonsgegevens (AP) gemeld moest worden. De voornaamste oorzaken van deze incidenten waren menselijk handelen.
10. Het waarborgen van informatiebeveiliging en privacybescherming in gemeentelijke projecten is procesmatig niet afgedwongen, maar lukt in de praktijk steeds beter door overleggen tussen het team privacy en informatiemanagement die projecten in portefeuille hebben.
11. Het bijhouden van het register van verwerkingen gebeurt niet structureel, maar is recent voorgelegd aan teamleiders ter controle. Er is in het register een koppeling gemaakt tussen verwerkingen van persoonsgegevens en applicaties/systemen.
12. Westerveld heeft een Governance, Risk & Compliance (GRC) tool geïmplementeerd en maakt hier beperkt gebruik van (ten behoeve van de ENSIA-verantwoording).

[14] Gemeenten verantwoorden zich over informatiebeveiliging en informatiekwaliteit middels ENSIA. Dat staat voor Eenduidige Normatiek Single Information Audit. De focus van ENSIA ligt op verantwoording richting de gemeenteraad, het hoogste politieke orgaan van de gemeente. Parallel hieraan leggen gemeenten verantwoording af aan de rijksoverheid waar het gaat om het gebruik van landelijke voorzieningen. https://ensia.nl/wat-is-ensia/

[15] Een verplichte overeenkomst tussen de verwerkingsverantwoordelijke en verwerker die hun onderlinge afspraken over de verwerking van persoonsgegevens regelt.

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

13. Westerveld is zoekende hoe ze vanuit het oogpunt van informatiebeveiliging regie moet voeren op ONS (partner-leverancier dilemma).[16] De demandmanager is het aanspreekpunt voor de technische dienstverlening vanuit SSC-Ons.
14. Westerveld heeft een Service Level Agreement (SLA) en Dossier Afspraken en Procedures (DAP) met SSC-Ons afgesloten.
15. SSC-Ons stelt een dashboard voor beveiligingsincidenten beschikbaar en de CISO kan daarbij. SSC-Ons voert oorzaakanalyses en doet verslag van majeure incidenten.
16. SSC-Ons heeft voor de HRM-dienstverlening een ISAE3402[17] verklaring en is een traject gestart voor een ISAE3000[18] verklaring.
17. SSC-Ons beschikt over een aantal architecten (werkplek, cloud en enterprise).
18. SSC-Ons bepaalt zelf het technisch beveiligingsbeleid.
19. Westerveld valt onder een andere veiligheidsregio en de samenwerking met SSC-Ons is voornamelijk gericht op de provincie Overijssel, in de praktijk kan dat een risico vormen voor Westerveld.
20. SSC-Ons heeft een security team bestaande uit een CISO, twee TISO's en meerdere OSO's (Operational Security Officer).
21. De informatiemanagers voeren portfolio-overleg met SSC-Ons en de input komt vanuit de teamleiders van Westerveld. Projecten bij Westerveld en SSC-Ons worden op deze manier op elkaar afgestemd.
22. In het Bedrijfsvoeringsberaad (BVB) wordt besproken welke risico's in het SSC-Ons samenwerkingsverband (on)acceptabel zijn waarmee de risicobereidheid deels wordt bepaald.
23. Sporadisch worden wijzigingen door SSC-Ons zonder afstemming of communicatie doorgevoerd, waardoor Westerveld hinder ondervindt. In het wijzigingsproces van SSC-Ons wordt de CISO niet door SSC-Ons geïnformeerd.
24. De burgemeester is portefeuillehouder informatiebeveiliging.
25. Westerveld kent een informele organisatiecultuur, waarbij de toegang tot het (senior) management laagdrempelig is. Zo spreken de CISO en gemeentesecretaris elkaar wekelijks.
26. De interactie met de gemeentesecretaris en burgemeester over informatiebeveiliging vindt op ad-hoc basis plaats.

[16] Het Shared Service Center (SSC) Ons levert bedrijfsvoeringsoplossing aan overheidsorganisaties in de regio Zwolle, zoals ICT, Inkoop & Contractmanagement en HR. https://www.ssc-ons.nl/

[17] ISAE 3402 is een internationale standaard voor het auditen van interne controles bij serviceorganisaties

[18] Het ISAE 3000 / SOC 2-rapport geeft zekerheid dat uitbestede processen op het gebied van informatiebeveiliging en niet-financiële dienstverlening aantoonbaar betrouwbaar en goed ingericht zijn.

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. De interactie met het Managementteam (MT) over informatiebeveiliging is ad-hoc gedreven.
28. Het borgen en uitdragen van verantwoordelijkheden ten aanzien van informatiebeveiliging door verantwoordelijken (eerste lijn) is uitdagend. Bijvoorbeeld het koppelen van verantwoordelijken aan informatie en het classificeren van de informatie.
29. Er is naar aanleiding van een GAP-analyse op de Cyberbeveiligingswet (NIS2) een werkgroep ingesteld.
30. De CISO neemt deel aan het Drents CISO-overleg en de Privacy Officer (PO) aan het Drents PO/FG overleg.
31. Het onderwerp informatiebeveiliging komt regelmatig aan de orde tijdens de maandelijkse informatiebijeenkomsten voor medewerkers. Hier worden bijvoorbeeld recente incidenten met elkaar besproken.
32. Verantwoording over informatiebeveiliging is beperkt tot de verplichte elementen zoals ENSIA, Planning & Control (P&C) cyclus en de jaarrekening.
33. Westerveld handelt voornamelijk compliance georiënteerd en richt zich op hetgeen wettelijk verplicht is en extern gecontroleerd wordt.
34. Risicobeheer ten aanzien van informatiebeveiliging is informeel georganiseerd en er is geen overzicht van beveiligingsrisico's.
35. Er zijn geen SMART[19] doelstellingen voor informatiebeveiliging vastgesteld.
36. De 'check' en 'act' fasen van het managementsysteem voor informatiebeveiliging worden niet conform ISO 27001 uitgevoerd. Er wordt geen verantwoording over informatiebeveiliging afgelegd daar waar dit niet wettelijk verplicht is (zoals ENSIA).
37. De CISO houdt een overzicht van alle autorisaties bij en controleert deze ieder kwartaal. De bevindingen worden gedeeld met teamleiders.
38. De gemeentelijke kritieke processen en -systemen zijn niet expliciet vastgesteld.
39. De (onderlinge) afhankelijkheden van de IT-infrastructuur, in beheer bij SSC-Ons, zijn onduidelijk. SSC-Ons voert het technisch (applicatie)beheer uit en Westerveld het functioneel beheer.
40. Er is geen volledig beeld van decentrale applicaties (applicaties die niet door Westerveld of SSC-Ons gefaciliteerd worden).
41. De formele verantwoording over informatiebeveiliging door SSC-Ons aan Westerveld ontbreekt.
42. Er is geen consensus tussen de CISO's/gemeenten die gebruik maken van SSC-Ons over de speerpunten ten aanzien van informatiebeveiliging.

