Informatiebeveiligingsbeleid 2025
&
Informatiebeveiligingseisen

Informatiebeveiligingsbeleid 2025

Inleiding
MTB erkent dat informatiebeveiliging steeds belangrijker wordt. MTB wil in alle opzichten een betrouwbare partner zijn. Zorg en respect zijn belangrijke kernwaarden in het handelen en de omgang tussen de medewerkers en cliënten. Een betrouwbare informatievoorziening waarbij de informatie van inwoners en medewerkers en cliënten wordt beschermd en de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens is geborgd, is hier onlosmakelijk mee verbonden. Niet alleen kan inadequate beveiliging leiden tot beschadiging van het vertrouwen, maar ook kunnen medewerkers geschaad worden als bijvoorbeeld privéinformatie openbaar wordt of identiteitsgegevens worden misbruikt.
Dit document legt de basis voor informatiebeveiliging binnen MTB en is één van de thema's die onderdeel uitmaakt van de Baseline Informatiebeveiliging Overheid (BIO[1]).

Beleid van Informatiebeveiliging
Gegevens t.b.v. informatievoorziening zijn één van de voornaamste bedrijfsmiddelen van MTB. Het verlies van gegevens, uitval van ICT-systemen en/of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie kan ernstige gevolgen hebben voor de bedrijfsvoering. Informatieveiligheid is van groot belang.

Beleidsdoelstelling voor informatiebeveiliging
De directie van MTB wil door middel van dit beleid veilige en betrouwbare diensten leveren en vertrouwen bieden aan onze klanten en medewerkers door informatie en persoonsgegevens te beschermen tegen interne en externe bedreigingen Het betreft hier zowel opzettelijke als onbedoelde bedreigingen, die de continuïteit en/of de reputatie van de onderneming en haar belanghebbenden kunnen schaden.

Onze informatiebeveiliging richt zich op de volgende vier aspecten:
- Beschikbaarheid, de informatie moet op de gewenste momenten beschikbaar zijn;
- Integriteit, de informatie moet juist en volledig zijn en de informatiesystemen moeten juiste en volledige informatie opslaan en verwerken;
- Vertrouwelijkheid, de informatie moet alleen toegankelijk zijn voor degene die hiervoor bevoegd is;
- Privacy, de bescherming van persoonsgegevens en de rechten van de betrokkenen.

MTB wil ervoor zorgen dat de beheersmaatregelen om bovenstaande aspecten te bereiken op transparante wijze ingevoerd en opgeslagen worden.

[1] De Baseline Informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen overheden.

Het doel is enerzijds om het beveiligingsniveau te verhogen, maar anderzijds ook om onze werkwijze van risicobeheersing - op basis van een selectie van passende maatregelen - aantoonbaar te maken aan derden. In het geval van een datalek kan aan de autoriteit persoonsgegevens aangetoond worden dat er passende maatregelen genomen zijn.
MTB heeft haar ICT-diensten uitbesteed. De technische beveiliging van de ICT-omgeving (o.a. virusscanner, toegangsbeveiliging van buitenaf) van MTB ligt bij de ICT-leverancier.

Leiderschap, betrokkenheid en verantwoordingsplichten
Het management van MTB neemt alle technische en organisatorische maatregelen die noodzakelijk en in economische zin rendabel zijn om:

- de veiligheid van de informatie, medewerkers, klanten en cliënten te waarborgen;
- aan de relevante wet- en regelgeving te voldoen;
- de continuïteit van de bedrijfsvoering te waarborgen;
- de reputatie te beschermen.

De verantwoordingsplicht voor de privacywetgeving ten aanzien van rechtmatigheid, transparantie, doelbinding en juistheid wordt aangetoond met behulp van:

- het bijhouden van een register van verwerkingsactiviteiten;
- het uitvoeren van een Data Protection Impact Assessment voor gegevensverwerkingen met een hoog privacy risico;
- het bijhouden van een register van datalekken die zijn opgetreden;
- het aantonen dat een betrokkene daadwerkelijk toestemming heeft gegeven voor een gegevensverwerking wanneer MTB voor een verwerking toestemming nodig heeft. (bijvoorbeeld bij foto's).

