# Merlin – Securitybeleid

## Introductie

Merlin helpt haar klanten met praktische softwaretools voor het voorbereiden op, ondersteunen tijdens en verbeteren van het crisismanagement.

Om dit te kunnen doen moeten we ervoor zorgen dat uw data veilig is, en het beveiligen hiervan is een van onze hoogste prioriteiten. We zijn voorstander van transparantie over onze beveiligingsprincipes en helpen u om onze benadering te begrijpen.

Onze beveiliging is afgestemd op de ISO 27001 norm en wordt regelmatig gecontroleerd en beoordeeld door derde partijen.

### Beveiliging van personeel

Personele maatregelen zijn van toepassing op alle tijdelijke en vaste, interne en externe werknemers en leveranciers die toegang hebben tot CrisisSuite, haar interne informatiesystemen en/of toegang tot Merlin's kantoorruimte.

Alvorens toegang wordt afgegeven voor systemen moeten alle werknemers akkoord gaan met de geheimhoudingsverklaring, een achtergrond screening doorstaan en een securitytraining bijwonen. Deze training omvat privacy en security onderwerpen, inclusief device security (BYOD), acceptabel gebruik, voorkomen van malware, fysieke beveiliging, dataprivacy, accountbeheer, wachtwoordbeheer, en incidentrapportage.

Bij beëindiging van de werkzaamheden wordt alle toegang tot systemen onmiddellijk uitgeschakeld.

### Security en privacy training

Tijdens het dienstverband moeten alle medewerkers minstens een keer per jaar hun kennis van privacy en security opfrissen. De medewerkers ondertekenen dat zij Merlin's informatiebeveiligingsbeleidstukken hebben gelezen en zich daaraan houden. Sommige medewerkers, zoals beheerders en ondersteunend personeel, die extra toegang tot systemen of gegevens hebben, krijgen aanvullende werk specifieke training over privacy en beveiliging. Werknemers zijn verplicht om veiligheids- en privacy problemen te melden. Werknemers zijn geïnformeerd dat niet-naleving van beleid gevolgen tot en met beëindiging van het dienstverband kunnen opleveren.

### Toegewezen security professionals

Merlin heeft rollen en verantwoordelijkheden gedefinieerd om te bepalen welke rollen in de organisatie verantwoordelijk zijn voor de werking van de verschillende aspecten van ons Managementsysteem voor Informatiebeveiliging (ISMS). De verantwoordelijkheden van elke rol zijn gedetailleerd beschreven in onze beveiligingsdocumenten.

Merlin heeft een Security Manager aangesteld met de algemene verantwoordelijkheid voor de implementatie en het beheer van ons ISMS.

## Beleid en standaarden

Merlin onderhoudt een reeks beleidsdocumenten, normen, procedures en richtlijnen die de werknemers de weg wijzen voor het gebruik van ons ISMS. Onze beveiligingsdocumenten zorgen ervoor dat onze klanten erop kunnen vertrouwen dat onze werknemers zich veilig en ethisch gedragen. Beveiligingsdocumenten omvatten, maar zijn niet beperkt tot:

- Bring Your Own Device (BYOD)
- Aanvaardbaar Gebruik
- Geclassificeerde Informatie
- Telewerken
- Toegangsbeleid
- Bedieningsprocedures voor Beheersing van ICT
- Beveiligde ontwikkeling
- Beveiligingsbeleid Leveranciers
- Incidentbeheer
- Bedrijfscontinuïteit
- Regelmatig uitvoeren van risicobeoordelingen, audits, penetratietesten
- Plan voor Training & Bewustzijn

De beleidsdocumenten zijn levende documenten: Zij worden regelmatig beoordeeld en bijgewerkt en indien nodig beschikbaar gesteld aan alle werknemers op wie zij van toepassing zijn.

## Audits, wet- en regelgeving, en derde partij beoordelingen

*Audits*

Merlin evalueert het design en de operatie van haar algemene ISMS voor de naleving van interne en externe normen. Merlin laat zich beoordelen door externe auditors. Auditresultaten worden gedeeld met het management en alle bevindingen worden opgevolgd.