[19] Specifiek, Meetbaar, Acceptabel, Realistisch, Tijdgebonden

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. Identiteiten voor nieuwe accounts worden via een IT Service Management (ITSM) tool aangevraagd door teamleiders.

44. De digitale toegang is niet ingericht op basis van rollen, maar op basis van attributen. Teamleiders moeten aanvinken voor welke applicaties iemand toegang nodig heeft.

45. Voor het merendeel van de applicaties is geen vastgestelde autorisatiematrix waardoor het onduidelijk is wie welke rechten mag hebben op basis van functie of rol.

46. SSC-Ons levert overzichten van inactieve of vertrokken medewerkers aan voor autorisatie controles. De accounts worden niet automatisch geblokkeerd.

47. SSC-Ons werkt aan een oplossing om het autorisatiebeheerproces te verbeteren (Identity & Access Management (IAM)). Een uitkomst hiervan moet bijvoorbeeld zijn dat er referentieprofielen ontstaan.

48. Datalekken kunnen gemeld worden via een meldknop op het intranet, waarbij de Privacy Officer (PO) en Functionaris Gegevensbescherming (FG) betrokken worden. Vastlegging hiervan vindt plaats in het zaaksysteem.

49. Beveiligingsincidenten worden via de ITSM tool gemeld en doorgezet naar de juiste behandelgroep (door de servicedesk van SSC-Ons).

50. Een overzicht van beveiligingsincidenten wordt bijgehouden in Excel en trendanalyses worden daarop uitgevoerd. Dit geldt niet voor de technische (bijna) incidenten die door SSC-Ons worden geregistreerd/gemeld.

51. Oorzaakanalyses van beveiligingsincidenten worden door Westerveld niet consequent en aantoonbaar uitgevoerd.

52. Bij grootschalige incidenten worden de demandmanger, het MT en de CISO via een chatgroep geïnformeerd.

53. Terugkerende operationele incidenten worden besproken met SSC-Ons om verdere herhaling te voorkomen.

54. SSC-Ons voert niet consequent, al dan niet in samenwerking met Westerveld, impactanalyses en evaluaties van technische wijzigingen uit.

55. Er is geen herstelprioriteit en herstelplan gedefinieerd voor de gemeentelijke systemen (door SSC-Ons).

56. SSC-Ons levert een dashboard waarin de servicelevels gemonitord kunnen worden. Echter door het ontbreken van handhavingsmiddelen wordt daar beperkt/niet op gestuurd.

57. Westerveld neemt deel aan het partneroverleg met SSC-Ons waarin strategische en tactische keuzes gemaakt en afgestemd worden. Een vertegenwoordiging van alle partners en SSC-Ons nemen hieraan deel.

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

58. De afhankelijkheid van individuen ten aanzien van informatiebeveiliging is hoog (single points of failure). Kennis en kunde is niet breed aanwezig en achtervang is niet altijd gerealiseerd.
59. Functioneel beheer heeft onvoldoende inzicht in de backup en uitwijkprocessen bij SSC-Ons.
60. Westerveld en SSC-Ons hebben beide crisisplannen, maar oefenen separaat.
61. Er zijn geen draaiboeken om de continuïteit van kritieke processen te garanderen.
62. Naleving van afspraken met leveranciers worden onvoldoende gecontroleerd.

2.1.2 Aanbevelingen

1. Voeg de status ten opzichte van de Cyberbeveiligingswet (en overige cybersecurity wetgeving) toe aan het jaarverslag.
2. Stem continuïteitsplannen af met SSC-Ons en verricht samen crisisoefeningen om de effectiviteit en doeltreffendheid daarvan vast te stellen. Identificeer verbetermogelijkheden en voer die op basis van de evaluatie door.
3. Ga met SSC-Ons in gesprek over het verbeteren van de onderlinge communicatie en informatievoorziening met betrekking tot (bijna) incidenten, wijzigingen en overige ontwikkelingen.
4. Zorg ervoor dat er structureel overleggen plaatsvinden met de verschillende ondersteunende domeinen over informatiebeveiliging (HRM, Facilitair, ICT).
5. Richt het managementsysteem voor informatiebeveiliging in conform ISO 27001 en besteed voornamelijk aandacht aan het aanscherpen van de check en act fasen. Dit omvat ook het tussentijds afleggen van verantwoording over informatiebeveiliging in bredere zin en het professionaliseren van risicobeheer. Zorg ervoor dat de teamleiders (eerste lijn) bekend zijn met hun verantwoordelijkheden en goed aangestuurd en ondersteund worden bij het uitoefenen daarvan. Maak nadrukkelijker gebruik van de GRC-tool ter ondersteuning van deze processen.
6. Werk de achterstand ten aanzien van DPIA's en verwerkersovereenkomsten risicogebaseerd weg. Overweeg nauwere samenwerking in de regio of het tijdelijk inhuren van extra capaciteit.
7. Dwing procesmatig af dat informatiebeveiliging en privacybescherming vanaf de start worden meegenomen in projecten, dat er tussentijdse verantwoording plaatsvindt en dat er decharge door de security en privacy functionarissen wordt afgegeven.
8. Leg ten aanzien van het regievoeren op SSC-Ons de nadruk op de belangrijkste beveiligingsrisico's voor Westerveld en zoek daar de samenwerking meer in op. Het Bedrijfsvoeringsberaad is het gremium waar dit op strategisch niveau behandeld kan worden. SSC-Ons staat open voor het meewerken en -denken aan specifieke

