Informatiebeveiliging volgens NIS2

IT die voor zich spreekt.

Informatiebeveiliging volgens NIS2

I. Risico beheer

Risico analyse

Conform de ISO27001 houden we jaarlijks een risico analyse. Dan worden de risico's en kansen voor het behalen van het gewenste informatiebeveiligingsniveau geïnventariseerd. Op basis van de risico analyse worden gepaste maatregelen bepaald om de risico's voor de beschikbaarheid, integriteit en vertrouwelijkheid van informatie tot een aanvaardbaar niveau terug te brengen. Zo kan tevens de prioriteit worden bepaald van de inzet van middelen en de volgorde waarin de maatregelen worden geïmplementeerd. Mochten tussentijds urgente risico's zich voordoen worden deze ook volgens onderstaande methode in behandeling genomen.

Acties en risico's worden door Compliance vastgelegd in ons ERP systeem met een verantwoordelijke en specifieke workflow waardoor gewaarborgd wordt dat de acties en risico's behandeld worden volgens de vastgestelde procedures. De Security Officer in combinatie met de Compliance manager zijn verantwoordelijk voor alle gedefinieerde risico's en opvolging hiervan. Directie is eindverantwoordelijk.

Methode risicomanagement

We hanteren de zogenoemde RAM methode conform onderstaande tabel.

Risicoscore = Kans * impact

	Kans		
Impact	Hoog	Midden	Laag
Hoog	9	6	3
Midden	6	4	2
Laag	3	2	1

Risicoscore 6 & 9 : maatregelen worden direct ingepland en afgehandeld.
Risicoscore 3 & 4 : maatregelen worden op korte termijn ingepland en afgehandeld.
Risicoscore 2 : maatregelen worden met lage prioriteit ingepland en afgehandeld.
Risicoscore 1 : risico wordt geaccepteerd

NIS2 conform

Conform de zorgplicht van de NIS2 moeten organisaties risico analyses uitvoeren en passende maatregelen om hun systemen te beveiligen. Dit omvat technische en organisatorische maatregelen, zoals het beveiligen van informatiestromen, personeelstrainingen en incidentbeheer. Wat we hiervoor hebben ingeregeld is in dit document te lezen.

2. Beveiligingsmaatregelen

Om de vertrouwelijkheid en de geheimhouding van gegevens te waarborgen heeft VTM diverse technische en organisatorische maatregelen genomen. Dit conform de verschillende ISO-certificeringen die we in bezit hebben. Dit betreffen de ISO27001 (informatiebeveiliging), NEN7510 (informatiebeveiliging in de Zorgsector) en ISO9001 (Kwaliteit). Deze beveiligingsmaatregelen dienen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau te bieden gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen.

Domein	Technische/ organisatorische maatregel
Veilig personeelsbeleid	**Vertrouwelijkheidsverplichtingen** Medewerkers van VTM zijn onderworpen aan vertrouwelijkheidsverplichtingen en deze verplichtingen worden formeel opgenomen in arbeidsovereenkomsten. Bij indiensttreding van een nieuwe medewerker vragen we standaard een VOG (Verklaring Omtrent het Gedrag), algemeen screeningsprofiel, aan voor de volgende functies: - Leidinggevende functies - Technische functies - Financiële functies De VOG wordt vervolgens elke 3 jaar opnieuw aangevraagd. **Beveiligingstraining en AI geletterdheid training** In de informatiebeveiligingstraining stelt VTM haar medewerkers op de hoogte van de relevante beveiligingsprocedures voor het beschermen van klantendata en hun rol daarbij. Tevens dienen medewerkers AI geletterd te zijn. Aan de hand van trainingen worden deze skills aangeleerd. **Beëindiging.** Toegangsrechten worden bij beëindiging van de samenwerking tijdig ingetrokken, in overeenstemming met formele beveiligingsadministratieprocedures.
Beheer van bedrijfsmiddelen	**Inventaris van bedrijfsmiddelen** VTM houdt een inventaris bij van alle ICT-materiaal en media in gebruik. Toegang tot de inventarissen is beperkt tot hiervoor geautoriseerde medewerkers. **Behandeling van bedrijfsmiddelen**

