BMC
YACHT GROUP

Brochure BMC-safety

Bewustwordings- en opleidingsprogramma informatieveiligheid & privacy

Brochure | 26 november 2021

Partners in verbetering

BMC-safety

Bewustwordings- en opleidingsprogramma informatieveiligheid & privacy

Brochure

BMC

26 november 2021

Classificatie : Openbaar

Naam projectleiders :

- Oumaima Karmon
  Oumaima.karmon@bmc.nl
  06 13 43 59 01

- Lisanne Knol
  Lisanne.knol@bmc.nl
  06 13 95 40 16

Projectteam:

- Marita Bulten
- $$
- $$

Inhoudsopgave

H1 | BMC-safety

De bakermat voor een bewuste en veilige organisatie

BMC werkt al jaren samen met overheidsorganisaties op het gebied van informatiebeveiliging en privacy. Uit ervaring weten we als geen ander dat op deze gebieden de mens vaak de zwakste schakel blijft. Het is daarom essentieel dat medewerkers bewust met (persoons)gegevens omgaan. Om overheden hiermee te ondersteunen heeft BMC nu een passend bewustwording- en opleidingsprogramma ontwikkeld onder de noemer: BMC-safety.

1.1 Wat hebben we eigenlijk te verliezen?

De afgelopen jaren doen zich in de publieke sector tal van incidenten en/of datalekken voor met betrekking tot informatieveiligheid en privacy. De oorzaak hiervoor wordt mede gevonden in onvoldoende kennis en kunde van medewerkers en bestuurders ten aanzien van deze onderwerpen. Het gevolg van dit 'bewustwordingsniveau' is dat de organisatie risico's loopt op het gebied van onder andere continuïteit van dienstverlening, schadeclaims en imagoschade.

Voorbeelden van de incidenten die zich binnen de organisatie kunnen voordoen zijn: klikken op kwaadwillende links en openen van bijlagen in e-mails, verzoeken tot wijziging banknummers leveranciers, et cetera. Daarnaast is er een duidelijke kwaliteitsverbetering te constateren bij de pogingen van criminelen waardoor deze pogingen steeds professioneler worden en dus moeilijker te herkennen zijn door de medewerkers en bestuurders. Door te investeren in bewustwording wordt juist de eventuele financiële schade beperkt of zelfs voorkomen.

1.2 Ad hoc vs. structurele aanpak

Er worden op het gebied van informatiebeveiliging en privacy vaak verschillende bewustwordingsactiviteiten en trainingen/workshops georganiseerd. Deze activiteiten staan echter los van elkaar, worden ad hoc ingezet of zijn eenmalige acties. Doorgaans is er geen eenduidig en structureel plan voor. De effectiviteit van de bewustwordingsactiviteiten die wel ingezet worden en de kennis die daarbij is opgedaan, verdwijnen hierdoor na verloop van tijd. Nieuwe medewerkers en externen zijn bovendien ook niet altijd op de hoogte van de privacy- en informatiebeveiligingsregels die van toepassing zijn binnen organisatie.

De organisatie lijkt behoefte te hebben aan een continue aanpak van bewustwording. Dit is overigens ook een verplichting uit de Baseline Informatieveiligheid Overheid (BIO). Een bewustwordingsprogramma wat zich ieder jaar herhaalt, toegespitst op thema's en doelgroepen die op dat moment urgent zijn om te behandelen of waar de organisatie op dat moment behoefte aan heeft. Gedragsverandering is een proces wat tijd vergt. Door het inzetten van een bewustwordingsprogramma wat zich jaarlijks herhaalt, wordt het kennis- en bewustwordingsniveau van de medewerkers op peil gehouden en biedt het ook de mogelijkheid om het niveau te laten stijgen.

1.3 PDCA-cyclus

Door de inrichting van een jaarlijkse leer- en gedragsveranderende cyclus op basis van een door het college vastgesteld bewustwordingsplan, zorgen we ervoor dat de weerbaarheid van de organisatie verder wordt vergroot om in te spelen op de toenemende (cyber)dreigingen. Hierdoor worden medewerkers in staat gesteld om veilig en risicobewust te werken met (persoons)gegevens en risico's te herkennen. Alle medewerkers van de organisatie moeten zélf de behoefte gaan voelen om zich op een manier te gedragen dat ze continu de privacy wet- en regelgeving en de BIO naleven, zonder hierbij na te denken over mogelijke repressie. Zij moeten het als taak en onderdeel van hun werk zien om elkaar te motiveren en aan te spreken wanneer het niet wordt nageleefd. Om dit continue verbeterproces vorm te geven, wordt gebruikgemaakt van de PDCA-cyclus (Plan, Do, Check, Act) met als doel een hoger volwassenheidsniveau te behalen op het gebied van bewustwording door middel van een jaarlijkse terugkerende leercyclus.

1.4 Waarom kiezen voor BMC?

De adviseurs van BMC hebben een brede kennis van en ervaring met overheidsorganisaties. Zij weten vanuit alle vakgebieden, zoals ICT, het sociaal domein of HRM de verbinding te leggen met informatieveiligheid en privacy. Zij staan naast de medewerkers vanuit hun ervaring met het dagelijks werk binnen de gemeente. Altijd pragmatisch en resultaatgericht. BMC heeft een brede kennis en expertise binnen alle domeinen. Hierdoor zijn wij in staat per geïnventariseerde doelgroep de juiste relevante onderwerpen te koppelen. Bijvoorbeeld medewerkers binnen het sociaal domein, medewerkers aan de balie, maar ook raadsleden. Wij bieden uw organisatie een veelzijdig, uitdagend bewustwordings- en opleidingsprogramma omtrent informatieveiligheid en privacy met de juiste ondersteuning om bewustwording te laten groeien binnen uw organisatie en structureel deel uit te laten maken van uw organisatiecultuur.

