SECURITY AGREEMENT

ROC Midden Nederland

Dienst Onderwijs Services en ICT & Informatie Management
Auteur: Edo Meinema
Contactpersoon: Pepijn de Vette
Versie: 1.2
Datum versienummer: 27 augustus 2024

DOCUMENTINFORMATIE

Dit document maakt onderdeel uit van een set met formeel vastgestelde documenten op strategisch, tactisch en operationeel niveau gerelateerd aan informatiebeveiliging. Dit document heeft betrekking op de laag Thema-Beleid in de beleidspiramide[1].

Versiebeheer

Versie	Datum	Auteur	Verwerking
1.0	16 november 2022	Definitief	Eveline van Oostrom
1.1	23 mei 2023	Definitief	Eveline van Oostrom
1.2	27 augustus 2024	Definitief	Eveline van Oostrom

Distributielijst

Versie	Datum	Ontvanger	Doel

Vaststelling

Versie	Datum	Vastgesteld door	Vastgesteld op
1.0	16 november 2022	Definitief	Eveline van Oostrom
1.1	23 mei 2023	Definitief	Eveline van Oostrom
1.2	27 augustus 2024	Definitief	Eveline van Oostrom

Samenhang met andere documenten

Naam	Bovenliggend	Gelijk niveau	Onderliggend
InformatieBeveiligingsBeleid ROC MN	X		

Verwijzingen naar SURFaudit Toetsingskader Informatiebeveiliging en Privacy

Kader	Verwijzing (tags)
SURFaudit Toetsingskader Informatiebeveiliging	GO.01; GO.02;
SURFaudit Toetsingskader Privacy	

[1] Voor meer informatie zie Bijlage B: Beleids- en documentenstructuur.

Inhoudsopgave

INLEIDING

Voor ROC Midden Nederland als onderwijsinstelling is een integere bedrijfsvoering noodzakelijk. Daarbij wordt ook gestuurd op een integere bedrijfsvoering bij Leverancier van ROC Midden Nederland.

Voorliggend Security Agreement is gerelateerd aan het informatiebeveiligingsbeleid (IBB) van ROC Midden Nederland. Het IBB beschrijft 5 strategisch leidende beleidsprincipes waaraan middels deze Security Agreement invulling wordt gegeven voor business partners en leveranciers van ROC Midden Nederland, te weten:

1. **Risico-gebaseerd**: We baseren de maatregelen op de mogelijke veiligheidsrisico's van onze informatie, processen en IT-faciliteiten.

2. **Iedereen:** Iedereen is en voelt zich verantwoordelijk voor een juist en veilig gebruik van middelen en bevoegdheden.

3. **Altijd:** Informatiebeveiliging zit in het DNA van al onze werkzaamheden.

4. **Security by Design**: Informatiebeveiliging is vanaf de start een integraal onderdeel van ieder project of iedere verandering m.b.t. informatie, processen en IT-faciliteiten.

5. **Security by Default**: Gebruikers hebben alleen toegang tot informatie en IT-faciliteiten die zij nodig hebben voor hun werkzaamheden. Het openstellen van informatie is een bewuste keuze.

In deze Security Agreement zijn de voorwaarden met betrekking tot informatiebeveiliging opgenomen waaraan Leverancier dient te voldoen bij het verlenen van de Prestatie. Het principe "comply or explain" is van toepassing op deze voorwaarden. Afhankelijk van de te leveren Prestatie kunnen bepaalde onderwerpen wel of niet van toepassing zijn voor Leverancier. Dit ter beoordeling van ROC Midden Nederland.

Security Office ROC Midden Nederland

1. BEVEILIGINGSORGANISATIE

BO.1 Leverancier dient een beveiligingsbeleid op schrift op te stellen en te onderhouden, dat richting geeft aan alle beveiligingsinspanningen van haar organisatie. Dit beleid dient minimaal te voldoen aan de eisen hieraan gesteld vanuit de NEN-ISO/IEC 27001:2023 norm en voor zover aanvullend de in de markt gehanteerde best practices te bevatten. De hoogste leiding van Leverancier moet het beveiligingsbeleid hebben geaccordeerd.

BO.2 Leverancier houdt zich aan dit beveiligingsbeleid en verstrekt dit op verzoek aan ROC Midden Nederland.

BO.3 De verantwoordelijkheid voor het Beveiligingsbeleid en de controle op de naleving hiervan wordt belegd bij een specifieke functionaris, zijnde de Security Officer van Leverancier.

BO.4 Leverancier hanteert en executeert een sanctiebeleid voor het overtreden van de door Leverancier gestelde beveiligingsrichtlijnen.

2. FYSIEKE- EN OMGEVINGSBEVEILIGING

FB.1 Computerzalen, netwerkruimtes en overige kritische ruimtes (daar waar van toepassing) van Leverancier, waarin apparatuur staat opgesteld voor de verwerking van ROC Midden Nederland productiegegevens, dienen beveiligd te zijn met een (geautomatiseerd) toegangscontrolesysteem met centrale administratie.