	Data op draagbare apparaten is versleuteld. VTM beschikt over procedures voor het veilig vernietigen van media en afgedrukt materiaal die vertrouwelijke data bevatten.
Cryptografie	Versleuteling van vertrouwelijke data gebeurt volgens cryptografische standaarden. Data uitwisseling tussen systemen van VTM en derden gaat uitsluitend via beveiligde kanalen. Hierbij wordt TLS-encryptie (minimaal TLS versie I.2) gebruikt.
Fysieke beveiliging en beveiliging van de omgeving	**Fysieke toegang tot faciliteiten** - VTM beperkt de toegang tot faciliteiten waar vertrouwelijke informatie wordt verwerkt tot geïdentificeerde, geautoriseerde personen. - Fysieke toegang tot datacentra wordt uitsluitend toegekend volgens een formele autorisatieprocedure, en toegangsrechten worden periodiek beoordeeld **Bescherming tegen verstoringen** VTM gebruikt verschillende systemen die voldoen aan industrienormen om haar datacentra te beschermen tegen gegevensverlies als gevolg van stroomuitval en brand.
Toegangscontrole	**Toegangsbeleid** VTM hanteert een toegangscontrolebeleid op basis van 'need-to-know'- en 'least privileges'-beginselen. **Toegangsautorisatie** Elk individu die toegang heeft tot systemen die klantengegevens bevatten, heeft een aparte, unieke ID-gebruikersnaam. VTM beperkt de toegang tot klantengegevens tot die personen die dergelijke toegang nodig hebben om hun functie uit te voeren. **Authenticatie** VTM maakt gebruik van standaardpraktijken die voldoen aan industrienormen om gebruikers te identificeren en te authentiseren die zich proberen toegang te verschaffen tot de netwerk- of informatiesystemen van VTM, waaronder sterke authenticatie. Indien authenticatiemechanismen gebaseerd zijn op wachtwoorden, dan vereist VTM dat de wachtwoorden ten minste acht tekens lang en voldoende complex zijn. Gedeactiveerde of

	verlopen ID's / gebruikersnamen worden niet toegekend aan andere personen. Accounts worden vergrendeld bij herhaalde pogingen om met behulp van een ongeldig wachtwoord toegang te krijgen tot het informatiesysteem. **Netwerktoegang** VTM implementeert de nodige controlemaatregelen (bv. firewalls, security appliances, netwerk segmentatie) die een redelijke mate van zekerheid bieden dat toegang tot het netwerk op gepaste wijze wordt beschermd.
Beveiliging van de bedrijfsactiviteiten (operationele beveiliging)	**Gegevensherstel** VTM maakt op periodieke basis, maar in geen geval minder vaak dan één keer per week (tenzij tijdens die periode geen gegevens bijgewerkt werden), back-ups van klantengegevens voor hersteldoeleinden. VTM bewaart kopieën van klantengegevens en gegevensherstelprocedures op een andere plaats dan waar de primaire computerapparatuur die de klantengegevens verwerkt, zich bevindt. **Beveiligingsupdates** Beveiligingsupdates worden opgevolgd en geïnstalleerd volgens een gedocumenteerd patch managementproces.
Communicatie beveiliging	**Netwerksegregatie** VTM heeft een netwerksegmentatiebeleid en controles ingevoerd om te vermijden dat personen toegang krijgen tot communicatie en systemen waarvoor ze geen autorisatie hebben. **Transfer buiten eigen netwerk** VTM versleutelt klantengegevens die worden verzonden via publieke, niet-vertrouwde netwerken. **Informatieoverdracht.** Overdracht van klantengegevens aan derde partijen geschiedt enkel na het sluiten van een formele schriftelijke overeenkomst.
Verwerving, ontwikkeling en onderhoud van informatiesystemen	**Beveiligingsvereisten.** De vereisten voor de bescherming van gegevens en systemen worden geanalyseerd en gespecificeerd.

