Informatiebeveiligingsbeleid en beveiligingsmaatregelen

Documentnaam:	Informatiebeveiligingsbeleid en beveiligingsmaatregelen
Versie:	1.2
Datum:	Januari 2021

Missing Piece BV • Frankenweg 2 • Postbus 250 • 3960 BG Wijk bij Duurstede • T+31 (0)33 750 81 81 • Servicedesk T+31 (0)33 750 81 00
info@missingpiece.nl • www.missingpiece.nl • KvK 30198258 • Bank NL03INGB0006407883 • BTW NL8138.97.956.B01

Inhoud

1. Informatiebeveiligingsbeleid

1.1. Inleiding

Voor u ligt het informatiebeveiligingsbeleid van Missing Piece BV. Binnen dit document beschrijven wij de kaders van het informatiebeveiligingsbeleid, de getroffen beveiligings-maatregelen en de visie die wij op informatie-beveiliging hebben.

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten “beschikbaarheid”, “integriteit” en “vertrouwelijkheid” van de informatie-voorziening te garanderen. De kwaliteitsaspecten:

- *Beschikbaarheid:* de mate waarin gegevens of functionaliteiten op de juiste momenten beschikbaar zijn voor de gebruikers;
- *Integriteit:* de mate waarin gegevens of functionaliteiten juist ingevuld zijn;
- *Vertrouwelijkheid:* de mate waarin de toegang tot gegevens of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.

Hierbij gaat het ook om de controleerbaarheid van de maatregelen die genomen zijn om deze kwaliteitsaspecten te borgen.

De directie verplicht zichzelf tot het naleven van de voorschriften volgens de ISO/IEC 27001:2013 en verklaart al het nodige te doen om het managementsysteem op te zetten en te implementeren, op peil te houden en de effectiviteit van het systeem daar waar nodig continue te verbeteren. De directie ziet er op toe dat de integriteit van het management-systeem wordt gehandhaafd wanneer veranderingen worden doorgevoerd.

1.1.1. Toepassingsgebied

Het toepassingsgebied van het informatiebeveiligingsbeleid is als volgt gedefinieerd:
Het realiseren van IT-infrastructuur en het leveren van:

- consultancy-,
- hosting-,
- applicatie-,
- beheer- en
- supportdiensten.

Ten behoeve van de diensten Koper, Brons en Zilver in overeenstemming met de Verklaring van Toepasselijkheid versie 2.1 d.d. 02-10-2018.

1.1.2. Doelstellingen van het informatiebeveiligingsbeleid

- Het beschermen van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie;
- Behalen van de met klanten overeengekomen contractafspraken en SLA's;
- Beheersing van risico's op het gebied van informatiebeveiliging en het voldoen aan wet- en regelgeving;
- Voldoen aan beleidsregels, processen, procedures en andere werkafspraken om bovenstaande doelen te kunnen bereiken.

1.1.3. Uit te voeren activiteiten voor het bereiken van de doelstellingen

Het management van informatiebeveiliging is als proces ingericht. Dit houdt in dat de jaarlijkse planning en controlcyclus conform ISO27001 wordt uitgevoerd (Plan, Do, Check, Act). Er worden jaarplannen opgesteld en uitgevoerd. De resultaten ervan worden geëvalueerd en vertaald naar nieuwe jaarplannen (Management review).

1.1.4. Inschakelen andere verwerkers

Indien Missing Piece BV andere verwerkers inschakelt ter uitvoering van de verplichtingen voortvloeiende uit de overeenkomst met haar relaties is deze, conform artikel 6 uit de Verwerkersovereenkomst, verplicht de relatie (is de verwerkersverantwoordelijke) hiervan op de hoogte te stellen.

De lijst van sub-verwerkers is als bijlage bij dit document gevoegd. Mochten zich mutaties in deze lijst voordoen wordt er een nieuwe bijlage verstrekt.

1.2. Informatiebeveiliging gedurende Projecten / Consultacy opdrachten

Missing Piece deelt informatie en projectdocumentatie tijdens de uitvoering van het project uitsluitend met onze primaire en secundaire betrokkenen bij de klant.