FB.2 De procedures voor het verlenen en intrekken van toegangsrechten tot de beveiligde ruimtes en de procedures voor de periodieke controle zijn schriftelijk vastgelegd en geaccordeerd door de Security Officer van Leverancier. De uitvoering van de procedures wordt zodanig geregistreerd dat controle op juiste naleving mogelijk is.

FB.3 Personeel dat uit dienst treedt, dient direct de aan ROC Midden Nederland gerelateerde autorisaties te worden ontnomen.

FB.4 Schoonmaakpersoneel en onderhoudspersoneel dienen uitsluitend onder toezicht toegang te verkrijgen tot ruimten met een verhoogd beveiligingsniveau. Toegang van ROC Midden Nederland medewerkers tot kritische ruimten van Leverancier wordt verleend op basis van functionele noodzaak.

FB.5 Door Leverancier dienen maatregelen te zijn getroffen gericht op een adequate preventie, signalering en bestrijding van onder meer brand, rook, wateroverlast, spanningsuitval of –schommelingen, trillingen, stof, statische elektriciteit en temperatuurschommelingen. Dit om de continuïteitseisen van ROC Midden Nederland te kunnen waarborgen.

FB.6 Minimaal jaarlijks dient de effectiviteit van de maatregelen en de werking van (o.a. brand en blus, klimaatregeling, UPS) installaties te worden getest.

FB.7 Media, waaronder ook papieren output, met vertrouwelijke informatie van ROC Midden Nederland mogen niet onbewaakt worden achtergelaten tenzij opgeborgen in een afgesloten ruimte. De wijze van verwijdering en vernietiging van deze media dient te zijn uitgewerkt in een met ROC Midden Nederland afgestemde verwijderingsprocedure.

FB.8 Bij fysiek vervoer van mediadragers voor back-up dienen maatregelen getroffen te worden onder meer tegen diefstal en omgevingsfactoren zoals fluctuatie in temperatuur, vochtigheid etc.

FB.9 Back-ups van ROC Midden Nederland gegevens worden fysiek op een andere locatie bewaard.

FB.10 Uitkomsten uit controles op de fysieke beveiligingsmaatregelen worden op aanvraag gedeeld met ROC Midden Nederland indien deze betrekking hebben op de door ROC Midden Nederland afgenomen Prestatie. In geval van negatieve afwijkingen maakt Leverancier daarbij afspraken met ROC Midden Nederland over de doorlooptijd voor verbetering en houdt ROC Midden Nederland periodiek op de hoogte van de voortgang.

3. LOGISCHE TOEGANGSBEVEILIGING

LB.1 Het aantal beheerders dat toegangsrechten heeft tot de gegevens en omgeving van ROC Midden Nederland dient tot een minimum beperkt te zijn. ROC Midden Nederland bepaalt in overleg, in voorkomende gevallen wie autorisatie krijgt tot de applicaties en data. Hiertoe dient Leverancier een autorisatiematrix op te stellen. Deze matrix dient door Leverancier intern te worden getoetst en goedgekeurd. De autorisatiematrix dient op verzoek aan ROC Midden Nederland beschikbaar te worden gesteld ter beoordeling. Onderdeel van deze autorisatiematrix is een lijst van rollen, namen en rechten van onder andere beheerders. Wijzigingen in de geaccordeerde autorisatiematrix dienen door Leverancier te worden vastgelegd ten behoeve van eventuele controles. Leverancier draagt zorg voor de effectuering van de geaccordeerde autorisatiematrix.

LB.2 Leverancier medewerkers mogen alleen toegang krijgen tot systemen middels een persoonlijk toegewezen user identificatie (user-id). Indien dit technisch niet mogelijk is, worden er procedurele maatregelen genomen. De kritische werkzaamheden van een beheerder, inclusief het user-id van de beheerder, worden gelogd, en gecontroleerd door Leverancier. Op verzoek van ROC Midden Nederland zal Leverancier (gedeelten van) de logs, die betrekking hebben op de aan ROC Midden Nederland geleverde Prestatie, ter inzage verstrekken.

LB.3 Er dienen maatregelen getroffen te worden, die ervoor zorgen dat de logging van activiteiten niet muteerbaar is ter waarborging van de authenticiteit/betrouwbaarheid van de logging. De toegang tot deze logging dient beperkt te zijn tot de hoogstnoodzakelijke beheeractiviteiten, c.q. minimaal aantal beheerders.

LB.4 Leverancier medewerkers in de rol van ontwikkelaar, tester of ontwerper mogen alleen toegang hebben tot de ontwikkel en test omgeving, binnen één OTAP (Ontwikkel, Test, Acceptatie, Productie) straat. Toegang tot acceptatie en productie omgevingen vindt alleen plaats na schriftelijke goedkeuring door de Security Officer van Leverancier. Indien het een omgeving betreft die exclusief voor of door ROC Midden Nederland wordt gebruikt, dient ook goedkeuring te worden verleend door ROC Midden Nederland.