H2 | De BMC-Safety aanpak

Het doel van het BMC-safety bewustwordings- en opleidingsprogramma gaat verder dan traditionele bewustwordingscampagnes die zich richten op informatiebeveiliging en privacy. Veel campagnes beperken zich tot het zenden van kennis, terwijl mensen door meerdere factoren dan alleen kennis worden gedreven. Het alleen opdoen van kennis is niet het doel van dit bewustwordingsprogramma. Het weten wat je moet doen staat los van het daadwerkelijke gedrag van de medewerkers. BMC-safety richt zich op het overbruggen van deze kloof om zowel de kennis als gedragsverandering op het gebied van informatiebeveiliging en privacy van de medewerkers bij elkaar te brengen.

Het BMC-safety bewustwordings- en opleidingsprogramma zorgt ervoor dat bewustwording deel gaat uitmaken van de PDCA-cyclus, zodat bewustwording in de organisatiecultuur wordt ingebed. We willen het volwassenheidsniveau van de organisatie verhogen. Van ad hoc naar het inzetten van structurele bewustwordingsactiviteiten of zelfs naar het niveau van een proactieve organisatie.

2.1 De visie

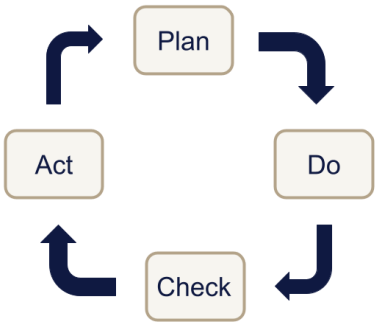
Het BMC-safety bewustwordings- en opleidingsprogramma is een samengesteld programma waarbij elke medewerker meerdere interventies en leervormen krijgt aangeboden om awareness, kennis en vaardigheden te ontwikkelen omtrent informatieveiligheid en privacy. De visie die BMC hanteert is gebaseerd op de drie onderstaande principes, welke leidend zijn bij alle activiteiten binnen de cyclus:

1. Realiseren van veilig gedrag en kennis vereist maatwerk.
2. Realiseren van meetbare gedragsverandering.
3. Bevorderen van veilig gedrag vraagt elke dag aandacht.

Het BMC-safety bewustwordings- en opleidingsprogramma biedt u thema's die het risicobewustzijn rondom informatieveiligheid en privacy bevorderen. Samen met u richten wij een continu proces in van 'leren en doen' en we zorgen dat dit geborgd is in het dagelijks handelen. Het BMC-safety bewustwordings- en opleidingsprogramma is praktisch en maakt de vertaalslag naar uw dagelijkse realiteit. Uw medewerkers, managers of bestuurders worden begeleid om in hun rol en binnen hun werkterrein op een juiste wijze met informatie om te gaan. Wij ondersteunen u bij het creëren van een inclusieve cultuur aangaande informatiebeveiliging en privacy, waar iedereen meedoet en waar men elkaar kan aanspreken op houding en gedrag. In deze cultuur is het nuttig en leerzaam om eventuele incidenten of ongewenste werkwijzen aan de orde te stellen zonder dat dit negatieve spanningen veroorzaakt. Ongeacht hun kennisniveau kunnen alle medewerkers en bestuurders aan dit programma deelnemen. Met het BMC-safety bewustwordings- en opleidingsprogramma zorgen wij ervoor dat houding en gedrag van de medewerkers meetbaar zijn. De effecten van het programma worden daarmee zichtbaar voor de hele organisatie. Het bestuur en management krijgen daarmee inzicht in knelpunten en risico's in de houding en het gedrag van de medewerkers.

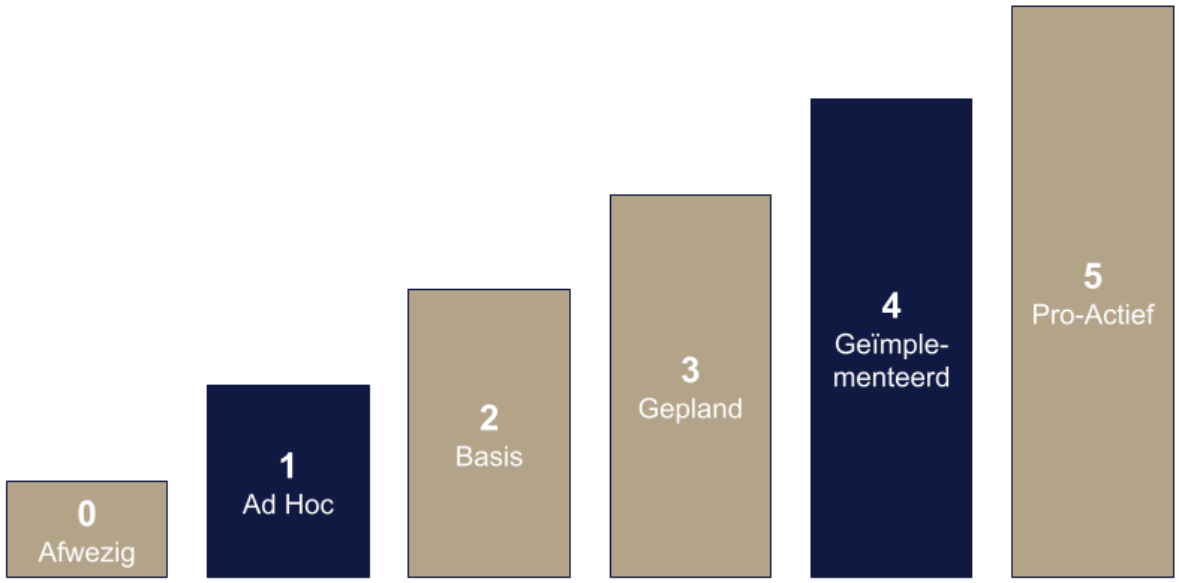
Volwassenheidsniveau

Wij willen met ons BMC-safety bewustwordings- en opleidingsprogramma zorgen dat bewustwording deel uitmaken van een plan-do-check-act (PDCA-) cyclus. De PDCA-cyclus geeft het principe weer van continue verbetering. Met dit principe wordt aangegeven dat voor het bereiken van een hogere kwaliteit een continue cyclus op gang moet worden gebracht.