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

verantwoordingsrapportages die Westerveld kunnen helpen risico's adequaat te beheersen. Blijf daarnaast kritisch op SSC-Ons en verlang transparantie over technische kwetsbaarheden en misconfiguraties en de opvolging daarvan.

9. Blijf met SSC-Ons als partner in gesprek over incidentele afwijkingen van processen en procedures, zoals ongewenste of impactvolle wijzigingen. Zorg ervoor dat de oorzaken daarvan achterhaald en opgelost worden om herhaling te voorkomen. Spreek af hoe de impact bepaald en gecommuniceerd wordt.
10. Zet het onderwerp informatiebeveiliging regelmatig op de agenda van het MT zodat het onderwerp op tactisch niveau meer gaat leven. Nodig de CISO vaker uit om zaken toe te lichten en om vragen te stellen.
11. Stel de kritieke systemen en -processen formeel vast zodat er consensus is over de te beschermen belangen. Dit is ook van belang voor SSC-Ons zodat zij weten wat de herstelprioriteit is ten tijde van calamiteiten.
12. Ga door met de samenwerking met SSC-Ons om te komen tot referentieprofielen waarmee de toegang op basis van rollen ingericht kan gaan worden. Dit verkleint de kans op fouten en ongeautoriseerde toegang.
13. Zorg voor een integraal overzicht van beveiligingsincidenten in plaats van versplinterde overzichten. Dit geeft een vertekend beeld van de werkelijkheid en bemoeilijkt trendanalyses en verantwoording. Zorg ervoor dat oorzaakanalyses altijd uitgevoerd worden en de uitkomsten daarvan gebruikt worden om maatregelen of activiteiten ten behoeve van veilig gedrag aan te scherpen.
14. Probeer de bekende single points of failure te elimineren door kennis te documenteren, taken te rouleren of in regio backup voorzieningen te treffen.
15. Stel draaiboeken op om de kritieke processen en -systemen te continueren ten tijde van een crisis. Oefen deze draaiboeken vervolgens in samenwerking met SSC-Ons.
16. Classificeer leveranciers en pas risicogebaseerd controlemechanismen toe om informatiebeveiliging in de keten te waarborgen. Denk hierbij aan het periodiek opvragen van audit- en pentestresultaten, het voeren van SLA-gesprekken, enzovoort.

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.

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

2.2.1 Bevindingen

1. Nieuwe medewerkers krijgen tijdens hun introductie een algemene training over informatiebeveiliging en privacybescherming. Medewerkers vinden dit belangrijk.
2. Westerveld heeft een leerplatform ter beschikking gesteld voor informatiebeveiliging, maar deelname is vrijwillig (managementbesluit).
3. Er zijn geen specifieke trainingen voor informatiebeveiliging die aansluiten op de verantwoordelijkheden en beleveniswereld van medewerkers.
4. Wachtwoorden worden soms op papier of in digitale notities bewaard.
5. Voor bepaalde functies en/of rollen dient bij indiensttreding een geldige Verklaring omtrent het Gedrag (VOG) overlegd te worden. Dit proces wordt niet herhaald. In gezamenlijkheid met de SSC-Ons partners en een interne collega van openbare orde en veiligheid is gesproken om dit op termijn anders in te richten. Ook wordt er gesproken om bijvoorbeeld periodiek (eens per 3 jaar) de medewerkers een nieuw VOG te laten aanvragen.
6. Medewerkers in vaste dienst leggen de eed of belofte af.
7. Externen ondertekenen een geheimhoudingsverklaring.
8. Er is een personeelshandboek inclusief app waarin men meer informatie kan vinden.
9. Twee keer per jaar wordt er door de CISO een informatiesessie georganiseerd.
10. Er vindt door Westerveld geen toezicht plaats richting SSC-Ons en de leverancier van het HR-systeem ten aanzien van informatiebeveiliging en privacybescherming.
11. Medewerkers zijn zich bewust van de risico's en weten welk gedrag er van hen wordt verwacht, zoals het vergrendelen van schermen, printjes niet laten liggen, bezoekers begeleiden, etc.
12. Gevoelige informatie wordt niet zomaar per telefoon of e-mail verstrekt, maar per post naar het bekende woonadres verzonden.
13. Medewerkers geven aan dat het onderwerp niet structureel wordt behandeld in teams en dat zij onvoldoende op de hoogte zijn van (beleids)afspraken omtrent informatiebeveiliging. Ook weten zij niet allemaal waar of bij wie ze informatie over dit onderwerp kunnen krijgen. Ze geven aan behoefte te hebben aan meer structurele aandacht, heldere communicatie en zichtbare ondersteuning op dit onderwerp.
14. Medewerkers geven aan dat de compartimentering ook nadelig kan uitpakken, bijvoorbeeld wanneer verschillende teams niet van elkaar weten dat ze aan een casus werken voor dezelfde persoon.
15. Door een hoog verloop van personeel is het borgen van zaken uitdagend.

