Veiligheidskader
GIDS Open Standaarden

Introductie

GIDS Open Standaarden beperkt zich uitdrukkelijk niet tot het medische domein maar verbindt juist oplossingen over de domeinen van gezondheid, welzijn en zorg heen. Daarbij variëren de organisaties die gebruik maken van GIDS Open Standaarden in sterk in grootte en expertise. Zo worden via GIDS Open Standaarden zowel grote behandelplatformen voor de GGZ als kleine sites die opgezet worden vanuit een wijk met elkaar gekoppeld. Tegelijkertijd vertrouwen de gebruikers en de organisaties die de standaard gebruiken onderling er wel op dat alle deelnemers een goed veiligheidsbeleid hebben. Bestaande veiligheidskaders als de ISO27000 en NEN7510 zijn niet flexibel genoeg om zo een divers veld te reguleren. Daarom hanteert GIDS Open Standaarden een eigen veiligheidskader. Dit veiligheidskader hanteert een aantal uitgangspunten:

- Het kader moet aanzetten tot *effectief veiligheidsbeleid* en zichtbaar maken wat er aan beveiliging gedaan wordt. Daarvoor kijkt het niet alleen naar de genomen maatregelen, maar ook naar de context van het gebruik en de organisatie.
- Het kader moet aanzetten tot *openheid*. Openheid vergroot het vertrouwen van de gebruikers en de organisaties onderling en maakt het mogelijk dat de organisaties elkaar steunen in het verbeteren van hun veiligheid.
- Het kader moet *laagdrempelig* zijn en ook kleine organisaties met weinig kennis op beveiligingsgebied steunen bij het opzetten van een goed veiligheidsbeleid.
- Het kader moet aansluiten bij de *wettelijke eisen* die gelden voor de activiteiten van de specifieke organisaties. Voorbeelden van zulke wetten zijn: de AVG, de WGBO, de Medical Devices Regulation, de wet Elektronische Gegevensuitwisseling in de Zorg etc.
- Het kader moet *geen dubbel werk* opleveren voor organisaties die al een eigen veiligheidsmanagement systeem (bijvoorbeeld uit de ISO 27000 of NEN7510 familie) hebben draaien.
- Het kader moet, met *peer review*, door de organisaties onderling te controleren zijn.
- Het kader moet *controleerbaar* zijn, als een organisatie niet aan een set minimumeisen voldoet, dan moet dat ook duidelijk worden.

Dit veiligheidskader is losjes gebaseerd op de “ISSA-UK 5173, Information Security for Small and Medium Sized Enterprises” norm. Het kader volgt, voor zover relevant, dezelfde categorieën en structuur als ISSA-UK 5173. Dit is verder ingevuld met items uit de OWASP top-10 en de NEN7510-1/2.

Dit kader wijkt op een punt af van de eisen die door de ISO27001 of NEN7510-1 normen gesteld worden. Het risico management, punt 3 in deze norm, wordt expliciet opgesplitst naar twee aparte stappen: het op hoog niveau in kaart brengen welke bedreigingen voor de doelgroep relevant zijn (punt 3a) en op basis daarvan invullen welke incidenten daadwerkelijk kunnen optreden (punt 3b).

Er is voor deze splitsing gekozen om veilig te stellen dat het risicomanagement ook daadwerkelijk aansluit bij de zeer diverse doelgroepen die van GIDS Open Standaarden gebruik maken. Een organisatie die al ISO27001 of NEN7510-1 gecertificeerd is, zal moeten nagaan of dit voldoende in het risicomanagement tot zijn recht komt.

Review methode

Optie 1: peer review

Een organisatie die deelneemt aan GIDS Open Standaarden nodigt minimaal een keer per jaar twee of meer collega organisaties uit het GIDS netwerk uit voor een veiligheidsreview. De organisatie die uitnodigt kan van te voren al documenten opsturen waaruit blijkt dat ze aan de onderdelen van het kader voldoen. De organisatie kan ook ter plekke met een mondelinge toelichting laten zien hoe het veiligheidsbeleid in de praktijk uitwerkt. Daarbij is het wel het uitgangspunt dat de review zodanig voorbereid moet zijn dat de review binnen twee uur gedaan kan worden.

Als de collega organisaties twijfel hebben over de review, kunnen ze ruggenspraak vragen bij de Stichting Beter Met Elkaar.