Dit vindt plaats door het plannen van de acties op basis van de meetresultaten, eventuele nieuwe dreigingen en ontwikkelingen. Vervolgens worden de geplande acties ten uitvoer gebracht. In de check- fase worden de resultaten van de acties gecontroleerd of deze werkelijk zijn zoals was beoogd. In de laatste fase vindt een evaluatie plaats van alle genomen stappen en het bijsturen van de uitvoering of plannen naar aanleiding van de resultaten. Op deze manier wordt bewustwording structureel ingebed in uw organisatiecultuur. We willen een beweging in gang zetten

waardoor het volwassenheidsniveau wordt verhoogd van ad hoc naar structureel aanwezig en geïmplementeerd, en zelfs proactieve medewerkers.



Op basis van bovenstaand model wordt in afstemming met het bestuur en management vastgesteld welk volwassenheidsniveau op het gebied van bewustwording de organisatie wil bereiken.

2.2 De aanpak

Stap 1: analyseren

In de eerste fase van elke cyclus wordt het kennisniveau en gedrag beoordeeld door middel van kennis- en gedragsmetingen. Tevens vindt een inventarisatie plaats van de organisatiedoelen, omgevingsfactoren, organisatierisico's en de reeds genomen stappen op het vlak van bewustwording.

Stap 2: focus aanbrengen

BMC richt zich in deze fase op het aanbrengen van focus voor het verdere verloop van het BMC-safety bewustwordings- en opleidingsprogramma. Hiervoor worden de resultaten van diverse metingen verzameld en geanalyseerd. Dit ten behoeve van het opleveren van een implementatiestrategie en opleidingsplan waarin onder andere de leerdoelen, doelgroepen en tijdsinvesteringen voor de organisatie worden opgenomen. Dit alles wordt gepresenteerd aan de stakeholders van het programma, zoals bijvoorbeeld het MT, DT en/of het bestuur.

Stap 3: activeren

In deze fase is het van belang om het BMC-safety bewustwordings- en opleidingsprogramma te activeren en de organisatie handvatten te bieden om het programma in te leiden. Dit gebeurt door middel van het versturen van uitnodigingen,het maken van infographics en posters en dergelijke per doelgroep en per thema.

Stap 4: implementeren

In deze fase is het van belang om het BMC-safety bewustwordings- en opleidingsprogramma te activeren en de organisatie handvatten te bieden om het programma in te leiden. Dit gebeurt door middel van het versturen van uitnodigingen, het maken van infographics en posters en dergelijke per doelgroep en per thema.

In deze fase start BMC tevens met het uitvoeren van de interventies (workshops, trainingen, et cetera) en facultatief met de e-learning/kennistesten met feedback. BMC zorgt voor een bewustwordingsplan en activiteitenplanning met daarin de gekozen interventies die aansluiten op de diverse doelgroepen.

Stap 5: evalueren

In deze fase vindt een evaluatie en monitoring plaats van de cyclus. Op basis van de uitkomsten van het BMC-safety bewustwordings- en opleidingsprogramma in de check-fase worden er weer nieuwe campagnes georganiseerd voor het nieuwe jaar en zal, indien noodzakelijk, het BMC-safety bewustwordings- en opleidingsprogramma aangescherpt worden. Indien in de check-fase grote risico’s worden geconstateerd, is dit input voor het nieuwe BMC-safety bewustwordings- en opleidingsprogramma. Blijvend effect en continuïteit staan voorop.

Doelgroepen

In de context van het BMC-safety bewustwordings- en opleidingsprogramma onderscheiden we zes doelgroepen die ieder een eigen aanpak nodig hebben om het gewenste effect te bewerkstelligen.

1. Lijnmanagement

Deze doelgroep treedt idealiter op als 'voorbeeldfunctie' naar de rest van de werknemers.

2. Privacy- en informatiebeveiligingsbeheerders

Deze doelgroep betreft personen die in het kader van hun reguliere werkzaamheden veel te maken hebben met privacy en informatiebeveiliging en vormen de 'ambassadeurs'.

3. Medewerkers+

Onder de werktitel 'medewerkers+' verstaan we werknemers die reeds enige kennis en/of ervaring hebben met privacy, veiligheid en data (zoals bijvoorbeeld HR, (concern)control, applicatiebeheer, inkoop, ICT, Sociaal Domein en Publiekszaken).

4. Medewerkers

Medewerkers die geen ervaring en/of direct gerelateerde werkzaamheden hebben met data, veiligheid, informatiebeveiliging en/of privacy.

5. Bestuur

De college- en raadsleden dienen op de hoogte te zijn hoe onbevoegden geen toegang kunnen krijgen tot deze informatie en hoe zij bewust met deze gegevens dienen om te gaan, naast dat er op dit niveau verantwoordelijkheid wordt gedragen voor het vakgebied.