Missing Piece deelt informatie en projectdocumentatie gepast en selectief met de leveranciers en externe betrokkenen tijdens de uitvoering van het project.

Missing Piece verwerkt de gegevens van de betrokkenen initieel in de inventarisatie uitwerkingen en de projectadministratie (Cherwell), vanaf dat moment wordt in de projectadministratie de laatste status van alle betrokkenen vastgelegd.

Bedrijven of personen buiten de geregistreerde betrokkenen zullen van Missing Piece alleen informatie ontvangen via de primaire of secundaire contactpersoon bij de klant.

Zodra zich nieuwe betrokkenen melden tijdens de uitvoering van het project zal de projectleader van Missing Piece een inschatting maken van de relevantie van deze betrokkenen tot het project en deze indien relevant, toevoegen aan het project in de projectadministratie. Bij twijfel zal dit in samenspraak met de primaire contactpersoon besloten worden.

Missing Piece zal tijdens de uitvoering van het project leveranciers en externe betrokkenen toegang verschaffen tot de systemen van de klant, hiervoor wordt een leveranciersaccount aangemaakt per leverancier of externe betrokkene.

Hoe wil de klant dat we hier tijdens de uitvoering van het project mee omgaan:

☒ Missing Piece kan zonder toestemming leveranciers en externe toegang verschaffen tot het systeem, zolang dit in het belang is van het project. Bij twijfel overleggen we met de Projectleader en de primaire contactpersoon van cliënt. *(Voorkeur Missing Piece)*

☐ Missing Piece vraagt eerste toestemming aan de klant, voordat wij leveranciers en externe toegang verschaffen tot het systeem. *(Dit kan vertragend werken)*

In het geval dat Missing Piece tijdens de uitvoering van het project te maken krijgt met datauitwisseling zullen wij dit uitvoeren conform hetgeen hierover beschreven is in de Algemene Voorwaarden van Missing Piece BV.

1.3. Beveiligingsmaatregelen

1.3.1. Algemeen

Missing Piece BV is in het bezit van een ISO27001:2013 certificering voor informatie-beveiliging. De in verband hiermee geïmplementeerde beheersmaatregelen zijn opgenomen in de Verklaring van Toepasselijkheid.

Enkele met name te noemen beheersmaatregelen opgenomen in de Verklaring van Toepasselijkheid zijn:

- Personeel wordt voorafgaande aan het dienstverband gescreend;
- Personeel heeft een geheimhoudingsverklaring ondertekend;
- Er is een beleid voor geclassificeerde informatie;
- Er is een clear-desk en clear-screen beleid van toepassing.

In het Beleid voor Aanvaardbaar Gebruik zijn onder meer zaken geregeld als; omgang met mobiele apparatuur, wachtwoordbeleid, telewerken etc.

In het managementsysteem voor informatiebeveiliging (ISMS), opgezet in kader van de ISO27001:2013 certificering, is onder meer opgenomen dat Missing Piece BV jaarlijks een risicobeoordeling van de informatiebeveiliging uitvoert en een behandelplan opstelt voor de behandeling van informatie beveiligingsrisico's.

De doeltreffendheid van het ISMS wordt geëvalueerd door het periodiek monitoren en meten van onder andere de omgang met en de uitvoering van de vastgestelde beheersmaatregelen. Deze resultaten hiervan worden en vastgelegd en jaarlijks meegenomen in de hierboven genoemde risicobeoordeling. Daarnaast vindt er jaarlijks een interne en een externe audit plaats.

1.3.2. Fysieke Beveiligingsmaatregelen

De opslag van data vindt plaats op servers die in beheer zijn bij Missing Piece BV, deze bevinden zich in het datacenter van BIT te Ede. De off-site back-up bevindt zich in het datacenter AM5 van Equinix te Amsterdam.