Optie 2: externe audit

Een organisatie die deelneemt aan GIDS Open Standaarden vraagt minimaal een keer per jaar een externe auditor om na te gaan of hun organisatie voldoet aan het GIDS Open Standaarden veiligheidskader. De externe auditor moet of door de Raad voor Accreditatie geaccrediteerd om NEN7510 of ISO27000 audits te doen, of de externe auditor is door Stichting Beter Met Elkaar aangewezen als auditor.

Rapportage

De bezoekende organisaties, of de auditor, vullen het overzicht uit bijlage 1 in. Bij de velden ‘Toelichting’, ‘Nog open vragen / verbeterpunten’ en ‘Opmerkingen’ moet een korte (hoogstens enkele zinnen) samenvatting in begrijpelijke taal gegeven worden. Opsommingen van, of details over, beveiligingsmaatregelen horen hier niet thuis.

Bij de rapportage moet er uitgegaan worden van wat er daadwerkelijk geconstateerd is. De gebruikers gaan het komende jaar er op vertrouwen dat de beveiliging daadwerkelijk op orde is. Het is beter dat een organisatie tussentijds een nieuwe review moet doen dan dat het vertrouwen van de gebruikers geschonden wordt.

De uitnodigende organisatie publiceert vervolgens de bevindingen en voegt daar, indien gewenst een reactie aan toe. Die reactie kan bijvoorbeeld maatregelen vermelden die genomen zijn of worden naar aanleiding van de bevindingen. Bij een tussentijdse wijziging in het beveiligingsbeleid kan de organisatie vervroegd een nieuwe review vragen.

Kader

De *cursief* gedrukte tekst zijn voorbeelden van manieren om iets vast te stellen. Deze voorbeelden zijn niet leidend.

Deel 1: Verplichte maatregelen

Deze maatregelen moeten altijd aanwezig zijn om te voldoen aan het GIDS beveiligingskader.

1. Veiligheid is een prioriteit van de eigenaar/eigenaren of de directie
Het veiligheidsbeleid kan alleen werken als actief door de leiding uitgedragen en ondersteund wordt. Tijdens de review moet die betrokkenheid van de leiding duidelijk worden.

Voorbeelden van manieren waarop dat aangetoond kan worden:

- *De eigenaar of eigenaren bemoeien zich actief met de review en laten blijken goed op de hoogte te zijn van de details.*
- *Er zijn aantoonbare voorbeelden van bedrijfsmatige keuzes op directieniveau waarbij de beveiliging prioriteit kreeg.*
- *Medewerkers laten blijken zich door de directie gesteund te voelen bij het uitvoeren van de beveiligingsmaatregelen.*

2. Directie en medewerkers weten aan welke verplichtingen ze moeten voldoen
Het gaat hier om algemene wetten, zoals de AVG, sector specifieke wetten, zoals de WGBO en om contractuele verplichtingen, zoals de overeenkomsten die geïmplementeerd moeten zijn bij het deelnemen aan MedMij in een bepaalde rol. Het moet aantoonbaar zijn dat hier voldoende overzicht op is in de organisatie.

Voorbeelden van manieren waarop dat aangetoond kan worden:

- *Er is een overzicht beschikbaar van de verplichtingen waaraan voldaan moet worden.*
- *Directie en medewerkers kunnen direct de voor het werk relevante eisen noemen.*

3. Er is begrip van de beveiligingsrisico's die voor de doelgroep relevant zijn
Welke bedreigingen relevant zijn, hangt sterk van de context en de doelgroep af. Daarom is het van belang om eerst algemeen en op hoog niveau vast te stellen wat voor een soort manieren gebruikers in de problemen kunnen komen, bijvoorbeeld: "ik ga door mijn buren met de nek aangekeken worden als zij weten welke problemen ik heb". Pas als dat duidelijk is, kan er ingezoomd worden op incidenten die dat kunnen veroorzaken.