Het management van MTB is verantwoordelijk voor de werking van de informatiebeveiliging en zal de taken en verantwoordelijkheden voor de implementatie en het beheer van de maatregelen voortkomend uit dit beleid beleggen bij de medewerkers.

Doelen
MTB heeft als streven om die maatregelen te treffen, die noodzakelijk zijn en die binnen alle redelijkheid en billijkheid voor de organisatie in economische zin haalbaar zijn.
Hierbij dient rekening gehouden te worden met zowel de beschikbare middelen als de beschikbare mancapaciteit. Daarnaast kan een beperkt risico ook – mits onderbouwd met argumenten – worden geaccepteerd, zonder dat er verdere maatregelen geïmplementeerd worden.

De achterliggende doelen van maatregelen rondom informatiebeveiliging zijn:

- de veiligheid van de informatie en het personeel te waarborgen;
- aan de relevante wet- en regelgeving te voldoen;

- de continuïteit van de bedrijfsvoering te waarborgen;
- de reputatie als betrouwbare partner te beschermen.

Risicobewustzijn
Het ‘informatie-, cyber-, en privacybeveiliging risicobewustzijn’, ofwel security awareness, van alle medewerkers is de sleutel tot een effectieve informatiebeveiliging. Het belang van security awareness wordt volledig onderkend door het management en wordt gestimuleerd door het onderwerp periodiek te behandelen op werkoverleggen en publicaties via onder meer het intranet. Al sinds 2022 loopt er een continue training voor alle gebruikers via het trainingsprogramma van Awaretrain.

Toegang en verwerking van informatie
Toegang tot informatie en IT-faciliteiten wordt op basis van ‘need to know’ beperkt zodat gebruikers toegang krijgen tot datgene wat noodzakelijk is voor het uitvoeren van de functie. Dit is één van de essentiële principes van veilig informatiebeheer. Tweede uitgangspunt is om niet meer gegevens te verwerken dan noodzakelijk.
Beveiligingsmaatregelen die worden getroffen, hebben betrekking op zowel door MTB verstrekte middelen als privé-apparatuur die voor zakelijk gebruik worden ingezet ('bring your own device' (BYOD)). Op privé-apparatuur waarmee verbinding wordt gemaakt met het netwerk van MTB is MTB bevoegd om beveiligingsinstellingen af te dwingen, als de situatie hierom vraagt. Extern toegang tot het netwerk van MTB vindt plaats via multifactor authenticatie.

De toegang tot informatiesystemen wordt toegekend door het management of leidinggevende op basis van de functie en taken van de individuele medewerkers.

Borging van de informatiebeveiliging
Borging van de informatiebeveiliging vindt plaats door middel van vastlegging van de overeengekomen werkwijze in procesbeschrijvingen, richtlijnen, gedragscodes, procedures, en werkinstructies.
Periodiek vindt er een penetratietest[2] plaats om vast te stellen dat er sprake is van een toereikende mate van beveiliging van de data binnen de applicaties.
Het management van MTB dient te waarborgen dat het informatiebeveiligingsbeleid wordt nagevolgd en regelmatig wordt beoordeeld en indien nodig aangepast aan organisatorische veranderingen en/of technologische ontwikkelingen.

Medewerkersverantwoordelijkheid en naleving
Alle medewerkers van MTB hebben de persoonlijke verantwoordelijkheid om dit beleid na te leven en opvolging te geven aan de maatregelen die voortvloeien uit dit beleid zoals richtlijnen,

[2] Door middel van een penetratietest (ook wel pentest genoemd) kan inzichtelijk worden gemaakt waar de risico's en kwetsbaarheden van de onderzochte systemen liggen en kunnen verbeteringen gericht worden doorgevoerd om de beveiliging te versterken en daarmee de risico's en kwetsbaarheden te bestrijden.

procedures en werkinstructies.
Wanneer een medewerker een incident, tekortkoming of overtreding van dit beleid ziet of ervaart, dient hij/zij dit te melden bij de Functionaris Gegevensbescherming.
Naleving van het beleid wordt gecontroleerd. Het niet naleven van het beleid kan tot disciplinaire maatregelen leiden. Jaarlijks wordt er een verslag uitgebracht.