LB.5 Source code en ontwikkeldocumentatie opgeslagen en bewerkt bij Leverancier worden door Leverancier beveiligd tegen ongeautoriseerde toegang. Hiervoor worden de gewenste en werkelijke autorisaties ingericht en gemonitord. Indicatie van onbevoegd toegang wordt gemeld aan ROC Midden Nederland indien dit een mogelijk risico voor ROC Midden Nederland met zich meebrengt.

LB.6 Beheerders mogen niet meer autorisaties bezitten dan strikt noodzakelijk is voor de uitoefening van de functie. Voor tenminste de volgende activiteiten dient zorgvuldig en aantoonbaar afgewogen te worden of de betreffende autorisaties noodzakelijk zijn:

a) Mutatie systeeminstellingen;
b) Mutatie autorisatie(s)/autorisatietabellen;

c) (Beheer)Activiteiten die hoge rechten vereisen;
d) Aanpassen (Group) policies;
e) Aanpassen source code en ontwikkel- programmatuurdocumentatie;
f) Aanpassen (job) schedules;
g) Lezen van bedrijfsinterne/vertrouwelijke gegevens;
h) Zaaltoegang datacenters met apparatuur en gegevens gebruikt ten behoeve van dienstverlening aan ROC Midden Nederland.

LB.7 Het mag niet mogelijk zijn gegevens en/of programmatuur van ROC Midden Nederland over te zetten naar een andere klant-omgeving en vice versa. De ROC Midden Nederland omgeving dient volledig geïsoleerd te zijn (logisch) van omgevingen van andere klanten op zowel netwerk-, besturingssysteem- en dataniveau. Zowel binnen de besturingssystemen als binnen applicaties dienen wachtwoordmanagement-systemen te voldoen aan de eisen gesteld in de betreffende Security Baseline zoals opgesteld door Leverancier. Voor wat betreft informatie in mailsystemen, laptops en removable media dient dit zo veel als mogelijk gescheiden te zijn. De Leverancier dient ervoor te zorgen dat gegevens van ROC Midden Nederland niet onbeheerd achtergelaten worden.

LB.8 Zowel binnen de besturingssystemen als binnen applicaties dienen wachtwoordmanagement-systemen te voldoen aan de eisen gesteld in de betreffende Security Baseline zoals opgesteld door Leverancier.

4. BEVEILIGING VAN GEGEVENS EN PROGRAMMATUUR

BG.1 Leverancier is op de hoogte van het classificatieniveau van gegevens, programmatuur en documentatie zoals deze door ROC Midden Nederland vastgesteld en verstrekt is. Leverancier treft beveiligingsmaatregelen in lijn met deze BIV-classificatie om de beschikbaarheid, integriteit en vertrouwelijkheid te waarborgen en treedt hierover in overleg met ROC Midden Nederland ter vaststelling of deze maatregelen voldoende zijn.

BG.2 Gegevens en programmatuur van ROC Midden Nederland moeten fysiek (dan wel logisch) gescheiden zijn van overige klanten van Leverancier. Indien bij Leverancier centrale opslag (storage) oplossingen (of andere vergelijkbare functionaliteit) wordt gebruikt, moet door een onafhankelijke derde partij aantoonbaar worden gemaakt dat de isolatie van gegevens van andere klanten is gewaarborgd.

BG.3 Gegevens van ROC Midden Nederland mogen niet in directe verbinding staan met een publiek of niet-beveiligd netwerk (waaronder het Internet), behalve wanneer de Prestatie dit specifiek vereist. Tenzij expliciet anders overeengekomen worden certificaten, gekoppeld aan ROC Midden Nederland assets zoals (sub)domeinnamen, door ROC Midden Nederland beheerd en aangeschaft.

BG.4 Programmatuur van andere klanten mag geen bewerkingen (lezen, toevoegen, wijzigen en verwijderen) kunnen uitvoeren op de gegevens van ROC Midden Nederland. De gegevens en programmatuur van ROC Midden Nederland dienen waar mogelijk in gescheiden omgevingen te draaien met een eigen ongedeeld beveiligingssysteem dat voldoet aan de beveiligings-eisen zoals gesteld in artikel BO.1.

BG.5 Er dient een scheiding te worden gerealiseerd en gehandhaafd tussen de verschillende omgevingen (OTAP) b.v. Productie, Test en Acceptatie omgevingen. Bestanden mogen alleen worden benaderd door programmatuur die onderdeel uitmaakt van de door de Leverancier geleverde Prestatie.

Overdracht van programmatuur naar de verschillende omgevingen moeten geschieden conform vastgestelde procedures en richtlijnen.