6. Nieuwe medewerkers

Ook voor nieuwe medewerkers en externen is het van belang dat zij bij binnenkomst gelijk kennismaken met de belangrijkste inzichten en bedrijfsregels ten aanzien van risicomanagement op de onderwerpen informatiebeveiliging en privacy.

H3 | BMC-safety pakketten

Er zijn vier verschillende varianten van het bewustwordings- en opleidingsprogramma BMC-safety mogelijk, welke in onderstaande tabel summier en schematisch staan weergegeven.

	Meting & advies	Basis	Medium	Premium
Kennismeting	X	X	X	X
Rondje gebouw*	X	X	X	X
Gedragsmeting**			X	X
Implementatiestrategie & opleidingsplan	X	X	X	X
Communicatiemateriaal			X	X
Webinar basis IB&P		XX	XX	XX
Interactieve basistraining IB&P		XX	XX	XX
Vakinhoudelijke training			X	XX
Verdiepingstraining			X	XXX
Ludieke acties			X	XX
Evaluatie		X	X	X

*Rondje door het gebouw om veilig gedrag te analyseren
**Keuze tussen mystery guest, mystery caller
*** Keuze uit een verdiepingstraining óf een vakinhoudelijke training

3.1 Pakketten en interventies

De onderstaande tabellen geven de diverse varianten van het het BMC-Safety programma nog gedetailleerder weer. Hierbij zijn de basisactiviteiten per uitvoeringsfase weergegeven. Vervolgens staan de diverse interventies - workshops, webinars, ludieke acties et cetera - aangegeven. Hiermee wordt de invulling van het programma geformuleerd in de interventiefase.

Pakket 1: Meting en advies

Fase	Onderzoek en Advies
1	Kennismakingsgesprek
	Inventarisatie van organisatiedoelen, omgevingsfactoren, organisatierisico's en de al genomen stappen op het gebied van bewustwording
	Kwantitatieve kennismeting op basis van 300 medewerkers: de nulmeting inclusief infographic
	Rondje gebouw (voorbeeld cleandeskbeleid)
2	Resultaten van diverse metingen verzamelen en analyseren
	Opleveren van een implementatiestrategie en opleidingsplan waarin de leerdoelen van de organisatie en de diverse doelgroepen worden opgenomen
	Sessie met projectgroep en formulering voorstel DT/bestuur

Pakket 2: Basispakket

Fase	Basispakket BMC-safety
1	Kennismakingsgesprek
	Inventarisatie van organisatiedoelen, omgevingsfactoren, organisatierisico's en de al genomen stappen op het gebied van bewustwording
	Kennismeting met een standaardset van vragen inclusief infographic
	Gedragsmeting: rondje gebouw
2	Resultaten van diverse metingen verzamelen en analyseren
	Opleveren van een implementatiestrategie en opleidingsplan waarin de leerdoelen van de organisatie en de diverse doelgroepen worden opgenomen
3	**Activering en ondersteuning zijn geen onderdeel van het basispakket**
4	Bewustwordingsactiviteiten algemeen: - 2 x webinar basis IB&P voor alle medewerkers EN - 2 x interactieve basistraining IB en P voor doelgroep(en) naar keuze
5	Evaluatie en opbouw advies naar nieuwe cyclus (NB Nieuwe kennismeting zou ten behoeve van leercyclus 2 zijn)

Pakket 3: Mediumpakket

Fase	Mediumpakket BMC-safety
1	Kennismakingsgesprek
	Inventarisatie van organisatiedoelen, omgevingsfactoren, organisatierisico's en de al genomen stappen op het gebied van bewustwording
	Kennismeting op basis van 300 medewerkers: de (nul)meting inclusief infographic
	Gedragsmetingen (keuze uit een van de onderstaande op basis van resultaten kennismeting):
	○ Mysteryguest
	○ Social engineering
	○ Phishing telefoon
	Rondje gebouw (voorbeeld: controleren cleandeskbeleid)
2	Resultaten van kennis en gedragsmeting verzamelen en analyseren
	Opleveren van een implementatiestrategie en opleidingsplan waarin de leerdoelen van de organisatie worden opgenomen
	Presentatie aan inhoudelijk betrokkenen/MT/DT in afstemming met opdrachtgever
3	Activering BMC-safety Bewustwordings- en opleidingsprogramma
	● activeringsmateriaal aanleveren (2 infographics/posters, 5 intranetberichten)
	● ondersteuning bewustwordingsteam bij communicatie-uitingen
4	Bewustwordingsactiviteiten algemeen: - 2 x webinar basis IB&P voor alle medewerkers EN - 2 x interactieve basistraining IB en P voor doelgroep(en) naar keuze Keuze uit (zie tabel: losse activiteiten): - 1 x vakinhoudelijke training; EN - 1 x verdiepingstraining privacy en informatieveiligheid met een domein naar keuze EN - 1 x ludieke actie
5	Evaluatie en opbouw advies naar nieuwe cyclus (NB Nieuwe kennismeting zou ten behoeve van leercyclus 2 zijn)