BIT Datacenter factsheet

Hoogte serverruimte:	Minimaal 6 meter boven NAP
Vloerbelasting	1500 kg/m²
Afmeting racks	46 HE hoog, 60 cm breed, 100 cm diep
Branddetectie	Een onafhankelijk, gecertificeerd very-early-warning systeem met automatische doormelding naar de brandweer
Brandblussing	Gecertificeerde installatie met Argonite (Ar+N²)
Koelinstallatie	N+1 computairs N+1 koelmachines
Koelvermogen	1500 W/m²
Temperatuur	25 °C (+/- 2 °C) in koude paden
Bliksembeveiliging	Gecertificeerd volgens NEN-normen
Elektrische installatie	Twee inkomende feeds tot in rack aparte UPS voor iedere feed
Noodstroomvoorziening	N+1 dieselaggregaten
Dieselvoorraad	48 uren
Stroom per rack	Tot 96 A
Informatiebeveiliging	ISO/IEC 27001 en NEN 7510 gecertificeerd
Fysieke beveiliging	VEB gecertificeerd beveiligingsklasse 4*
Alarm	Redundante verbinding naar meldkamer
Surveillance	Twee onafhankelijke surveillancediensten
Toegangscontrole	Dubbele authenticatie biometrisch met irisscanners RFID toegangspassen
Service Level Agreement	Beveiliging klimaat stroom

Beveiliging datacenter Ede:
Camera's, zowel buiten als binnen;
Inbraakbeveiligingssysteem;
Twee onafhankelijke surveillancediensten;
Redundante verbinding naar meldkamer;
Dubbele authenticatie met RFID-toegangspassen en irisscanners;
VEB gecertificeerd, beveiligingsklasse 4;
ISO/IEC 27001 en NEN 7510 gecertificeerd.

Brandbeveiliging datacenter Ede:
De serverruimtes bij BIT zijn voorzien van een onafhankelijk, gecertificeerd very-early-warning (VEW) systeem met automatische doormelding naar de brandweer. Wanneer er

een brand uitbreekt wordt de zuurstofconcentratie in de ruimte door gasblussing verlaagd zodat het vuur snel dooft. Hiervoor wordt een gasmengsel van Argon en stikstof gebruikt (Argonite). Door op deze manier de brand te bestrijden ontstaat er geen (water)schade aan de apparatuur.

Koeling datacenter Ede:
De datacenters van BIT staan vol met servers die veel warmte produceren. Bij meer computeractiviteit betekent dit dat er ook meer warmte vrijkomt, daarvoor is gespecialiseerd, schaalbaar en betrouwbaar warmtebeheer nodig. Ontoereikende koeling kan namelijk dure onderbrekingen veroorzaken. De koelinstallatie zorgt in combinatie met de closed-cold-corridors voor een optimale koeling van alle apparatuur. De installatie is op alle punten, inclusief pompen en leidingwerk, redundant uitgevoerd. Daarnaast is de installatie zo energiezuinig mogelijk, wat zowel het milieu als kosten bespaart.

Stroomvoorziening datacenter Ede:
Voor bedrijven, organisaties en overheden is een goede stroomvoorziening één van de belangrijkste redenen om hun IT-apparatuur in een datacenter te plaatsen. Om de betrouwbaarheid van die stroomvoorziening te garanderen worden noodstroom-voorzieningen maandelijks getest.
BIT-2BCD heeft twee rechtstreekse aansluitingen op het verdeelstation van de netbeheerder. De stroom- en noodstroomvoorziening zijn tot in de racks volledig dubbel uitgevoerd.

Equinix Datacenter Factsheet

Colocation space	6000 kg/m2
Building type	2 floors, concrete steel frames
Floor type	Raised
Floor load capacity	2000 kg/m²
Seismic design category	Low
Fire Suppression	VESDA, HI-FOG, water mist fire suppression, double knock fire activation
Power and cooling density	3.0 - 15.0 kVA
Utility feeders	2 x 15 MVA
UPS redundancy	N+1
Standby power configuration	8 x 2.410 kVA 2 x 2.410 kVA
Standby Power redundancy	N+1
Cooling configuration	Chilled water + ATES
Cooling redundancy	N+2
Physical security	Man trap entry, single entry point, CCTV surveillance, proximity access card, BMS perimeter intruder alarm, perimeter fence
Human security	24x7 onsite security officers
Electronic security	Card readers, biometric readers, CCTV

	surveillance with 90 day video retention
Certifications	ISO 14001:2004 ISO 27001 ISO 50001 ISO 9001:2015 OHSAS 18001 PCI DSS SOC 1 Type II SOC 2 Type II