Geldigheid en evaluatie
Het management van MTB is eigenaar van dit beleidsdocument. Dit beleid is drie jaar geldig en wordt minimaal één keer per jaar geëvalueerd op:

- naleving;
- de tactische en operationele uitvoering ervan;
- de stand van de techniek (beveiliging en bedreigingen);
- voortschrijdend inzicht;
- veranderende wet- en regelgeving;
- mogelijke reorganisaties of organisatorische veranderingen.

Op grond van de jaarlijkse beoordeling, veranderende wet- en regelgeving of door andere omstandigheden, kan dit beleid tussentijds bijgesteld worden.

MTB Informatiebeveiligingseisen

Informatiebeveiligingseisen

Bij de aanschaf van een ICT-product of ICT-dienst of bij het verlengen van een (onderhouds)contract welk betrekking heeft op een bestaand ICT-product of ICT-dienst, dient te worden getoetst of het ICT-product of de ICT-dienst voldoet aan de actuele eisen die aan het beveiligen van informatie worden gesteld. Deze informatiebeveiliging eisen zijn onlosmakelijk gekoppeld aan het inkoopproces.

In dit document zijn de eisen welke betrekking hebben op informatiebeveiliging beschreven. Om de risico's op verlies/diefstal van data en uitval van het ICT-product of de ICT-dienst te minimaliseren, dienen een aantal basismaatregelen in acht genomen te worden.

“Pas toe of leg uit”

MTB past hierbij het “Pas toe of Leg uit” principe toe. Dit houdt in dat bij het betreffende ICT-product of ICT-dienst gebruik wordt gemaakt van standaarden welke zijn beschreven door Forum Standaardisatie.Forum Standaardisatie is een adviescommissie met deskundigen uit diverse overheidsorganisaties, het bedrijfsleven en de wetenschap. De leden worden op persoonlijke titel benoemd door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Het Forum wordt ondersteund door het Bureau Forum Standaardisatie (BFS). Dit bureau is gehuisvest bij Logius, de dienst digitale overheid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

‘Pas toe’ houdt in dat, op het moment dat een ICT-product of ICT-dienst wordt aanschaft, deze moet voldoen, afhankelijk van het betreffende toepassingsgebied, aan de verplichte standaarden voor het toepassingsgebied zoals deze beschreven zijn in de 'Pas toe of leg uit'-lijst. De ‘Pas toe of leg uit’-lijst is terug te vinden op de website van Forum Standaardisatie (https://www.forumstandaardisatie.nl/open-standaarden/verplicht).

Afwijken van het gebruik van de voorgeschreven standaarden mag alleen als een dergelijke dienst of product in onvoldoende mate wordt aangeboden, het product of dienst onder de geldende standaard onvoldoende veilig of zeker functioneert of om een andere reden die van bijzonder gewicht is. De afwijking en de reden daarvan moeten beschreven worden. Dit is de betekenis van ‘leg uit’.

Basismaatregelen

MTB eist van de leverancier van een ICT-product of ICT-dienst dat deze, indien van toepassing op het ICT-product of ICT-dienst, de volgende basismaatregelen in acht neemt.

1. Regelmatig installeren van updates

   De leverancier brengt regelmatig, doch minimaal 1 maal per jaar, functionele en technische updates uit.

   In het geval van een geconstateerde kwetsbaarheid zorgt de leverancier voor een patch om de kwetsbaarheden in hun software te verhelpen. De leverancier brengt de corrigerende patch zo spoedig uit na het constateren van de kwetsbaarheid. Deze patch zal, in overleg met MTB, worden geïnstalleerd.

   In het geval van een geconstateerd beveiligingslek zorgt de leverancier ervoor dat dit middels een security patch zo spoedig mogelijk gedicht wordt. De leverancier informeert MTB binnen 24 uur na het constateren van het beveiligingslek over de mitigerende maatregelen die zullen worden toegepast.