BG.6 Systeemprogrammatuur (zijnde alle non-applicatie programmatuur) dient altijd te voldoen aan het juiste beveiligingsniveau (patch level) aanbevolen door de softwareleverancier. Leverancier dient beschreven procedures operationeel te hebben voor het proactief managen van meldingen inzake security-kwetsbaarheden, malafide programmatuur (zoals rootkits, worms of virussen) of andere zaken van belang voor de continuïteit, integriteit en beschikbaarheid van de ROC Midden Nederland gegevens en processen. Indien ROC Midden Nederland Leverancier niet in staat stelt hieraan te voldoen als gevolg van beperkingen van de applicatieprogrammatuur, dient Leverancier dit schriftelijk te melden aan ROC Midden Nederland en zullen partijen in overleg treden omtrent de gevolgen daarvan.

BG.7 Programmatuur, Scripts of procedures ontwikkeld door de Leverancier in opdracht van ROC Midden Nederland dient minimaal te voldoen aan de ROC Midden Nederland ontwikkeleisen voor secure coding zoals beschreven bij Beveiligingsnormen voor Systeemontwikkeling.

5. CONTINUÏTEITSPLANNING

Het betreft hier de continuïteitsplanning die zich richt op het kunnen leveren van de Prestatie door de leverancier. De continuïteitseisen van de interne organisatie van Leverancier zijn geen onderdeel van de in dit hoofdstuk beschreven continuïteitsplanning.

In aanvulling op de definities zoals opgenomen in de Overeenkomst zullen in deze agreement nog de volgende gedefinieerd begrippen worden gebruikt:

> *Calamiteit*: Een Calamiteit is een gebeurtenis die het gevolg heeft dat de IT-infrastructuur op een zodanige wijze wordt getroffen dat aanzienlijke maatregelen moeten worden genomen om de IT-dienst weer te herstellen (beschikbaar te hebben).
>
> *Uitwijk*: De verzameling procedures en maatregelen, die ervoor zorgt dat de continuïteit van de informatievoorziening gewaarborgd kan worden, dan wel dat de informatievoorziening binnen een bepaalde periode kan worden hervat.
>
> *Disaster Recovery Plan*: Plan waarin beschreven staat hoe de IT-dienstverlening in geval van een Calamiteit met vervangende IT-middelen wordt voortgezet.

DR.1 ROC Midden Nederland eist gedocumenteerde back-up en restore procedures en een volledig Disaster Recovery Plan (DRP). Daartoe zijn gedocumenteerde back-up en restore procedures en instructies en een DRP vereist voor de gecontracteerd Prestatie.

DR.2 Het DRP zal de voorwaarden, taken en verantwoordelijkheden bevatten om in geval van een Calamiteit binnen het overeengekomen tijdsbestek hiervan te herstellen. Het tijdsbestek voor herstel wordt opgenomen in het DRP. Het DRP zal daar waar mogelijk workarounds bevatten om de onderliggende bedrijfsprocessen draaiende te houden totdat de systemen volledig hersteld zijn.

DR.3 Als onderdeel van het DRP zal de Leverancier een jaarlijkse test uitvoeren, om vast te stellen of het DRP effectief is.

DR.4 Back-up en recovery van transactiegegevens, logbestanden, autorisatietabellen, source code, ontwikkel- en programmatuurdocumentatie dienen te zijn gewaarborgd. De back-up gegevens dienen te worden opgeslagen op een externe locatie (off-site storage). Periodiek , doch minimaal jaarlijks, dient te worden vastgesteld of de back-up en restore-procedure werkt.

DR.5 Er dient tussen de primaire verwerkingslocatie en de externe locatie (off-site storage locatie) op basis van risico-inschatting o.b.v. natuurlijke, economische, politieke en geografische risico's, rekening gehouden te worden met voldoende afstand tussen elkaar.

6. SECURITY BASELINES

SB.1 Leverancier conformeert zich, in uitvoering van haar dienstverlening en oplevering van deliverables, aan de security parameters, instellingen en uitgangspunten voor alle systeemcomponenten, databasemanagementsystemen, operating systemen, netwerkcomponenten en middleware. Dit dient te worden vastgelegd in Security Baselines. Deze Baselines dienen door ROC Midden Nederland opvraagbaar en controleerbaar te zijn.

SB.2 Indien Leverancier af wil wijken van deze Security Baselines, dienen deze afwijkingen te worden geregistreerd waarbij de beveiliging en continuïteit van de Prestatie is geborgd. Afwijkingen dienen te worden goedgekeurd door de Security Officer van Leverancier. Acties worden gedefinieerd met uiterste oplosdatum om de afwijking te corrigeren. Indien een afwijking niet opgelost kan worden, worden aanvullende maatregelen bepaald, vastgelegd en geïmplementeerd. Leverancier richt deze aanvullende maatregelen in en rapportage over de effectiviteit van deze maatregelen is op aanvraag voor ROC Midden Nederland beschikbaar.