	Controle over wijzigingen. VTM heeft een formeel wijzigingsbeheerproces geïmplementeerd om ervoor te zorgen dat wijzigingen in operationele systemen en toepassingen plaatsvinden op een gecontroleerde wijze.
Verwerkersrelaties	**Keuze van verwerkers** VTM evalueert de beveiliging en privacy praktijken van een verwerker/partner met betrekking tot gegevensverwerking. **Contractuele verplichtingen** (sub) Verwerkers met toegang tot klantengegevens zijn onderworpen aan verplichtingen inzake gegevensbescherming en deze worden formeel opgenomen in verwerkerscontracten.
Beheer van informatiebeveiligingsincidenten	**Incident response** VTM houdt een register van beveiligingsinbreuken bij met een beschrijving van de inbreuk, het tijdstip, de gevolgen van de inbreuk, de naam van de melder en van degene aan wie de inbreuk werd gemeld. **Notificatie van incidenten** In geval van een informatiebeveiligingsincident dat impact heeft op de vertrouwelijkheid of integriteit van klantengegevens, zal VTM, zonder onredelijke vertraging, de klant hiervan informeren (zoals beschreven in de overeenkomst).
Bedrijfscontinuïteit	**Noodherstel** VTM handhaaft een noodherstelplan voor de datacentra waar zich informatiesystemen van VTM bevinden die klantengegevens verwerken. **Redundantie** De redundante opslag en procedures voor gegevensherstel van VTM zijn ontworpen met als doel klantengegevens te herstellen in hun laatst geback-upte staat voor het tijdstip waarop ze verloren gegaan zijn of vernietigd werden.

3. Incidentbeheer

VTM heeft een incidentresponsplan dat voldoet aan de eisen van de NIS2-richtlijn. Het plan omvat stappen voor detectie, response, herstel en communicatie tijdens incidenten. Tevens bevat het plan evaluaties na incidenten om processen te verbeteren.

Verder hebben we een SOC (Security Operation Center). Het SOC zorgt ervoor met behulp van verschillende systemen dat beveiligingsincidenten worden gedetecteerd, gemeld en opgelost.

4. Leveranciersbeheer

In ons inkoop- en leveranciersbeleid is vastgelegd hoe we leveranciers selecteren en wat onze eisen aan deze leveranciers zijn t.a.v. informatiebeveiliging. Wij verwachten daarin het volgende:

- Dat onze leveranciers een actief informatiebeveiligingsbeleid voeren conform de VTM voorwaarden. Deze komen daarmee overeen met de NIS2, ISO27001 en NEN7510.
- Dat onze leveranciers encryptie toepassen op de data die met VTM wordt uitgewisseld (transport) en wordt opgeslagen. Daarbij gaan we ervan uit dat bij het gebruik van encryptie de wet- en regelgeving in acht wordt genomen.

Leveranciersbeoordeling

Binnen VTM maken we onderscheid tussen kritieke en niet-kritieke leveranciers. Kritieke leveranciers zijn leveranciers die diensten leveren en niet-kritieke leveranciers betreffen onze hardware leveranciers. Hardware is een vervangingsmarkt en daardoor eenvoudiger bij verschillende leveranciers in te kopen. Voor diensten is dit lastiger.

De kritieke leveranciers worden elk jaar beoordeeld door degenen die verantwoordelijk zijn voor de betreffende dienst.

5. Continue verbetering

We evalueren onze beveiligingsmaatregelen doordat we jaarlijks audits laten uitvoeren door geaccrediteerde organisaties. Dan wordt de informatiebeveiliging getoetst en vindt evaluatie van ons informatiebeveiligingsbeleid plaats. Indien zaken niet toereikend zijn starten we een verbeteringstraject op.

Informatie over dreigingen ontvangen we van verschillende belangengroepen, denk aan National Cyber Security Center (NCSC) via RSS feeds, maar ook onze verschillende partners (Fortinet, Microsoft, etc.) berichten ons over eventuele dreigingen. Ook houdt ons eigen SOC de dreigingen in de gaten.

VTM services B.V.
Honderdland 190
2676 LT Maasdijk
0174 52 73 20
info@vtmgroep.nl
vtmgroep.nl