Begrip van de risico's			
	Niveau	**Eis**	***Voorbeelden van manieren waarop dat aangetoond kan worden***
3a begrip van bedreigingen	Basis	Er is overzicht van de bedreigingen die voor de doelgroep relevant zijn.	*Er kan mondeling weergegeven worden welke bedreigingen relevant zijn.* *Er kan een lijst met bedreigingen overlegd worden.*
	Middel	Niveau basis + het overzicht van de bedreigingen is in samenwerking met de doelgroep vastgesteld.	*Er kan mondeling weergegeven worden welke nieuwe inzichten de gesprekken met gebruikers opgeleverd hebben.* *Er is een gespreksverslag van een overleg met gebruikers hierover.*
	Geavanceerd	Niveau middel + het overzicht van de bedreigingen is onderbouwd.	*Het beveiligingsnieuws, bijvoorbeeld de nieuwsberichten van SANS of Security.nl, wordt gevolgd en er kan uitgelegd worden welke nieuwe relevante bedreigingen er uit een nieuwsbericht volgen.* *De eigen analyse is vergeleken met de analyse van andere partijen en de verschillen kunnen verklaard worden.*
3b overzicht op mogelijke incidenten	Basis	Er zijn bij elke geformuleerde bedreiging mogelijke incidenten benoemd. Deze lijst bevat minimaal de OWASP top-10 (https://owasp.org/www-project-top-ten/). Als een van de incidenten uit de OWASP top-10 niet relevant is, kan er uitgelegd worden waarom niet.	*Controle van de papieren versie van de lijst.* *Een van de ontwikkelaars kent de OWASP top 10 uit zijn hoofd en kan aangeven of er bedreigingen zijn die niet door de OWASP top 10 gedekt worden.*
	Middel	Niveau basis + er is onderbouwd dat bij elke bedreiging alle relevante incidenten genoemd zijn.	*Documentatie van de risico analyse.* *De hoofdontwikkelaar kan mondeling uitleggen welke routes er mogelijk zijn bij elke*

			bedreigen en welke incidenten die routes kunnen bestaan.
	Geavanceerd	Niveau middel + aan elk incident is een gewicht toegekend op basis van de waarschijnlijkheid van optreden en mogelijke schade.	*Documentatie van de risico analyse.* *Inhoud van een tool voor risicomanagement.*

4. Basisbeveiligingsmaatregelen

Tegen alle bij 3a genoemde incidenten zijn maatregelen genomen. Voor de incidenten die in de OWASP top-10 staan geldt voor de door OWASP genoemde maatregelen dat als die maatregel niet genomen is, er uitgelegd kan worden waarom de maatregel niet relevant is. Als een deel van de software of een component ervan door een derde partij geleverd wordt, kan getoond worden dat er maatregelen zijn genomen tegen de bij 3a genoemde incidenten. Daarnaast is er een systeem en procedure voor het maken van backups en het terugzetten van backups. Het terugzetten van een backup is getest.

Voorbeelden van manieren waarop dat aangetoond kan worden:

- *De maatregelen kunnen, met mondelinge toelichting, ter plekke getoond worden.*
- *Er is een security management systeem, bijvoorbeeld NEN-7510 of ISO-27001, aanwezig en de OWASP top-10 en de bijbehorende maatregelen zijn op basis van 'comply or explain' in het security management systeem opgenomen.*
- *Er kan, via de bugtracker of via de Common Vulnerability Database getoond worden dat gebruikte componenten van derde partijen geen kritisch veiligheidsproblemen hebben.*
- *Er kan getoond worden dat er een actief veiligheidsbeleid is voor een externe component.*

Deel 2: Optionele beveiligingsmaatregelen

Deze maatregelen zijn niet verplicht om te voldoen aan het veiligheidskader van GIDS Open Standaarden, maar ze kunnen gebruikt worden om te laten zien welke aanvullende beveiligingsmaatregelen genomen zijn. Zeker bij grotere organisaties of als er met zeer risicovolle gegevens gewerkt worden, zullen deze maatregelen in beeld komen. Ook eisen sommige andere partijen of wetten deze maatregelen. Ze zijn niet verplicht omdat ze niet voor alle deelnemers aan GIDS Open Standaarden relevant zijn of omdat ze voor kleine organisaties een onnodige last vormen.

5. Er zijn voor de medewerkers concrete beveiligingsregels
Voorbeelden: regels voor wachtwoorden, het gebruik van USB-sticks, het gebruik van open WiFi etc.

Voorbeelden van manieren waarop dat aangetoond kan worden:

- *De medewerkers hebben een lijstje met do's en don'ts en kunnen dat makkelijk opzeggen of terugvinden.*
- *In contracten zoals verwerkersovereenkomsten staan regels waar de medewerkers zich aan houden.*

6. Het is duidelijk wie waar verantwoordelijk voor is
Er zijn veel veiligheidsgerelateerde taken, zoals het maken van backups, het toewijzen van toegangsrechten, het uitvoeren van updates, het actueel houden van de lijst van mogelijke incidenten, etc. Voor elk van die taken is duidelijk wie er verantwoordelijk voor is en wie er achterwacht is bij afwezigheid. Voor taken die een onafhankelijke positie vragen, zoals Functionaris Gegevensbescherming of overzicht over het beveiligingsgebied, zijn er maatregelen genomen om die onafhankelijkheid te waarborgen.