SB.3 Daar waar geen beschreven en goedgekeurde Security Baselines voorhanden zijn conformeert Leverancier zich aan algemeen geldende security normen (ten minste ISO 27001/27002) waarbij de beveiliging en continuïteit van de Prestatie is geborgd op het door ROC Midden Nederland vereiste niveau. Deze normen-set dient te zijn geaccordeerd door de Security Officer van Leverancier.

SB.4 Beveiligingsparameters of besturingssysteem parameters die de beveiliging kunnen beïnvloeden moeten worden ingesteld volgens de aanwijzingen van de Security Officer van Leverancier. De betreffende Security Baseline dient hiervoor als leidraad. Wijzigingen in de basisinstellingen dienen pas na goedkeuring van de Security Officer van Leverancier aangebracht te worden, waarbij de beveiliging en continuïteit van de Prestatie is geborgd. Indien er wijzigingen zijn, wordt door Leverancier een overzicht gemaakt van de thans geldende instellingen en de eventuele aangebrachte wijzigingen (Changelog).

SB.5 Kritische aanpassingen of voorzieningen die de beveiliging van het besturingssysteem kunnen beïnvloeden mogen alleen na accorderen van de Security Officer van Leverancier geïmplementeerd worden, waarbij de beveiliging en continuïteit van de Prestatie is geborgd. Leverancier rapporteert periodiek over de status van deze kritische aanpassingen of voorzieningen van het besturingssysteem en de mutaties daarop. Deze rapportage is op aanvraag voor ROC Midden Nederland beschikbaar.

SB.6 Indien er gebruik gemaakt wordt van publieke netwerken (zijnde infrastructuur die niet exclusief voor ROC Midden Nederland toegankelijk is, zoals gedeelde infrastructuur van Leverancier en/of het internet), dient Leverancier te zorgen voor afdoende encryptie van de datacommunicatie om verlies of enige vorm van onrechtmatige verwerking te voorkomen. Deze encryptie garandeert, rekening houdend met de stand van de techniek, een passend beveiligingsniveau gelet op de risico's en de aard van de gegevens. Daarnaast dient Leverancier te zorgen voor een logische scheiding van ROC Midden Nederland gegevens en gegevens van andere klanten van Leverancier.

SB.7 Alle Externe Koppelingen nodig voor het leveren van de Prestatie aan ROC Midden Nederland moeten minimaal voldoen aan de eisen gesteld aan externe koppelingen, zoals verderop beschreven bij Externe Koppelingen.

SB.8 Overige niet expliciet genoemde componenten of platformen dienen minimaal te voldoen aan de eisen zoals gesteld in het Beveiligingsbeleid van Leverancier voor zover deze volledig of hoofdzakelijk voor ROC Midden Nederland ingezet worden.

7. RAPPORTAGE EN CONTROLE

RC.1 Beveiligingsincidenten worden altijd per direct gemeld bij de security officer van ROC MN. Dit zijn onder andere:

a) Ongeautoriseerde sourcecode, database en data, server, middleware en netwerkcomponent mutaties;
b) Continuïteit, back-up & recovery fails;
c) Ongeautoriseerde koppelingen;
d) Lekken van bedrijfsinformatie.

RC.2 Periodiciteit en rapportagevorm van overige rapportages wordt in overleg met ROC Midden Nederland vastgesteld. Rapportages zijn onder andere:

a) Leverancier medewerkers met hoge rechten;
b) Tijdelijk productie autorisatie;
c) Uitwijk evaluatierapport;
d) Generieke logging over kritische werkzaamheden van beheerder;
e) Specifiek loggingrapport;
f) Parameter settings en wijzigingen van Operating Systeem en/of Security Systeem;
g) Alle aangebrachte wijzigingen in functionaliteit van de applicatiesoftware, het OS en de onderliggende infra-structuur;
h) Certificaten incl. bijbehorend normenkader;
i) Voortgang Security acties Leverancier Service Improvement Plan;
j) Third Party Memorandum incl. bijbehorend normenkader en voortgang oplevering;
k) Specifieke rapportage Netwerk en Werkstations met o.a.: Virus besmetting, Intrusion Detection, Security Patch Level, Backup en Restore.

RC.3 Leverancier voert regelmatig security- en penetratietesten uit wanneer er bij de levering van de Prestatie gebruik gemaakt wordt van (web)applicaties, (web)services en/ of infrastructuur. De diepgang en frequentie van deze security- en penetratietesten is (mede) afhankelijk van de BIV-classificatie zoals vastgesteld door ROC Midden Nederland en voldoet aan in de markt gehanteerde best practices. Nadere afspraken over de testen en rapportage worden vastgelegd in de Overeenkomst.

De security afdeling van ROC Midden Nederland moet in goed overleg met Leverancier aanvullend de mogelijkheid hebben om controles met betrekking tot de Prestatie te kunnen uitvoeren, inclusief, maar niet beperkt tot het (laten) uitvoeren van security- en penetratietesten.