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. Leg de rollen, taken, verantwoordelijkheden en bevoegdheden ten aanzien van informatiebeveiliging duidelijk vast en communiceer ze, bijvoorbeeld voor functioneel beheerders.
2. Zet een doelgroep gericht programma op waarin kennis en kunde ten aanzien van informatiebeveiliging en privacybescherming wordt toegespitst op de beleveniswereld van de doelgroep. Zorg voor een drempelwaarde van deelname (bijvoorbeeld 80%).
3. Blijf periodiek rondes maken om onveilig gedrag te constateren en gebruik die praktijkvoorbeelden om medewerkers hiervoor te behoeden. Geef ze instructies hoe ze vergelijkbare situaties veilig kunnen afhandelen en leg uit waar ze terecht kunnen voor vragen en meer informatie.
4. Overweeg om voor bepaalde (vertrouwens)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[20] 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.
5. Zorg ervoor dat het onderwerp informatiebeveiliging geen feestje van de CISO is, maar een integraal onderdeel uitmaakt van iedere managementverantwoordelijke. Zet het onderwerp regelmatig op de agenda, nodig de CISO uit, en geef collega's de mogelijkheid om praktijkgerichte vragen te stellen of zorgen aan te kaarten.
6. Denk na over manieren om andere teams of afdelingen te informeren over lopende zaken bij inwoners en bedrijven zonder direct de details te delen. Bijvoorbeeld door het plaatsen van een vlaggetje in een systeem of applicatie zodat anderen weten dat er iets speelt.

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. Het beheren van de toegangspassen is grotendeels handmatig georganiseerd. Het retourneren van uitgegeven toegangspassen verloopt niet altijd goed, maar de fysieke

[20] 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

toegang wordt bij uitdiensttreding direct geblokkeerd. Medewerkers met een tijdelijke aanstelling krijgen een einddatum waarna de toegang automatisch geblokkeerd wordt.

2. De toegangsrechten worden ieder kwartaal gecontroleerd en indien nodig gecorrigeerd.
3. Bezoekers, medewerkers en externen worden onderscheiden op basis van hun rol. Op basis van een deurenprotocol is bepaald wie waar toegang tot mag hebben.
4. De identiteit van personen wordt niet structureel gecontroleerd bij het ophalen van toegangspassen (bijvoorbeeld wanneer die vergeten is).
5. Er vindt geen alarmering plaats wanneer iemand een ruimte probeert te betreden waarvoor hij of zij geen rechten heeft. Het gebruik van de toegangspassen wordt vastgelegd in digitale logboeken.
6. De kluisruimte wordt na 18:00 uur automatisch door een alarm beveiligd. Meldingen komen bij een beheerder terecht, ook buiten kantoortijden.
7. Het beheren van de camerasystemen berust bij Westerveld, de verbindingen verlopen wel via SSC-Ons.
8. Bezoekers worden alleen geregistreerd wanneer zij een bezoekerspas ontvangen. Aan het eind van de werkdag wordt gecontroleerd of alle bezoekerspassen geretourneerd zijn. Indien een pas ontbreekt wordt deze geblokkeerd door de beheerder (dit gebeurt automatisch na 17:00 uur).
9. Er is geen volledig overzicht van alle bezoekers die het pand verlaten.
10. Een selecte groep medewerkers beschikt over een noodsleutel. Deze sleutels zijn niet officieel geregistreerd en de beheerder weet aan wie deze zijn uitgegeven.
11. Het gebruik van de noodsleutels buiten kantoortijd triggert een alarm dat alleen uitgeschakeld kan worden met een persoonlijke pincode in combinatie met een tag.
12. Iedere medewerker beschikt over een eigen code, deze code wijzigt niet.
13. Westerveld heeft de weerbaarheid tegen fysieke indringers onafhankelijk laten toetsen (mystery guest).
14. Fysieke (toegangs)beveiliging is geen vast onderdeel in het introductieprogramma voor nieuwe medewerkers.
15. Medewerkers kunnen een locker aanvragen om hun persoonlijke eigendommen veilig op te bergen.
16. Bij de personeelsingang is geen direct toezicht op wie het pand betreed. Er is wel cameratoezicht dat via de balie te volgen is. Tijdens het bezoek is het gelukt om met een medewerker mee naar binnen te lopen via de personeelsingang.
17. Er is geen protocol voor het omgaan met verdachte pakketten of bommeldingen.

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

18. Vertrouwelijke documenten worden verzameld in afgesloten containers die vervolgens opgehaald worden door een gecertificeerd vernietigingsbedrijf.
19. Er zijn maatregelen getroffen tegen inbraak, zoals bewegingsmelders.
20. Het pand is verhoogd ten opzichte van het straatniveau en er zijn palen geplaatst voor de ingang.
21. Buiten het pand is een noodaggregaat dat maandelijks getest wordt.
22. De aanwezige brandblusser bij de Main Equipment Room (MER) blust de brand, maar richt mogelijk schade aan de techniek aan.
23. De ruimte met de RAAS-server heeft een alarm.
24. Voor het printen is een tag noodzakelijk.
25. De raadsleden hebben geen directe toegang tot de werkruimtes.
26. De schoonmakers zijn ingehuurd en het is onduidelijk of en in welke mate afspraken gemaakt zijn over integriteit en screening.

2.3.2 Aanbevelingen

1. Zorg ervoor dat de identiteit van bezoekers en medewerkers altijd gecontroleerd worden voordat toegangsmiddelen uitgegeven worden. Zorg ervoor dat bezoekers vooraf aangemeld moeten worden zodat de receptionisten dagelijks weten welke bezoekers zij kunnen verwachten en wie de begeleider is.
2. Neem fysieke (toegangs)beveiliging op in het introductieprogramma. Besteed expliciet aandacht aan het risico op meelopers via de personeelsingang en hoe daarmee om te gaan.
3. Stel een protocol op voor het omgaan met verdachte pakketten en bommeldingen.
4. Zorg ervoor dat de MER voorzien is van gasblussers om schade aan IT-infrastructuur te voorkomen.
5. Controleer of er afspraken gemaakt zijn met het schoonmaakbedrijf ten aanzien van de integriteit van medewerkers. Scherp deze afspraken indien nodig aan.