Pakket 4: Premiumpakket

Fase	Premiumpakket BMC-safety (inclusief extra begeleiding)
1	Kennismakingsgesprek
	Bewustwordingsprojectgroep samenstellen
	Inventarisatie van organisatiedoelen, omgevingsfactoren, organisatierisico's en de al genomen stappen op het gebied van bewustwording
	Kick-off BMC-safety Bewustwordings- en opleidingsprogramma met stakeholders en projectgroep
	Kwantitatieve kennismeting op basis van 300 medewerkers: de nulmeting inclusief infographic
	Gedragsmetingen (keuze uit een van de onderstaande op basis van resultaten kennismeting):
	• Mysteryguest
	• Social engineering
	• Phishing (telefoon)
	Rondje gebouw (voorbeeld: controle cleandeskbeleid)
2	Resultaten van diverse metingen verzamelen en analyseren
	Opleveren van een implementatiestrategie en opleidingsplan waarin de leerdoelen van de organisatie worden opgenomen
	Sessie met projectgroep en formulering voorstel DT/bestuur
	Presentatie aan DT/bestuur ten behoeve van accordering plan
3	Activering BMC-safety Bewustwordings- en opleidingsprogramma
	• activeringsmateriaal aanleveren (3 infographics/posters, 7 intranetberichten)
	• ondersteuning bewustwordingsteam bij communicatie-uitingen
4	Bewustwordingsactiviteiten: - 2 x webinar basis IB&P voor alle medewerkers EN - 2 x interactieve basistraining IB en P voor doelgroep(en) naar keuze EN - 2 x vakinhoudelijke training; EN - 3 x verdiepingstrainingen privacy en informatieveiligheid met een domein naar keuze EN - 2 x ludieke acties
5	Evaluatie en opbouw advies naar nieuwe cyclus (NB Nieuwe kennismeting zou ten behoeve van leercyclus 2 zijn)

3.2 Overzicht pakketonderdelen/keuze-interventies

Hieronder staan de beschikbare keuze-interventies beschreven op het terrein van privacy en informatieveiligheid waarover we spreken in de verschillende pakketten. In een inspirerende leeromgeving stimuleren wij uw medewerkers om het maximale leerrendement uit een opleiding te halen. Uw medewerkers kunnen kennismaken met een nieuw werkterrein, nieuwe inzichten opdoen of zichzelf verdiepen in een specifiek thema.

A. Workshops bewustwording - algemeen

Workshop	Omschrijving
Webinar **Basis IB en P - alle medewerkers**	Tijdens deze bewustwordingssessies bieden onze adviseurs een divers en interactief programma aan waarbij inzicht wordt geboden in het belang van gedegen informatiebeveiliging en bescherming van persoonsgegevens. Ook komen de meest voorkomende risico's en valkuilen op het gebied van informatieveiligheid en privacy aan bod. We bieden uw medewerkers handvatten om met deze gevaren en valkuilen om te gaan. Tijdens de informatiebijeenkomst gaan we dieper in op: Privacyonderwerpen: • Basisbegrippen en uitgangspunten AVG • Persoonsgegevens en bijzondere persoonsgegevens • Transparantie • Verwerkingsverantwoordelijken en verwerkers • Bewaartermijnen • Toestemming • Meldplicht datalekken • Rechten van betrokkene(n) Informatieveiligheidsonderwerpen: • Basisbegrippen en uitgangspunten informatieveiligheid • Omgang wachtwoorden • Openbare WiFi • Clear screen en clear desk • Toegangsbeveiliging • 10 gouden regels • Beveiligingsincidenten • Herkennen van risico's bij dagelijkse werkzaamheden • Phishing
Basis IB en P - nieuwe medewerkers of een	Tijdens deze bewustwordingsbijeenkomst nemen onze adviseurs nieuwe medewerkers aan de hand van de gemeentelijke 'IBP-gedragsregels' mee in hun verantwoordelijkheden ten aanzien van

gekozen groep medewerkers (max. 40 deelnemers)	informatieveiligheid en privacy. Tevens gaan zij in op het belang van informatieveiligheid en de bescherming van persoonsgegevens en worden de meest voorkomende risico's en valkuilen op het gebied van informatieveiligheid en privacy besproken.
Basis IB en P - Lijnmanagement	Tijdens deze bijeenkomst wordt het belang van informatieveiligheid en de bescherming van persoonsgegevens onderbouwd. Daarnaast worden de verantwoordelijkheden van het MT toegelicht. informatieveiligheid en privacy is een lijnverantwoordelijkheid. Dat betekent dat de lijnmanagers en afdelingshoofden primair de verantwoordelijkheid dragen voor een goede informatieveiligheid en bescherming van persoonsgegevens op hun afdeling/binnen hun eenheid. Dit omvat ook de keuze van maatregelen en de uitvoering en handhaving daarvan. Als er vanuit het lijnmanagement geen aandacht is voor informatieveiligheid en privacy, vindt de rest van de organisatie het ook niet belangrijk.
Basis IB en P - Bestuur	Tijdens deze bijeenkomst nemen onze adviseurs uw bestuurders mee in het belang van informatieveiligheid en de bescherming van persoonsgegevens. Tevens worden de grootste risico's op het gebied van informatieveiligheid en privacy toegelicht. Het doel van deze bijeenkomst is het creëren van draagvlak voor gedegen informatiebeveiliging en bescherming van persoonsgegevens.
Train-de-trainer	Tijdens deze bijeenkomst wordt een selectie medewerkers getraind in het ambassadeurschap voor informatieveiligheid en/of privacy. Na deze bijeenkomst(en) hebben de ambassadeurs voldoende handvatten om zelf bewustwordingsactiviteiten te organiseren en uit te voeren.