1.3.3. Databeveiligingsmaatregelen

Back-up procedure

De productie-data wordt continu naar productie (harde) schijven geschreven. Deze productie schijven zijn meervoudig (redundant) uitgevoerd. Vervolgens wordt deze data gekopieerd naar back-upschijven en wordt de data extra gekopieerd naar back-up schijven off-site in een separaat datacenter. De back-upschijven zijn ook in beide gevallen meervoudig uitgevoerd.

De back-up wordt zes (6) nachten per week (maandag tot en met zaterdag) gemaakt en is beschikbaar voor een periode van 90 dagen. Zes (6) nachten per week (maandag tot en met zaterdag) wordt er een extra back-up gemaakt van de productie-data naar de back-up schijven off-site in een separaat datacenter. Deze back-up is beschikbaar voor een periode van 10 dagen en dient als disaster recovery.

Alle back-up processen zijn standaard voorzien van verificatie, hiermee wordt weggeschreven data opnieuw gelezen en wordt aannemelijk gemaakt dat de data niet alleen met succes is weggeschreven, echter dat deze ook uitgelezen kan worden. Wordt hier een fout gevonden dan wordt hiervan in de netwerk monitoring tool PRTG een visuele melding gemaakt, tevens zal het back-up record in het IT-Service Managementsysteem de mislukte back-up tonen. Dit back-up record is tevens zichtbaar voor de klant in het Missing Piece Service Portal.

Iedere werkdag wordt in de ochtend (onafhankelijk van bovenstaande meldingen) een controle gedaan op de statussen van de back-up. Op het moment dat een back-up niet geslaagd is zal de oorzaak van het mislukken worden opgelost en de back-up handmatig worden herstart.

Restoretest procedure

Iedere zaterdag wordt de restoretestprocedure automatisch uitgevoerd, er vindt een restoretest plaats voor alle aanwezige back-upjobs (= alle klanten die hun data in onze datacenters hebben opgeslagen).

De procedure wordt alleen uitgevoerd voor de data op het primaire datacenter (BIT, Ede).

De restoretest vindt op willekeurige bestandselectie plaats per backupjob, er is dus geen volledige restore. Voor de steekproef wordt de volgende methode toegepast.

-
- Minimum bestandsgrootte is 10kb, de maximale bestandsgrootte is 1mb
- Het bestand is ouder dan 100 dagen
- Het aantal te restoren bestanden is maximaal 100 stuks
- Het maximaal aantal retries op de servers is 10 (is een server toegankelijk)
- Het maximaal aantal retries op de files is 100

Wordt er een fout in de restore gevonden dan zal dit visueel zichtbaar zijn in de monitoring tool PRTG, tevens zal het restoretest-record in het IT Service Managementsysteem de mislukte restoretest tonen. Dit is tevens zichtbaar voor de klant in het Missing Piece Service Portal.

Volledige restore virtuele servers uit back-up

Missing Piece zorgt jaarlijks voor een volledige restore van de virtuele machines in een geisoleerde omgeving op haar infrastructuur. Deze restore procedure is gebaseerd op het 'Zilver Concept' zoals aangeboden wordt door Missing Piece aan haar klanten. Hiermee is deze restore door blauwdruk voor elk van de bij Missing Piece aangesloten omgeving, omdat elke omgeving binnen dit concept op dezelfde manier binnen de procedure van back-up, restore en functionele inrichting bestaat. Het onderscheid tussen de klantomgevingen bevindt zich in de omvang, het aantal servers en de kernapplicatie die wordt teruggezet en zit het verschil in de doorlooptijd voor deze procedure per klant.

Ter volledigheid is gekozen om de procedure voor een volledige restore uit te voeren op elk van de 4 mogelijke kernapplicaties, te weten ANVA, Level, DIAS en ASSU. Alle bij Missing Piece aangesloten klantomgevingen vallen binnen een van de vier genoemde categorieën met de kernapplicatie.