Voorbeelden van manieren waarop dat aangetoond kan worden:

- *Er kan direct een naam en een naam van een achterwacht genoemd worden bij een taak.*
- *De Functionaris gegevensbescherming en degene die overzicht houdt over het beveiligingsbeleid hebben geen verantwoordelijkheid in het programmeren, onderhouden en beheren van het systeem.*
- *Er is een verdeling van rollen aanwezig zoals management systemen als de NEN-7510 en de ISO-27001 die vragen.*

7. Er zijn noodplannen
Er zijn plannen, procedures en voorbereidingen voor als er iets mis gaat.

Voorbeelden van manieren waarop dat aangetoond kan worden:

- *Medewerkers kunnen benoemen wat ze moeten doen als er iets mis gaat.*
- *Er is een handboek voor noodsituaties.*
- *Er zijn afspraken voor noodgevallen en noodvoorzieningen in plaats, zoals kanalen voor nood-communicatie, fall-back systemen, mogelijkheden om in noodgevallen zicht op de aard en omvang van het incident te krijgen en prioriteiten lijsten voor mogelijke acties.*

8. Er zijn procedures rond veiligheid
Voor taken als het aannemen en inwerken van nieuw personeel, het in gebruik nemen en afdanken van apparatuur, het in productie nemen van wijzigingen aan de software en het afhandelen van veiligheidsmeldingen zijn procedures opgesteld.

Voorbeelden van manieren waarop dat aangetoond kan worden:
- *Er kan getoond worden dat er workflows gevolgd worden waarin de procedures verankerd zijn, bijvoorbeeld bij een aanpassing aan de software een workflow in de version control.*
- *De procedures zijn beschreven.*

9. Er is een aanvullend veiligheidsmanagement systeem actief
Bijvoorbeeld NEN-7510 of ISO-27001/2.

Voorbeelden van manieren waarop dat aangetoond kan worden:
- *Documentatie van veiligheidsmanagement systeem.*
- *Audit verslag van veiligheidsmanagement systeem.*

10. Er zijn gespecialiseerde maatregelen genomen
Afhankelijk van de situatie kan het nuttig zijn om gespecialiseerde maatregelen te nemen, zoals procedures voor de bescherming van slachtoffers van huiselijk geweld tegen phishing door de daders of privacy-by-design patronen of geavanceerde encryptiesystemen.

Voorbeelden van manieren waarop dat aangetoond kan worden:
- *Mondelinge toelichting op de maatregelen.*
- *Schriftelijke beschrijving van de maatregelen.*

11. De medewerkers worden geschoold op het gebied van veiligheid
Denk aan trainingen om veilig gedrag te versterken, les in specifieke vaardigheden als veilig programmeren of aan het leren van de nieuwste inzichten op beveiligingsgebied.

Voorbeelden van manieren waarop dat aangetoond kan worden:
- *Medewerkers kunnen uitleggen wat ze doen om hun kennis over beveiliging up-to-date te houden.*
- *Er is een opleidingsplan voor medewerkers.*
- *Er zijn certificaten voor gevolgde trainingen aanwezig.*

Bijlage 1: Resultaten Beoordeling Veiligheid

GIDS Open Standaarden

Organisatie / product:
Reviewers (namen + organisaties):
Datum review:

Verplichte onderdelen				
Item	**Omschrijving**	**Bevinding**	**Toelichting**	**Nog open vragen/verbeterpunten**
1	Beveiliging heeft prioriteit			
2	De organisatie weet waar het aan moet voldoen			
3a	De organisatie weet welke gevaren de gebruikers lopen			
3b	De organisatie weet wat er mis kan gaan			
4	De maatregelen voor een basisniveau van beveiliging zijn genomen			
Optionele onderdelen				
Item	**Omschrijving**	**Bevinding**	**Opmerkingen**	
5	Er zijn duidelijke regels voor het personeel			
6	Het is intern duidelijk wie waar verantwoordelijk voor is			
7	Er zijn noodplannen			
8	Er zijn procedures voor het garanderen van de veiligheid			
9	De organisatie voldoet aan een veiligheidsnorm als NEN-7510 of ISO-27001			
10	Er zijn gespecialiseerde veiligheidstechnieken ingezet			
11	Het personeel is getraind op veiligheid			