B. Workshops bewustwording - domeinspecifiek

1. Burgerzaken/KCC	
Omschrijving workshop	Onze adviseurs nemen uw medewerkers van de afdeling Dienstverlening Burgerzaken/KCC mee in een aantal belangrijke aandachtspunten op het gebied van informatieveiligheid en privacy (waaronder ook de regelgeving PUN en Rijbewijzen). Er wordt onder andere stilgestaan bij de veiligheid rond de balies en in de backoffice. Ook krijgen uw medewerkers een aantal praktische tips, bijvoorbeeld over de omgang met waardedocumenten, dossiers, het verzenden/opslaan van fysieke en digitale bestanden en veilig thuiswerken.
Duur workshop	3 uur per workshop
Doelgroep workshop	Alle medewerkers

2. Sociaal Domein	
Omschrijving workshop	De uitdagingen binnen het Sociaal Domein op het gebied van privacy liggen voornamelijk in de uitgangspunten 'Eén gezin, één plan, één regisseur', onderlinge raadplegingen in het systeem ('wat'-/'dat'-informatie), hoe om te gaan met het registreren en delen van gegevens, fraudesignalen, geheimhoudingsplichten en toestemming. Onze adviseurs geven uw medewerkers praktische handvatten hoe om te gaan met deze en andere uitdagingen binnen het Sociaal Domein.
Duur workshop	3 uur per workshop, maatwerk mogelijk
Doelgroep workshop	Alle medewerkers en functies binnen het Sociaal Domein, inclusief management

3. Veiligheidsdomein (ondermijning/samenwerking RIEC)	
Omschrijving workshop	Tijdens deze workshop worden de aandachtspunten en uitdagingen van de gegevensuitwisseling bij ondermijning signalen besproken en de samenwerking met het Regionaal Informatie en Expertise Centrum (RIEC). Aandachtspunten zijn bijvoorbeeld: • het huidige LIEC-RIEC-stelsel onder het convenant; • de nieuwe Wet gegevensverwerking door samenwerkingsverbanden (Wgs);

	• de vraag: wat is ondermijning? • toezicht op gegevensverwerking; • begrippen: wat is een 'signaal' onder de Wgs? • intelligence en openbronnenonderzoek.
Duur workshop	3 uur per workshop, maatwerk mogelijk
Doelgroep workshop	Medewerkers werkzaam binnen het veiligheidsdomein van gemeente en samenwerkingspartners

4. Veiligheidsdomein (boa's)	
Omschrijving workshop	In deze workshop nemen onze adviseurs uw buitengewoon opsporingsambtenaren (boa's) mee in de Wet politiegegevens (Wpg) en de Algemene Verordening Gegevensbescherming (AVG). In deze workshop wordt onderscheid gemaakt tussen welke taken van de boa's onder de Wpg en welke taken onder de AVG vallen en wat dit betekent voor de werkzaamheden van de boa's. Ook wordt ingegaan op de vraag welke zaken (los of aanvullend op de AVG) ingericht moeten worden om te voldoen aan de Wpg.
Duur workshop	3 uur per workshop, maatwerk mogelijk
Doelgroep workshop	Medewerkers toezicht en handhaving bij onder andere gemeenten en gemeentelijke diensten

5. HRM	
Omschrijving workshop	In deze workshop wordt aandacht besteed aan de verschillende risicofactoren die zich in het HR-proces kunnen voordoen op het gebied van informatieveiligheid en privacy. Denk hierbij aan het sollicitatieproces (screening op basis van risicoprofielen), het omgaan met sollicitatie- en personeelsdossiers, het verstrekken van gegevens aan derden (arbodienst, leverancier bedrijfskleding et cetera), het inregelen van autorisatierechten, aandachtspunten bij het in-, door- en uitstroombeleid en de bewustwording van nieuwe medewerkers. Eveneens komen zaken als bewaartermijnen, recht op inzage et cetera aan de orde.
Duur workshop	3 uur per workshop
Doelgroep workshop	HR-medewerkers en leidinggevenden

6. Archief/DIV

Omschrijving workshop	Voorbeeld: Tijdens deze workshop worden uw medewerkers meegenomen in de informatieveiligheids- en privacyaspecten in de werkzaamheden van uw DIV-medewerkers. Hierbij kunt u denken aan onderwerpen als zaakgericht werken, logische toegangsbeveiliging, logging en crisisplannen, anonimisering van WOB-stukken, de eisen vanuit de Wpg. Ook de relatie met de Archiefwet en de Archiefinspectie komt uitgebreid aan de orde.
Duur workshop	3 uur per workshop
Doelgroep workshop	Medewerkers DIV en archief afdeling

7. Inkoop	
Omschrijving workshop	Deze workshop geeft duidelijkheid over de aandachtspunten voor privacy en informatieveiligheid die bij inkoop van belang zijn. Hierbij komt in ieder geval aan bod: waarmee uw medewerkers rekening moeten houden bij de screening van nieuwe aanbestedingen (verwerkersovereenkomsten, beveiligingseisen, VIR, GIBIT, overige wetgeving, ISO-certificering), de inrichting van de borging van privacy en informatieveiligheid in het inkoopproces en afspraken die vastgelegd moeten worden met nieuwe leveranciers of bij al bestaande leveranciersrelaties, inclusief contractmanagement dan wel het monitoren van de contractuele uitvoering van de afspraken.
Duur workshop	3 uur per workshop
Doelgroep workshop	Medewerkers inkoop en contractmanagement

8. Toegangsbeleid (authenticatie/autorisatie)	
Omschrijving workshop	Deze workshop biedt handvatten voor uw functionele applicatiebeheerders en andere deelnemers bij het inrichten van passende autorisaties. Onze adviseurs nemen uw medewerkers onder andere mee in onderwerpen als Identity Management, Authenticatie, Autorisatie en best practices voor de bijbehorende processen. Daarbij is het mogelijk om een eigen applicatie als voorbeeld in te brengen.
Duur workshop	3 uur per workshop
Doelgroep workshop	Functionele applicatiebeheerders, (proces)managers, projectleiders, informatieadviseurs, architecten, FG, CISO