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.

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

2.4.1 Bevindingen

1. SSC-Ons laat halfjaarlijks penetratietesten uitvoeren op haar IT-infrastructuur en deelt de bevindingen met de partners in een presentatie. Ieder kwartaal wordt de voortgang van de opvolging besproken met de partners. Westerveld heeft als partner inspraak op de scope van de penetratietesten.
2. SSC-Ons is een tool voor kwetsbaarhedenmanagement aan het implementeren. Westerveld heeft via een stuurgroep inspraak op de security projecten bij SSC-Ons.
3. Het merendeel van de applicaties is via Single-Sign-On (SSO) toegankelijk.
4. Een aantal belangrijke systemen zijn direct vanaf het internet benaderbaar: het zaaksysteem, het HRM systeem en ITSM.
5. Door SSC-Ons (in opdracht van Westerveld) uitgegeven apparaten worden beheerd met Microsoft Intune. Voor onbeheerde privé apparatuur worden profielen toegepast om eisen te stellen voordat toegang wordt verleend.
6. Westerveld heeft geofencing geïmplementeerd waarmee de toegang tot gemeentelijke netwerken en -systemen beperkt is tot bepaalde geografische regio's.
7. Westerveld neemt deel aan een aanbesteding voor security monitoring (SIEM/SOC[21]) en SSC-Ons doet de inrichting daarvan. Het is bij Westerveld onbekend welke logbronnen hierop zijn aangesloten en ontvangt geen rapportages daarover. Logging wordt door SSC-Ons 1 jaar bewaard en aanvullend op basislogging[22] wordt de Microsoft Azure omgeving aangesloten. Specifieke applicaties zijn niet gekoppeld aan security monitoring. Meldingen vanuit het SIEM worden door de OSO's opgepakt. Voor het SOC loopt een inkooptraject inclusief darkweb monitoring.
8. Facilitair is verantwoordelijk voor multimedia en dit zit deels op een virtueel gescheiden omgeving.
9. De netwerkcomponenten worden in 2026 vervangen en netwerkscheiding en -segmentatie wordt daarin meegenomen.
10. SSC-Ons maakt gebruik van tooling om aan het netwerk verbonden assets te identificeren en te koppelen aan de ITSM tool.
11. SSC-Ons heeft een twee datacenters en verricht uitwijktesten. Binnenkort vind een geplande stroomonderbreking plaats. SSC-Ons start eind 2025 een project voor de beveiligingsaspecten van continuïteitsbeheer.
12. SSC-Ons is voornemens een honeypot in te richten.[23]

[21] SIEM: Systeem waarin men informatie uit computersystemen verzamelt en analyseert. Het doel is om verdacht gedrag te ontdekken of zien dat iemand dingen in het systeem heeft veranderd, terwijl hij dat niet mocht. SOC: Afdeling, team of dienst dat digitale systemen en/of indentity's controleert en/of bewaakt en soms ook afhandelt.

[22] Active Directory, Entra ID, LDAP, DHCP, DNS, Microsoft Security alerts, servers, werkplekken, Office 365, firewalls, ESB, IAM-tooling

[23] Een digitaal systeem dat met opzet niet goed beveiligd is. Het doel van dit systeem is om het te laten besmetten met software die een digitaal systeem wil aanvallen. Daarna kan men deze software analyseren.

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

13. Westerveld heeft een oplossing voor veilig mailen geïmplementeerd.
14. Medewerkers ervaren problemen met het beantwoorden van Teams oproepen via de telefoon omdat zij twee codes moeten invoeren. Omdat de telefoons traag werken zijn ze regelmatig te laat met opnemen.

2.4.2 Aanbevelingen

1. Ga door met de implementatie van SIEM/SOC en bepaal risicogebaseerd welke logbronnen aanvullend aangesloten moeten worden, zoals specifieke cloudapplicaties. Overweeg om de respons functionaliteit bij het SOC te beleggen. Hiermee wordt het SOC te gemandateerd om al dan niet automatisch in te grijpen in de IT-infrastructuur om incidenten te isoleren. Hierdoor hoeft Westerveld niet 24/7 beschikbaarheid te realiseren en wordt zij maximaal ontzorgt.
2. Maak gebruik van de kennis en ervaring bij SSC-Ons om bij de vervanging van de netwerkcomponenten adequaat netwerkscheiding en -segmentatie toe te passen.
3. Verlang van SSC-Ons dat zij verantwoording afleggen over uitgevoerde hersteltesten en de opvolging daarvan. Idem voor het slagen en falen van backups inclusief hersteltesten.
4. Analyseer samen met SSC-Ons de problematiek rondom het beantwoorden van Teams oproepen via de telefoon en realiseer een werkbare oplossing voor medewerkers.

2.5 Aanbevelingen gemeenteraad

De gemeenteraad heeft een belangrijke rol ten aanzien van de informatieveiligheid binnen Westerveld. De VNG[24] 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, kaders te stellen, prioriteiten te bepalen, voldoende middelen beschikbaar te stellen en toezicht te houden op hoe Westerveld 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[25][26] 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

[24] https://vng.nl/artikelen/raadgever-digitale-veiligheid
[25] https://vng.nl/sites/default/files/2025-04/raadsleden-en-informatiebeveiliging.pdf
[26] https://vng.nl/sites/default/files/2023-04/checklist-raadsleden-digitale-veiligheid.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

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[27] 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.

[27] 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?

Het ontbreekt 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, hetgeen 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.