*Penetratietesten*

Merlin laat onafhankelijke instanties regelmatig applicatie-level penetratietesten uitvoeren. Resultaten van deze testen worden gedeeld met het management. De gerapporteerde bevindingen worden geprioriteerd en aangepakt.

*Wettelijke naleving*

Merlin maakt gebruik van toegewijde juridische en compliance professionals. Deze professionals zijn ingebed in de ontwikkelingscyclus en beoordelen producten en eigenschappen of ze voldoen aan de wettelijke vereisten.

## Security & Privacy by Design

### Secure Software Development

Merlin beoordeelt de beveiligingsrisico's van elk softwareontwikkelingsproject volgens Secure Software Development. Voor de voltooiing van de ontwerpfase onderneemt Merlin een beoordeling om het beveiligingsrisico van ingevoerde softwareveranderingen te kwalificeren. Deze risicobeoordeling maakt gebruik van zowel de OWASP Top 10 als de ervaring van Merlin's Security experts. Op basis van deze analyse creëert Merlin een aantal eisen waaraan voldaan moet worden voordat de resulterende verandering aan het product wordt gekoppeld.

Alle code wordt opgeslagen in een versiebeheer omgeving. Codewijzigingen zijn onderworpen aan peer reviews en continue integratie testen.

### Privacy by Design

Bij invoering van nieuwe verwerkingen van persoonsgegevens of bij wijzigingen worden vanaf het begin ontwerpcriteria gehanteerd waarmee invullen wordt gegeven aan het principe van "privacy by design".

## Bescherming van klantengegevens

De focus van Merlin's securityprogramma is om ongeautoriseerde toegang tot klantengegevens te voorkomen. Daartoe neemt ons team uitgebreide stappen om risico's te identificeren en te beperken, om de best practices te implementeren en voortdurend te evalueren om te verbeteren.

Meer informatie over privacy vindt u in ons Privacybeleid op http://www.merlincrisis.com/privacy-policy.

### Data encryptie 'in transit and at rest'

De gegevens tussen Merlin-klanten en de Merlin-dienst worden over openbare netwerken verzonden met behulp van sterke encryptie. De verbinding tussen de client (uw laptop, PC, tablet of smartphone) en de CrisisSuite server is uitsluitend mogelijk op basis van SSL beveiligde protocollen (https, wss, ssh), waardoor de communicatie tussen cliënt en server afgeschermd blijft.

### Netwerkbeveiliging

Binnen Merlin zijn regels opgesteld voor het versturen van informatie over publieke netwerken. De methode en het niveau van beveiliging wordt bepaald aan de hand van de toegewezen classificatie aan informatie.

### Classificatie en opslaan van data

Binnen Merlin wordt informatie geclassificeerd aan de hand van de volgende criteria:

- Waarde van de informatie gebaseerd op de gevolgen beoordeeld gedurende risicobeoordeling.
- Gevoeligheid en kritiek zijn van informatie gebaseerd op het hoogst berekende risico voor elk item van informatie gedurende risicobeoordeling.
- Wetgeving en contractuele verplichtingen gebaseerd op de Lijst Wet-, Regelgeving en Contractuele Verplichtingen.

Er wordt onderscheidt gemaakt tussen classificatie niveaus waarbij elk classificatie niveau is gekoppeld aan een set beveiligingsmaatregelen.

### Geautoriseerde toegang

Om de risico's van gegevensblootstelling te minimaliseren, volgt Merlin het principe van *need to know*. Werknemers hebben alleen toegang tot gegevens die ze redelijkerwijs nodig hebben om hun huidige taken te vervullen. Om dit te handhaven gebruikt Merlin de volgende maatregelen:

- De toegang van elke gebruiker wordt regelmatig beoordeeld om ervoor te zorgen dat de toegekende toegang nog steeds geschikt is voor de huidige werkverantwoordelijkheden van de gebruiker.
- Om het risico van onbevoegde toegang tot data verder te verminderen, past Merlin waar mogelijk twee-factor-authenticatie toe voor toegang tot systemen van derden.
- Merlin vereist dat personeel een goedgekeurde wachtwoordmanager gebruikt. Wachtwoordmanagers genereren, opslaan en invoeren unieke en complexe wachtwoorden. Gebruik van een wachtwoordmanager helpt bij het voorkomen van wachtwoordhergebruik, phishing en ander gedrag dat de beveiliging kan reduceren.