RC.4 Indien programmatuur ontwikkeld wordt door Leverancier, wordt door Leverancier een periodieke controle uitgevoerd op de beveiliging van de source code. Voor webapplicaties krijgt ROC Midden Nederland de mogelijkheid om, in goed overleg met Leverancier, een penetratietest uit te voeren op de (web)applicatie, (web)server en overige componenten die onderdeel zijn van de technische keten. Deze verplichte test dient plaats te vinden vóór het systeem in productie gaat. Eventuele tekortkomingen worden na onderlinge afstemming door Leverancier opgelost.

RC.5 Indien ROC Midden Nederland aanvullende informatie nodig heeft om het beveiligingsrisicoprofiel te kunnen bepalen voor ROC Midden Nederland specifiek en voor de rol van ROC Midden Nederland als onderwijsinstelling in het bijzonder, wordt een verzoek tot informatie bij Leverancier ingediend aan welk verzoek Leverancier zo spoedig mogelijk zal voldoen.

RC.6 Binnen het periodiek overleg tussen ROC Midden Nederland en Leverancier worden onder meer security incidenten, rapportages en logging geëvalueerd en eventuele verbeteringen besproken.

RC.7 Leverancier is verantwoordelijk voor het behalen van de Third Party Memorandum en, indien van toepassing, de certificering voor de ISO27001 norm van Leverancier en eventuele onderaannemers. ROC Midden Nederland en Leverancier bepalen in gezamenlijk overleg welke set aan maatregelen hiervoor in aanmerking komen. Deze set wordt onderdeel van deze Security Agreement.

RC.8 Ten aanzien van logging gelden de minimale eisen zoals vastgelegd in de Security Baselines. Eventuele aanvullende logging op personen of gegevens wordt ingericht middels State- en Event-monitoring indien de apparatuur in eigendom is van ROC Midden Nederland.

RC.9 Leverancier ziet toe dat de systeemklok op de diverse infrastructurele componenten juist is ingesteld.

RC.10 Toegang tot sourcecode en gegevens van ROC Midden Nederland op infrastructurele componenten wordt gelogd.

RC.11 Leverancier zal een proactieve en kritische houding aannemen om samen met ROC Midden Nederland het risicoprofiel vanuit securityperspectief inzichtelijk te maken.

8. EXTERNE KOPPELINGEN

Een “Externe koppeling” is de verbinding tussen “informatiesystemen” van ROC Midden Nederland met die van externe ketenpartners waarover gegevens worden uitgewisseld zonder tussenkomst van personen. De gegevens worden door de externe ketenpartner gebruikt/geleverd om een dienst aan ROC Midden Nederland te kunnen leveren.

EK.1 Alle technische en geografische gegevens betreffende Externe Koppelingen worden aantoonbaar en transparant geregistreerd en actueel gehouden door Leverancier.

EK.2 Leverancier treft maatregelen in lijn met de door ROC Midden Nederland aangegeven classificatie van gegevens zoals deze over de Externe Koppeling gaan.

EK.3 Nieuwe, gewijzigde, vervallen Externe Koppelingen en Firewall wijzigingen worden altijd als changes beschouwd. Formele goedkeuring van de Security Officer van Leverancier is nodig vóór uitvoering.

EK.4 Indien een Externe Koppeling noodzakelijk is op infrastructuur bij Leverancier waarbij het risico van ongeautoriseerd toegang tot ROC Midden Nederland gegevens groter wordt, dan dient dit eerst afgestemd te worden met ROC Midden Nederland.

EK.5 Externe Koppelingen in eigendom van ROC Midden Nederland worden juist en volledig vastgelegd.

EK.6 Periodiek wordt de effectiviteit van beveiligingsmaatregelen op deze Externe Koppelingen door eigenaar getoetst. ROC Midden Nederland wordt over de resultaten van toetsing geïnformeerd.

9. MAATREGELEN CONFORM SECURITY ARCHITECTUUR ROC MN

Afhankelijk van het benodigde beveiligingsniveau zoals vastgesteld door ROC Midden Nederland, wordt de implementatie van de relevante maatregelen met de ROC Midden Nederland architect afgestemd conform de Architectuur van ROC Midden Nederland.

ANNEX A: BEVEILIGINGSNORMEN VOOR SYSTEEMONTWIKKELING

Door Leverancier ontwikkelde software moet veilig zijn. Om aantoonbaar en structureel veilige software te kunnen leveren dient door Leverancier gebruik te worden gemaakt van ontwikkelmethodieken die gebaseerd zijn op algemeen geaccepteerde standaarden en “Best Practices”. Voor Softwareontwikkeling geldt dat dit plaatsvindt onder (functionele) aansturing van ROC Midden Nederland, waarbij de betreffende afdelingsmanager de binnen ROC Midden Nederland geldende eisen aan de te ontwikkelen software expliciet maakt.