Westerveld heeft een fulltime CISO aangesteld, een PO voor 0.7 fte en de FG wordt ingehuurd. In de praktijk valt en staat het managementsysteem met de inzet van de CISO, terwijl hij feitelijk ondersteunend en controlerend dienen te zijn.

Westerveld 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 intensiever gebruiken van de GRC-tool kan helpen om dit inzichtelijker te maken voor het 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.

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

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)?

Westerveld voldoet niet volledig (aantoonbaar) aan de AVG, BIO2 en Cyberbeveiligingswet eisen. Dit wil niet zeggen dat Westerveld 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.

Ten aanzien van de BIO2 naleving berust een belangrijk aandeel van de operationele verantwoordelijkheid bij SSC-Ons. Nauwe samenwerking is vereist om dit niet alleen te realiseren, maar vooral ook om dit aantoonbaar te maken. SSC-Ons zet hierin stappen door in de toekomst onafhankelijke zekerheid te verschaffen (ISAE3000 type II verklaring).

Ten aanzien van de Cyberbeveiligingswet heeft Westerveld 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 en worden aantoonbaar uitgevoerd. Er is echter een grote afhankelijkheid van de CISO waardoor de continuïteit mogelijk in het geding is. De toegang is ingericht op basis van attributen en niet op rollen, waardoor de noodzakelijke toegang niet (altijd) eenduidig gedefinieerd en controleerbaar is. Echter loopt er een traject in samenwerking met SSC-Ons om toe te werken naar rolgebaseerde toegang.

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?

Westerveld heeft een beeld van welke systemen kritisch zijn voor de dienstverlening en continuïteit, maar heeft deze niet expliciet vastgesteld. Westerveld 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?

Westerveld heeft onvoldoende de beschikbaarheidseisen van systemen en processen vastgesteld. SSC-Ons hanteert standaard beschikbaarheidsniveaus die zijn vastgelegd in de overeenkomsten tussen haar en Westerveld.

Westerveld heeft geen draaiboeken uitgewerkt om de continuïteit van haar kritieke processen te waarborgen tijdens calamiteiten. Vanuit technisch oogpunt wordt er sterk geleund op SSC-Ons.

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 opvalt is dat zij beiden crisisplannen hebben, maar niet integraal oefenen. Hierdoor is het aannemelijk dat deze plannen niet (geheel) op elkaar aansluiten.

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

Er is geen lijst met bekende technische kwetsbaarheden en -misconfiguraties gedeeld met de onderzoekers. Er is wel vastgesteld dat Westerveld in samenwerking met SSC-Ons investeert in het identificeren en oplossen van kwetsbaarheden. Bijvoorbeeld aan de hand van penetratietesten, kwetsbaarhedenscans en mystery guest onderzoeken. Aanvullend daarop controleert de Informatiebeveiligingsdienst (IBD) het externe aanvalsoppervlak van Westerveld op kwetsbaarheden.

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

Security monitoring is deels ingericht en wordt projectmatig verder uitgebreid met een externe SOC-leverancier en scope-uitbreiding. Het signaleren van beveiligingsproblemen is momenteel niet 24x7, maar gaat dat worden zodra de SOC-leverancier is aangehaakt. Het al dan niet automatisch reageren op beveiligingsproblemen is vooralsnog de verantwoordelijkheid van SSC-Ons en Westerveld zelf, ook buiten kantoortijden. In de SLA met SSC-Ons zijn afspraken gemaakt over piketdiensten in de avonduren (17:00 - 22:00 uur) en in weekenden en feestdagen (10:00 - 22:00 uur). Beveiligingsproblemen buiten deze vensters worden niet direct of op basis van best effort opgepakt.

3. Risicoanalyse en dreigingen

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

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

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?

Westerveld en SSC-Ons laten gespecialiseerde partijen penetratietesten uitvoeren om

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

kwetsbaarheden en aanvalspaden te identificeren. Westerveld adresseert de kwetsbaarheden. Westerveld 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 hoe zijn deze opgelost? Hoe wordt er bijvoorbeeld bij een datalek gecommuniceerd met de mogelijk betrokkenen binnen en buiten de gemeentehuizen?

In 2025 zijn maximaal 20 incidenten geregistreerd waarvan het merendeel werd veroorzaakt door eigen personeel. De technische (bijna-)incidenten zoals malware, poortscans of bruteforce pogingen zijn niet bijgehouden in het overzicht. Hierdoor ontstaat een vertekend beeld van de werkelijkheid. De datalekken worden geregistreerd in het zaaksysteem van Westerveld.

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?

Tijdens het indiensttredingstraject komt informatiebeveiliging aan de orde en tijdens het dienstverband sporadisch via bijvoorbeeld een gemeentelijke informatiebijeenkomst. De intrinsieke motivatie onder medewerkers is aanwezig — de uitdaging ligt in het structureel versterken van kennis, het verbeteren van de communicatie en de praktische toepasbaarheid binnen Westerveld.

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

De frequentie van de bewustwordingsactiviteiten is ad-hoc en de effectiviteit wordt deels bepaald aan de hand van mystery guest onderzoeken en inspecties, zoals rondes om te controleren op vergrendelde schermen en opgeruimte werkplekken. 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. Westerveld sluit bijvoorbeeld verwerkersovereenkomsten met leveranciers af, voert (pre-)DPIA's uit, houdt toezichtsacties, verricht oorzaakanalyses bij datalekken en past verbeteringen toe naar aanleiding daarvan. Westerveld heeft een achterstand opgebouwd en de afhankelijkheid van de PO en FG zijn hoog.

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

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

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

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. Westerveld heeft geen retainer afgesloten met een gespecialiseerde derde partij, het is onduidelijk of SSC-Ons dit wel heeft.