### Systeem monitoring, logging en alarmering

Binnen Merlin zijn rollen en verantwoordelijkheden vastgesteld voor zowel het controleren van de logs van automatisch gerapporteerde fouten als ook voor het registreren van fouten gerapporteerd door gebruikers om te analyseren waarom fouten optreden en om geschikte corrigerende acties te nemen.

### Bring Your Own Device (BYOD)

Merlin ondersteunt het gebruik van BYOD voor zakelijk gebruik. Dit geldt alleen voor werknemers die anders niet in staat zouden zijn om het werk op een andere wijze uit te voeren. Er wordt een lijst bijgehouden van de functienamen en/of welke medewerkers die BYOD mogen gebruiken, tezamen met de applicaties en databases waartoe zij toegang mogen hebben met hun eigen apparaten.

Daarnaast stelt Merlin diverse regels aan het gebruik van BYOD en is er een minimumconfiguratie vereist voor elk type device.

### Reageren op incidenten

Elke werknemer, leverancier of een andere derde partij die in contact komt met informatie en/of systemen van Merlin dient elke bedreiging, incident of gebeurtenis aan een systeem die zou kunnen leiden tot een mogelijk incident aan de Security Manager te melden. Er zijn diverse procedures ontwikkeld om snel en adequaat te reageren op incidenten.

Alle incidenten worden regelmatig beoordeeld en geëvalueerd om ervan te leren.

### Verwijdering en vernietiging van apparatuur en media

Binnen Merlin worden regels gehanteerd over het verwijderen en/of vernietigen van apparatuur en media voordat het wordt weggegooid, verkocht, gedoneerd, verzonden, gerepareerd, hergebruikt of aan een andere gebruiker wordt gegeven.

### Clear desk & clear screen

Binnen Merlin wordt er gewerkt conform het clear desk en clear screen beleid. Dit houdt in dat indien de geautoriseerde persoon niet op zijn/haar werkplek zit, dient hij/zij de informatie, papieren, opslagmedia, van het bureau of andere plaatsen zoals printers, kopieerapparaten etc. moeten worden verwijderd om ongeautoriseerde toegang te voorkomen.

Op dezelfde wijze geldt dat alle gevoelige informatie van het beeldscherm verwijderd dient te worden en dat schermvergrendeling wordt toegepast wanneer de geautoriseerde persoon zijn/haar werkplek verlaat.

## Bedrijfscontinuïteit

Merlin maakt gebruik van een hostingprovider. De servers zijn redundant uitgevoerd en worden 24/7 gemonitord. De serverruimtes worden 24/7 bewaakt. Systeemruimtes zijn voorzien van een redundant uitgevoerde stroomvoorziening met een back-up van dieselgeneratoren. De datacenters voldoen aan de strengste normen op het gebied van branddetectie, luchtkoeling en toegangsbeheer. Het door CrisisSuite gebruikte netwerk garandeert een uptime van 99,99%.

## Derde partijen

Om de business efficiënt te runnen vertrouwt Merlin op dienstverlenende organisaties. Waar de dienstverlenende organisaties de secundaire productie van Merlin kunnen beïnvloeden, neemt Merlin maatregelen om ervoor te zorgen dat het beveiligingsniveau wordt gewaarborgd. Merlin legt afspraken vast die vereisen dat dienstverleners zich houden aan de verplichtingen die Merlin aan hen hebben gesteld. Merlin controleert ten minste een keer per jaar de effectieve werking van de beveiligingsmaatregelen van de organisatie.

De datacenters zijn volgens ISO9001, ISO27001, ISO14001 en NEN7510 kwaliteitsnormen gecertificeerd en staan fysiek in Nederland.

## Conclusie

Bij Merlin nemen we beveiliging serieus omdat iedereen die onze dienst gebruikt, verwacht dat deze gegevens veilig en vertrouwelijk zijn. Beveiliging van deze gegevens is een kritische verantwoordelijkheid die we aan onze klanten hebben en we werken er hard aan om dat vertrouwen te behouden.