De voornaamste beveiligingsnormen voor systeemontwikkeling zijn hier opgenomen:

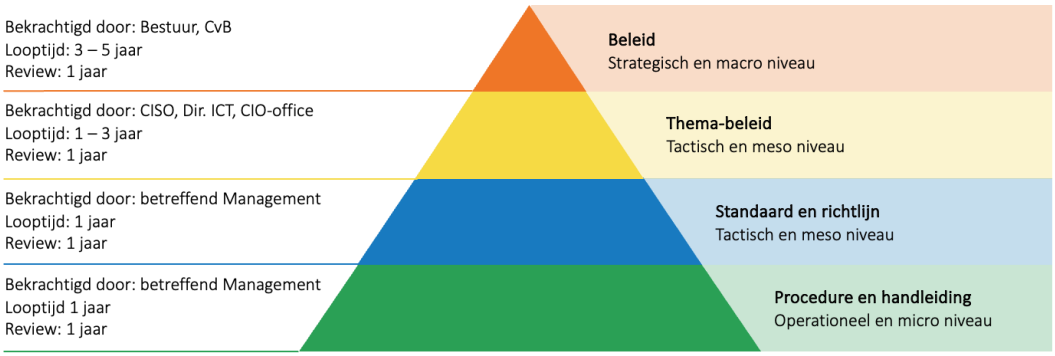
1. Leverancier dient in projectplannen de verschillende Secure Development Life Cycle (SDLC) activiteiten ter waarborging van de beveiliging op te nemen.
2. Elke ontwikkelfase dient afgesloten te worden met een formele goedkeuring van de deliverables rekening houdende met de gestelde beveiligingskwaliteitseisen. Toetsing dient plaats te vinden aan de hand van de ROC Midden Nederland Security Architectuur rekening houdende met de te gebruiken standaards binnen ROC Midden Nederland. Leverancier stemt dit af met zijn contactpersoon binnen ROC Midden Nederland.
3. Softwareontwikkelingstrajecten worden alleen gestart na een formeel akkoord door een ROC Midden Nederland architect waaronder minimaal een beschrijving van het globale risicoprofiel voor het systeem. Dit betekent dat aandacht gegeven wordt aan de BIV-classificatie en inzicht in de te treffen beveiligingsmaatregelen o.b.v. de gegevensstromen.
4. De te treffen technische en organisatorische beveiligingsmaatregelen dienen in lijn te zijn met het minimum classificatieniveau.
5. De STRIDE-methodiek van Microsoft, of een algemeen geaccepteerde equivalent hierop, dient in de analysefase toegepast te worden.
6. De mogelijke bedreigingen dienen te worden geïnventariseerd. Op basis van een impactanalyse dient vervolgens bepaald te worden welke maatregelen getroffen moeten worden.
7. Tijdens de analysefase dienen o.b.v. een threat analyse de te treffen maatregelen per risicogebied bepaald te worden. De uitkomsten dienen opgenomen te worden in het functionele en technische ontwerp.
8. Threats waarvoor op technisch niveau geen maatregelen getroffen kunnen worden dienen door de opdrachtgever beoordeeld te worden. Alleen als de systeemeigenaar het een acceptabel restrisico vindt, is een afwijking acceptabel. Dit dient formeel vastgelegd te worden ten behoeve van het verlenen van decharge in een project.
9. Een uitzonderingenlijst en de specifiek beschreven uitzonderingen dienen onder continu management aandacht te zijn van de systeemeigenaar. De systeemeigenaar is eigenaar van de lijst.
10. In het systeemontwerpdocument wordt de BIV-classificatie vermeld en het threatmodel (threats en maatregelen) opgenomen.
11. De security requirements inclusief use- en misuse cases dienen in de requirements-documentatie opgenomen te worden.
12. De (mis-)use cases dienen door vertaald te worden naar te realiseren technische en organisatorische maatregelen in het ontwerp. Hierbij rekening houdende met standaardoplossingen en beveiligingsmaatregelen in relatie tot de threat list, security building blocks en de security guidelines.
13. Voor de verschillende ontwikkelmethodes en ontwikkelplatformen dient een secure coding standaard (baseline per platform) opgesteld te zijn welke in lijn is met deze richtlijn uitgaande

van de security guidelines. Indien de ontwikkeling uitbesteed is, dient Leverancier een secure code standaard te hebben die minimaal gelijkwaardig is aan de door ROC Midden Nederland gehanteerde standaard.