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

Westerveld en SSC-Ons beschikken over een crisisplan, maar hebben deze niet op elkaar afgestemd en geoefend. Het is daarom aannemelijk dat deze niet volledig op elkaars behoeften aansluiten.

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?

De CISO heeft ±20k budget tot zijn beschikking voor informatiebeveiliging. Dit wordt voornamelijk ingezet voor de verplichte ENSIA-audits. Voor privacybescherming is geen separaat budget beschikbaar, dit moet uit hetzelfde budget bekostigd worden.

Circa €3.5 - €4.5 miljoen is begroot voor informatiebeveiliging bij SSC-Ons. Dit is exclusief de kosten van de CISO, Compliance Officer, etc.

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?

Westerveld 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 Westerveld 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

11 Assurance rapportage ISAE 3402 ONS 2024 v1.0.pdf
1701_Verbeterpunten Gemeente Westerveld_BIO-rapportage 2024_2024 ENSIA NON COMPLIANCE.docx
2024 Q2 Entitlement review.zip
20240115 Melding M240102888 Inputdocumentatie Autorisatiereview Q1 2024.xlsx
20240408 Melding M240306097 Inputdocumentatie Autorisatiereview Q2 2024 - Westerveld.xlsx
20240703 Melding M240306097 Inputdocumentatie Autorisatiereview Q3 2024 - Westerveld.xlsx
2025 Addendum - Eisen en wensen Architectuur en Ontwerp.pdf
2025 Bijlage - Eisen en wensen Architectuur en Ontwerp.pdf
2025 Q1 Entitlement review.zip
2025-2026 Jaarplan privacy n.a.v. borgingsproduct.docx
20250102 Melding M240306097 Inputdocumentatie Autorisatiereview Q1 2025 - Westerveld.xlsx
20250319 Pre DPIA vergunningen en meldingen graven kabels en leidingen.pdf
20250401 Melding M250102497 Accountantscontrole personele mutaties Westerveld 2025Q1.xlsx
21-01-2025 rapport.pdf
8.1 Beleid voor logische toegangsbeveiliging.docx
AccounInactive.csv
AccountExpiring.csv
AccountExpiring2.csv
accounts Westerveld 01012024.xlsx
Acties privacyteam 2025-2026.xlsx
AD export.xlsx
AD_PeriodiekeControle-Westerveld_04072024.csv
AD_Westerveld.csv
AD-WVLD-240329.xlsx
AD.xlsx
Afstudeervoorstel_isavanijsselmuiden_eerste_kans.pdf
asm_assets_all_clients_20250924_131255.csv
asm_risks_all_clients_20250924_131426.csv
Assetmgmt Projectdefinitie.docx
Autorisatie gebruikers GBA-V 2024.xlsx
autorisatiemeldingen Topdesk.xlsx
Autorisaties Centric Leefomgeving.xlsx
Autorisaties team Almar.xlsx
Autorisaties team Anita.xlsx
Autorisaties team Carly.xlsx
Autorisaties team Gerbrig.xlsx
Autorisaties team Michiel.xlsx
Autorisaties werkdocument 20250103.xlsx
Autorisaties werkdocument.xlsx
Autorisaties werkdocument20240208.xlsx
Autorisaties werkdocument20240419.xlsx
AutorisatiesKey2Financien_10053647#9062_.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

DMC GROUP
SECURITY MANAGEMENT

Autoriseren - aanvraagformulier BRP.docx
Beleidsplan privacy 2018 (2).pdf
Bijlage 1 Gemeentebreed informatiebeveiligingsbeleid Westerveld.pdf
Bijlage 2 Gemeentebreed informatiebeveiligingsbeleid Westerveld.pdf
BIO2-Gap-analyse-versie-0.99.xlsx
BIO2-Gap-analyse-versie-1.2 def.xlsx
BIO2-Gap-analyse-versie-1.2.xlsx
BIO2-Kans-en-Impact-tabellen-gemeenten.xlsx
BIO2-Kritieke-processen-gemeenten.xlsx
Brief DCT Weerbaarheid cybercrisis in Drenthe.docx
Budget Privacy.pdf
Budget security.pdf
Controle autorisaties kritische ruimten.docx
Controle op authorisaties Key2.msg
Cyber Security Assesment.xlsx
DAP V1.3 ICT Dienstverlening.pdf
Darktrace.xlsx
De-10-bestuurlijke-principes-voor-Informatiebeveiliging_20190109.pdf
Dis4all Aanpassen wachtwoorden.pdf
Domainadmins_wvldlocal.csv
DPIA-Diftar 2023_ondertekend_16-9-2024.pdf
Evaluatierapport Cybercrisissimulatie.pdf
FGRapport_Toezicht_2023_2024 - okt-BenW.pdf
Formulier management voor controle autorisatie.docx
Functiebeschrijving autorisatiebevoegde.docx
Gebruik Suwinet afgelopen 6 maanden - GSD-rapportage westerveld - april 2024.pdf
Gebruik Suwinet afgelopen 6 maanden - GSD-rapportage westerveld - augustus 2024.pdf
Gebruik Suwinet afgelopen 6 maanden - GSD-rapportage westerveld - december 2023.pdf
Gebruik Suwinet afgelopen 6 maanden - GSD-rapportage westerveld - januari 2024.pdf
Gebruik Suwinet afgelopen 6 maanden - GSD-rapportage westerveld - juni 2024.pdf
Gebruik Suwinet afgelopen 6 maanden - GSD-rapportage westerveld - maart 2024 review.pdf
Gebruik Suwinet afgelopen 6 maanden - GSD-rapportage westerveld - maart 2024.pdf
Gebruik Suwinet afgelopen 6 maanden - GSD-rapportage westerveld - september.pdf
Gebruik Suwinet Classic afgelopen 6 maanden - GSD-rapportage westerveld - december 2024.pdf
Gebruik Suwinet Classic afgelopen 6 maanden - GSD-rapportage westerveld - februari 2025.pdf
Gebruik Suwinet Classic afgelopen 6 maanden - GSD-rapportage westerveld - november 2024.pdf
Gebruikers GouwIT_20240712.xlsx
Gebruikers Key2fin 2024.csv
Gebruikers Key2Finance.xlsx
Gemeente Westerveld Azure AD gebruikersoverzicht.csv
Gemeente Westerveld Azure AD gebruikersoverzicht.xlsx
Gemeentebreed informatiebeveiligingsbeleid 2023.pdf
gsd11 december+2024.csv
gsd11 juni+2024.csv
gsd11 mei+2024.csv