2. Loginformatie

   De leverancier zorgt ervoor dat binnen het ICT-product de mogelijkheid bestaat tot het loggen van het volgende:

- Systeemlogging
- Netwerklogging
- Applicatielogging
- Cloudlogging

Deze logbestanden dienen ten minste 1 maand bewaard te blijven en voor MTB beschikbaar te zijn voor onderzoek.
Daarnaast dient de leverancier ervoor te zorgen dat het ICT-Product de mogelijkheid biedt tot het instellen van alarmering. Het instellen van de alarmeringen dient in overleg en op verzoek van MTB te geschieden.

Denk hierbij aan alarmeringen welke betrekking hebben op bijvoorbeeld:
- Verdachte inlogpogingen
- Benaderen vertrouwelijke data

In het geval van een datalek dient de leverancier mee te werken aan het eerste verzoek tot verschaffen van loginformatie.

3. AVG

Het ICT-Product en/of ICT-Dienst voldoet aan de, door de AVG gestelde, eisen. Dit houdt onder andere in dat aan de volgende eisen moet worden voldaan:
- De data wordt opgeslagen bij een datacenter welke in de Europese Unie is gevestigd
- Indien van toepassing zal een verwerkersovereenkomst worden afgesloten
- De leverancier levert op verzoek een DPIA aan welke betrekking heeft op de werking van het ICT-Product en/of ICT-Dienst
- Het ICT-Product biedt de mogelijkheid om data te anonimiseren
- Het ICT-Product biedt de mogelijkheid om date te verwijderen indien dit door belanghebbenden wordt gevraagd of indien de wettelijke bewaartermijn is overschreden
- In het geval van een datalek aan zijde van de leverancier, dient deze dit binnen 24 uur bij de Functionaris Gegevensbescherming (FG) van MTB te melden

4. Multifactor authenticatie (MFA)

Het ICT-product en/of ICT-dienst biedt de mogelijkheid tot het afdwingen van Multifactor authenticatie (MFA). Hierbij gaat de voorkeur uit tot het gebruik van MFA middels de Microsoft Authenticator app.

5. Single Sign On (SSO)

Het ICT-product en/of ICT-dienst dient de mogelijkheid te bieden om middels SSO toegang te krijgen tot het ICT-product en/of ICT-dienst. Om dit te realiseren dient vanuit het ICT-product en/of ICT-dienst een koppeling gerealiseerd te worden met Azure Active Directory.

6. Back-up

Leverancier hanteert de 3-2-1 regel als back-up strategie. Deze regel houdt in dat 3 versies van de data op 2 verschillende media wordt opgeslagen en waarvan één kopie fysiek op een andere locatie wordt bewaard.

De back-ups dienen versleuteld te worden opgeslagen conform de daarvoor geldende standaarden.

De leverancier heeft een restore procedure in place waarbij jaarlijks een restore test plaatsvindt. Deze restore test heeft betrekking op zowel het computersysteem als ook de data. De leverancier rapporteert hierover aan MTB.

7. Toegang tot data en diensten

De leverancier van het ICT-product en/of ICT-dienst verleent toegang tot het betreffende product en/of dienst vanuit het “principle of least privilege”. Dit houdt in dat medewerkers alleen toegang tot de data en systemen krijgen welke daadwerkelijk nodig zijn voor het uitvoeren van hun taak. Dit geldt zowel voor user accounts als ook voor fysieke toegang tot data.

Tevens dient een strikte scheiding tussen een user account en beheer account gerealiseerd te worden.

8. Versleutelen van data en dataverkeer

De leverancier van het ICT-product en/of ICT-dienst dient ervoor te zorgen dat de data middels veilige encryptiesoftware versleuteld wordt. Hiervoor dient de leverancier gebruik te maken van de standaarden zoals deze door Forum Standaardisatie zijn gedefinieerd.

Indien sprake is van digitale uitwisseling van gegevens met andere systemen, dient het dataverkeer, conform de door het National Cyber Security Center (NCSC) opgestelde ICT beveiligingsrichtlijnen, vormgegeven te zijn.