14. Bij de bouw van een applicatie dienen maatregelen getroffen te worden om de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens te waarborgen. Hiervoor dient minimaal rekening gehouden te worden met maatregelen die de beveiliging van gegevens waarborgen:
15. Voor de waarborging van de toekomstige beschikbaarheid, integriteit en vertrouwelijkheid van de applicatie en bijbehorende gegevens dient een actueel test plan opgesteld te worden. De kwalitatieve inhoud dient aan te sluiten op de (non-) functional requirements (threatlist, use en misuse, security guidelines en architectonische security building blocks)
16. Leverancier is bereid een ESCROW-overeenkomst aan te gaan ten behoeve van de borging van de continuïteit.
17. Met het testen van functionaliteit wordt rekening gehouden met de classificatie van de gegevens.
18. Alle systeemdocumentatie, functioneel en technisch ontwerp, testverslagen, project start en end architectuur dienen op een beveiligde locatie bewaard te zijn (fysiek en logisch beveiligd).
19. De infrastructuur van de Ontwikkel-, Test-, Integratie-, Acceptatie-, Leer-, Productie-omgeving dient over het geheel aan componenten eenzelfde patch en beveiligingsniveau te hebben.
20. Technische kennis van de applicatie in relatie tot de bedrijfsprocessen en keuzes die gemaakt zijn, dient gewaarborgd te blijven.
21. Ontwikkelaars dienen geen autorisatie te hebben in de productieomgeving en databaseomgeving.
22. De ontwikkelde programmatuur dient in een SMDB (Software Management Database) beschreven te zijn rekening houdende met versiebeheer, documentatie, koppelingen naar de CMDB, ketenafhankelijkheden, systeemeigenaar.

ANNEX B: BELEIDS- EN DOCUMENTSTRUCTUUR

Het informatiebeveiligingsbeleid maakt onderdeel uit van het beleid integrale veiligheid. Voor informatiebeveiliging wordt binnen ROC Midden Nederland een beleidsstructuur toegepast met formeel vastgestelde documenten op strategisch, tactisch en operationeel niveau. Voor alle documenten in de beleidsstructuur geldt dat zij minstens één keer per jaar worden beoordeeld en bijgewerkt om relevantie en actualiteit te waarborgen.



Figuur 1: Beleidsstructuur met beoogde looptijden

Beleid

Documenten op het strategisch niveau geven richting: waar staan we nu, wat willen we bereiken, waarom willen we dit bereiken en waar gaan we ons naartoe bewegen. Deze documenten beschrijven het beleid, voor de periode van 3 tot 5 jaar en zijn formeel bekrachtigd door het College van Bestuur.

Thema-beleid

Documenten op het tactische niveau geven sturing op een specifiek domein of thema: hoe geven we invulling aan onderdelen van het beleid en welke principes zijn daarbij leidend? Deze documenten beschrijven het thema-beleid, normaliter voor een periode van 1 tot 3 jaar en zijn formeel bekrachtigd door de Directeur DOS & IIM (Dienst Onderwijs Services en ICT & Informatie Management). Thema-beleid heeft vaak programma-elementen, en bestaat dus deels uit standaarden en richtlijnen maar ook deels uit veranderplannen en -planningen.
Binnen ROC Midden Nederland onderscheiden we de volgende thema's:

- Risicobeheer inclusief risico- en informatiebeveiligingsactieplannen, al of niet gecombineerd in een roadmap;
- HR-aangelegenheden waaronder awareness campagnes;
- Datamanagement waaronder systeem- en dataclassificatie;
- Identity- en Access Management;
- Operationeel securitymanagement inclusief security baselines voor technische inrichtingen en technische weerbaarheid;
- ITIL-gerelateerde processen zoals configuratiemanagement, incident-, problem- en change management, en fysieke beveiliging maar ook de beheersing van systeemontwikkeling;
- Business ContinuïteitsManagement;
- Leveranciersmanagement, waaronder Cloud-beheer.

Standaarden en richtlijnen

Ook op dit tactische niveau geven de documenten sturing op een specifiek domein of thema: hoe gaan we specifiek invulling geven aan het beleid of thema-beleid en welke standaarden en richtlijnen zijn daarbij leidend? Deze documenten beschrijven de standaarden en richtlijnen in meer detail, voor langere periodes en zijn formeel bekrachtigd door het betreffend management.
Standaarden geven maatregelen die moeten worden opgevolgd om zo te voldoen aan een beleid, framework, certificering of wet- en regelgeving. Richtlijnen geven advies of sturing bij het uitvoeren van standaard of procedure, maar alternatieve werkwijzen waarmee hetzelfde doel wordt bereikt, zijn mogelijk ('Pas toe of leg uit').
Standaarden en richtlijnen zijn gericht op procedures rond technische maatregelen en technische weerbaarheid.

Procedures, handleidingen en rapporten

Documenten op het operationele niveau zijn uitvoerend: wie doet wat, wanneer en op welke wijze. Deze documenten beschrijven de processen en procedures in detail als operationele handleidingen en zijn, waar noodzakelijk geacht, formeel bekrachtigd door het betreffend management. Ook standaardrapporten en andere formats vallen hieronder.

SECURITY AGREEMENT v1.2
ROC Midden Nederland

Dienst Onderwijs Services en ICT & Informatie Management
Auteur: Edo Meinema
Contactpersoon: Pepijn de Vette