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

gsd23 juni+2024.csv
gsd23 juni+2024.xlsx
gsd25 december+2024.csv
gsd25 juni+2024.csv
GSD25juni2024.xlsx
gsd34 december+2023.csv
gsd34 december+2024.csv
gsd34 mei+2024.csv
gsd41 december+2024.csv
gsd42 juni+2024.csv
ICT F1 Beleidsplan privacy 2018 (2).pdf
ICT F1 Bijlage 1 Gemeentebreed informatiebeveiligingsbeleid Westerveld.pdf
ICT F1 Bijlage 2 Gemeentebreed informatiebeveiligingsbeleid Westerveld.pdf
ICT F1 Gemeentebreed informatiebeveiligingsbeleid Westerveld.pdf
ICT F4.docx
Incident verslag Westerveld - Zonder informatie.pdf
Inputdocumentatie Autorisatiereview Q4 2024 - Westerveld.xlsx
Jaarplan CISO 2025.docx
Key2BAG databasegebruikers.pdf
Key2BAG_centric_passw_prof.sql
Key2BAGPassword policies voor service accounts Oracle Database 12c.pdf
Key2Begraven databasegebruikers (1).pdf
Key2Burgerzaken databasegebruikers.pdf
Key2DDS Wijzigen standaardwachtwoorden v1.0.pdf
Laatste rapport 10-10-2024.pdf
M240905398.xlsx
MatrixoverzichtAutorisaties_10053648#9062_.xlsx
Memo Suwi rapportage.docx
MT voorstel BCM.docx
MT voorstel Scope ISMS.docx
Nieuw - Microsoft Excel-werkblad.xlsx
NIS2 Quickscan 2025-03-24 13u48.pdf
Nis2 voorbereiding.pdf
Notitie verantwoordingsstelsel ENSIA 2023-2024 met bijlagen v1.0.pdf
Notities Recourse GRC.docx
Oorspronkelijke aanvraag (72).pdf
Opmerking ICT F7.docx
Opvolging acties ML 2024.xlsx
overzicht applicaties en wachtwoorbeleid.xlsx
Overzicht Informatiebeveiligingsincidenten 2025.xlsx
PDC V1.6 ICT Dienstverlening.pdf
pentest 2025.pdf
Planning control framework ICT dienstverlening Ons v2.xlsx
Presentatie_TL_Februari2024_Omgaan met privacy bij de gemeente Westerveld.pptx
Procedure autorisatie tot Suwinet.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

Procedure autoriseren van gebruikers voor toegang tot applicaties (1).docx
Procedure Operationele controle autorisatiebeheer.docx
Procedure Periodieke controle autorisatiebeheer.docx
Procedure toegang tot en gebruik van systemen (incl. RAAS) (1).docx
Rapport 26-03-2025.pdf
Rapport 29-03-2024.xlsx
Rapport 5-7-2024.pdf
Rapport medewerkers 2024.csv
Rapport medewerkers 2024.xlsx
Rapportage controle autorisaties Key2Finance WV.docx
Rapportage controle autorisaties sociale zaken.docx
Rapportage controle op de autorisaties en bevoegdheden.docx
Rapportage ENSIA BIO 2024.pdf
Rapportage security meldingen - Westerveld.png
RE Rapportage bevindingen pentest 2025.msg
Reactie vragen PO Security.xlsx
Reactie Westerveld___CISO.pdf
Richtlijn cryptografische beheersmaatregelen.docx
rollenresources december+2024.csv
Samenvatting Bevindingen.docx
sasExportAeolus.xlsx
sasExportKey2betalen.xlsx
sasExportKey2fin.xlsx
SLA 2025 ICT Dienstverlening.pdf
Soc projectbeschrijving.docx
Sociaal Domein Accounts en wachtwoorden (Versie 11).pdf
SSF Status 20-11-2025.pptx
Stappenplan actualiseren register van verwerkingen 2.0.pdf
SUWI aut.tabel.pdf
T.b.v autorisatiematrix applicatie Kikker.msg
TLP-AMBER - NCSC-dreigingsanalyse - Q3 2025.pdf
TLP-AMBER_-_NCSC-dreigingsanalyse_-_Q1_2025.pdf
TLP-AMBER_-_NCSC-dreigingsanalyse_-_Q2_2025.pdf
TLP-AMBER_-_NCSC-dreigingsanalyse_-_Q4_2024 (1).pdf
Update crisissimulatie _20241024_214316_0000.pdf
Voorstel MT Westerveld - Inrichtingsvoorstel ISMS, Scope en Governance.docx
Vulnerability Management projectbeschrijving.docx
Wachtwoordpolicies.xlsx
Werkdocument AD.xlsx
Westerveldse belevingsprincipes .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

B Interviews

Gemeente Westerveld:

- Teamleider informatievoorziening/ICT
- Functionaris Gegevensbescherming
- Teamleider openbare ruimte
- Chief Information Security Officer
- WMO
- Gemeentesecretaris
- Burgerzaken
- Facilitair
- Gebouwbeheer
- Teamleider KCC
- HRM
- KCC
- Receptionist
- Manager bedrijfsvoering
- BOA
- Privacy Officer

SSC-Ons:

- TISO
- CISO

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