9. Logging	
Omschrijving workshop	Deze workshop biedt handvatten voor uw functionele applicatiebeheerders en andere deelnemers bij het inrichten van logging en het gebruik daarvan bij het opsporen van inbreuken op de beveiliging en ongewenst gedrag. Daarbij worden methoden toegepast die de privacy van medewerkers zo goed mogelijk waarborgen. Aan de orde komen de doelen van logging, te loggen gegevens, de efficiënte analyse van loggegevens en mogelijke technische inrichtingen. Daarbij is het mogelijk om een eigen applicatie als voorbeeld in te brengen.
Duur workshop	3 uur per workshop
Doelgroep workshop	Functionele applicatiebeheerders, (proces)managers, projectleiders, informatieadviseurs, architecten, FG, CISO

10. Data Warehouse, Big Data en rapportage	
Omschrijving workshop	Deze workshop biedt handvatten voor iedereen die betrokken is bij de inrichting en het gebruik van data- warehouses om dit op een veilige en privacyvriendelijke manier te doen. Daarbij wordt ingegaan op het begrippenkader, Big Data en Kunstmatige Intelligentie, privacyrisico's en hoe die op te lossen en beveiliging van deze informatiesystemen.
Duur workshop	3 uur per workshop
Doelgroep workshop	DWH-beheerders, data-analisten, (proces)managers, projectleiders, informatieadviseurs, architecten, FG, CISO

C. Vakinhoudelijke trainingen

1. Privacy/security in projecten en Security by Design/default	
Omschrijving training	Privacy en Security by Design (PBD/SBD) betekent letterlijk: gegevensbescherming en beveiliging meenemen vanaf het ontwerp van nieuwe diensten, processen en ondersteunende informatiesystemen. Daarmee handelt u als organisatie proactief in plaats van reactief en zijn alle betrokkenen verantwoordelijk om privacy en beveiliging mee te nemen zodra er nieuwe ideeën tot stand komen. Dit vraagt om een gestructureerde aanpak van privacy en informatieveiligheid bij innovatie en in projecten en bij meer samenwerking tussen de verschillende vakgebieden binnen de gemeenten. De bedoeling van de workshop PBD is om alle leden van verschillende vakgebieden samen te brengen en te laten werken aan een praktijkcasus. In kleinere groepjes gaan de medewerkers uit elkaar om privacyvriendelijke en goed beveiligde oplossingen te zoeken voor de ingebrachte casus. De gemeente legt iets op. Hoe gaat u dat als gemeente inrichten op een manier die zo min mogelijk effect heeft op de privacy van burgers? Daarna komen de groepjes samen om de oplossingen te presenteren.
Duur workshop	3 uur per training
Doelgroep workshop	Projectleiders, informatieadviseurs, architecten en hun opdrachtgevers

2. Proces melden en afhandelen van beveiligingsincidenten en datalekken	
Omschrijving training	Tijdens deze training wordt de gemeentelijke meldprocedure voor beveiligingsincidenten stapsgewijs doorlopen met het ‘datalekteam’. Hiervoor maken onze adviseurs gebruik van actuele en herkenbare voorbeelden. Na deze trainingen heeft het ‘datalekteam’ handvatten om toekomstige beveiligingsincidenten en datalekken correct af te handelen. Ook gaan we in op de samenhang met IT-incident, management- en continuïteitsmanagement.
Duur workshop	3 uur per training
Doelgroep workshop	Zelf doelgroep bepalen, bijvoorbeeld: CISO, FG, continuïteitsmanagers, IT-(proces)managers, applicatiebeheerders, juristen

3. DPIA-training	
Omschrijving training	Het Data Protection Impact Assessment (DPIA) is een instrument om vooraf de privacyrisico's van de dataverwerking te kunnen inschatten. Een DPIA is verplicht als dataverwerking waarschijnlijk een hoog privacyrisico oplevert. Tijdens het theoretische gedeelte komen de volgende onderwerpen aan bod: • Wanneer is een DPIA verplicht? • Hoe is het DPIA-proces ingericht? • Uitleg over het eigen model en/of overige praktische modellen • Mogelijke risico's en maatregelen • Rollen en verantwoordelijkheden DPIA Tijdens het praktische gedeelte van de workshop gaan de medewerkers daadwerkelijk een DPIA uitvoeren aan de hand van een (standaard)casus. Gezamenlijk wordt de casus besproken en wordt er een risicoanalyse gemaakt. Daarna wordt er gekeken naar de risico's, de maatregelen die daarop genomen moeten worden en de restrisico's.
Duur workshop	3 uur per training
Doelgroep workshop	Projectleiders, Privacy Officers, FG, (C)ISO. Maatwerk is mogelijk.

4. Toegangsbeleid/Identity Access Management (IAM)	
Omschrijving training	De training gaat in op de aspecten van toegangsbeleid en hun implementatie: Identificatie, Authenticatie, Autorisatie, zowel on-premise als in de cloud. Daarvoor worden best practices behandeld, zoals wachtwoordbeleid, tweefactorauthenticatie en autorisatiematrices. Aan de orde komen ook technische standaarden en de risico's van het omzeilen van de toegangscontrole. Vervolgens kijken we naar de procesmatige vormgeving van deze processen en de link met het HR-proces.
Duur workshop	3 uur per training
Doelgroep workshop	(C)ISO's, IT-medewerkers

5. Cryptografie	
Omschrijving training	Bij het benaderen van een website wordt meestal een beveiligde verbinding opgezet (https ofwel het slotje dat in beeld verschijnt). Hieraan ten grondslag ligt cryptografie. Cryptografie

	kan gebruikt worden om ervoor te zorgen dat data onleesbaar is voor onbevoegden, maar ook om te garanderen dat gegevens niet ongemerkt aangepast kunnen worden voor het vaststellen van de identiteit van personen of de entiteit van systemen en zelfs voor het digitaal ondertekenen van documenten en berichten met mogelijk eenzelfde juridische geldigheid als een handtekening op papier. In deze basiscursus over cryptografie gaan we in op de mogelijkheden van cryptografie en de basisprincipes ervan, zodat de deelnemers aan het eind van de cursus een beeld hebben van wat er met cryptografie mogelijk is, hoe het werkt en waarop gelet moet worden. Ook kijken we naar manieren om eenvoudig de correcte configuratie te controleren. Ten slotte kijken we kort naar de ontwikkeling van de quantumcomputer en de gevolgen daarvan voor cryptografie.
Duur workshop	3 uur per training
Doelgroep workshop	IT-medewerkers, applicatiebeheerders

6. Verdiepende trainingen IBP-onderwerpen	
Omschrijving training	In overleg kunt u ook kiezen voor een verdiepende training in een van de onderstaande onderwerpen: - grondslagen (in het bijzonder toestemming eventueel toestemmingsregister); - verwerkers en verwerkersovereenkomsten; - het verwerkingsregister; - convenanten; - rollen: verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke en verwerker; - verzoeken van betrokken (in het kader van rechten van betrokken, zoals inzagerecht); - datawarehouse en privacy.
Duur workshop	3 uur (maatwerk in overleg)
Doelgroep workshop	Voor iedereen die er meer van wil weten en wil begrijpen hoe de AVG werkt.

D. Gedragsmetingen

Gedragsmeting	Omschrijving
Rondgang gebouw	Aan de hand van een checklist beoordelen onze adviseurs de fysieke beveiligingsmaatregelen die zijn getroffen in het gemeentehuis. Er wordt aandacht geschonken aan de verschillende zones (omgeving van het gebouw, de publieke ruimte, de medewerkerszone, beveiligde ruimtes en kritische ruimtes). Ook wordt er gecheckt of het cleandesk- en clearscreenbeleid wordt nageleefd.
Mysteryguest	Wilt u weten hoe goed uw gemeentehuis beveiligd is en hoe scherp uw medewerkers zijn op mogelijke insluipers? De mysteryguest kijkt op welke manieren hij/zij het gebouw van de gemeente kan binnengaan en tot welke ruimtes hij/zij zich toegang kan verschaffen. De bevindingen van de mysteryguest kunnen gepresenteerd worden aan het MT/DT/B enW om eventuele risico's aan te tonen. Dit draagt bij aan het 'commitment' op het gebied van privacy en informatieveiligheid.
Mysterycaller	Met een Mysterycaller actie wordt onderzocht of de maatregelen op het gebied van informatieveiligheid en privacy goed werken en de afspraken en procedures door medewerkers worden nageleefd. Daarnaast worden medewerkers zich bewust gemaakt van hun houding en gedrag. Een Mysterycaller actie helpt om de ogen van medewerkers en management te openen en om aandacht te vragen voor het onderwerp informatieveiligheid en privacy.

E. Ludieke acties

Ludieke actie	Omschrijving
Crisisgame CIP: incidentensimulatie	De crisisgame is een simulatie waarin een bericht is binnengekomen van een cybercrimineel die zegt dat hij de organisatie heeft gehackt. De organisatie is vrijwel volledig digitaal, met alle kwetsbaarheden van dien. Het doel van deze simulatie is om de hack zo efficiënt mogelijk te bestrijden, te voorkomen dat data bij onbevoegden terechtkomt en te achterhalen wie de dader is.

Opschoondag (dataminimalisatie)	Het organiseren van een opruimdag kan ingezet worden als bewustwordingstool om medewerkers meer bewust te maken van de manier waarop ze met informatie omgaan. Het doel kan zijn dat duidelijk is welke informatie waar wordt opgeslagen, dat (belangrijke) informatie uit mailboxen en persoonlijke schijven wordt gehaald en beter toegankelijk wordt voor anderen of dat de huidige dossiervorming compleet wordt gemaakt. De insteek van de opruimdag bepaalt hoe de organisatie en promotie eruitzien. Het zal dus afhankelijk zijn van de organisatie en het doel hoe de opruimdag eruit gaat zien. BMC-safety biedt organisatorische tips en marketingtips die kunnen helpen bij het maken van een plan van aanpak opruimdag.
Bordspel: Spion op je pad	In samenwerking met het Ministerie van Economische Zaken heeft de IBD het bordspel 'Spion op je pad' ontwikkeld. Onze adviseurs kunnen uw medewerkers begeleiden bij dit spel. In het spel maken de deelnemers kennis met de dilemma's rondom informatieveiligheid en privacy.[1] Spelers moeten er tijdens het spel voor zorgen dat de spion geen waardevolle informatie vanuit de organisatie in zijn bezit krijgt. Het spel wordt gespeeld onder tijdsdruk en onder begeleiding van een spelleider. De spelers werken samen tegen de spion, waarbij incidenten continu op de loer liggen. Het doel van dit spel is het vergroten van bewustzijn en alertheid in de omgang met gevoelige informatie.

[1] www.informatiebeveiligingsdienst.nl (zoek op: producten, Overzicht bewustwordingscampagnes, Spion op je pad)

BMC

Databankweg 26D
3821 AL Amersfoort

P.O. box 490
3800 AL Amersfoort

(033) 496 52 00
info@bmc.nl
www.bmc.nl

KvK BMC Implementatie 31046509
IBAN NL61ABNA0626023106
BTW NL80.55.22.827 B.01

Kijk voor meer info op onze website: bmc.nl