Van de uitvoering, de logs en het verloop in detail wordt een rapportage[1] opgesteld welke gedistribueerd kan worden aan haar klanten. Deze uitvoering van een volledige restore dient als aanvulling op de rapportages van de klant specifieke back-up status, en deel-restore die uitgevoerd wordt. Hiermee wordt expliciet aangetoond dat uit de procedure van back-up een herstel van de machines uitgevoerd kan worden in een functioneel operationele infrastructuur van Missing Piece.

De volledige restore procedure zoals uitgevoerd is een blauwdruk van het concept van Missing Piece en reikt tot aan het terugzetten in productie van de machine. Er wordt niet getest op de dataset welke eigendom is van de klant. Hiervoor wordt een aparte restore module opgesteld welke individueel per entiteit is af te nemen, en daarmee de test specifiek maakt voor de klantomgeving, en breder trekt door een aanvullende testfase welke door klant wordt afgetekend.

[1] *Beschikbaar in document "MissingPiece_Full-VM-Restore_Dienstverlening_Concept_Zilver_v1.0"*

Updates en patches

Microsoft updates

- De updates worden meerdere keren per dag automatisch gedownload;
- De monitoringstool PRTG geeft een melding dat er updates zijn opgehaald;
- Deze updates worden dagelijks ('s nachts) automatisch geïnstalleerd op de werkstations (fat-clients, alleen indien ze op het netwerk zijn aangesloten) en de Webservers;
- De updates worden wekelijks automatisch geïnstalleerd op een aantal geselecteerde XAP's en CTX'en(Citrix servers), dit zijn de servers van Missing Piece en de Missing Piece testomgeving;
- Indien er updates zijn (PRTG-melding) worden deze door de system administrator wekelijks handmatig geïnstalleerd op een 10-tal geselecteerde INFRA-servers;
- De laatste vrijdag van de maand wordt er door een (Senior) system administrator handmatig een accordering gegeven voor het uitvoeren van de updates op alle XAP-servers, alle ASK-servers en alle INFRA-servers;
- Naar aanleiding van de bovengenoemde accordering worden de updates op alle XAP-servers in de nacht van vrijdag op zaterdag automatisch uitgevoerd;
- Idem voor de ASK- en INFRA servers in de nacht van zondag op maandag.

Voor elke server die wordt geüpdatet wordt automatisch een reboot uitgevoerd. Er kan besloten worden bepaalde updates niet uit te voeren indien er signalen van derden zijn die problemen melden naar aanleiding van een update.

Updates thin-clients

Thin-clients worden geüpdatet door de afdeling System Administration wanneer nodig bevonden wordt, minimaal elk kwartaal wordt dit beoordeeld.

Updates overige software

Overige updates worden uitgevoerd op het moment dat er signalen zijn van derden dat er bijvoorbeeld een beveiligingslek is, daarnaast is een schema gemaakt met welke frequentie er minstens op updates gecontroleerd moet worden.

Beveiligingsbeheer voor het netwerk

- De gegevens passerend over het publieke netwerk zijn op verschillende manieren beveiligd;
- Verbindingen van klantlocaties naar het datacenter zijn beveiligd door middel van site-to-site VPN(Virtual Private Network);
- Verbindingen die tot stand komen door telewerken zijn beveiligd door middel van SSL VPN (Secure Socket Layer VPN);

- Voor e-mailverkeer is in de mailserver de 'preferred' optie aangezet voor versleuteling (TLS);
- De gegevens passerend over het draadloze netwerk zijn beveiligd door (uitgeleverde) Wifi te versleutelen door middel van WPA2-PSK;

- De apparatuur verbonden aan het netwerk vanaf externe locaties is beveiligd door de eis om met een RSA-token in te loggen;
- De beschikbaarheid van de netwerkdiensten wordt gewaarborgd doordat alles in het SAN, UCS-systeem en netwerkapparatuur redundant is uitgevoerd. Daarnaast beschikt de productieapparatuur over 24/7/4 support contracten.

Systeemmonitoring

Missing Piece maakt gebruik van de netwerkmonitoring tool PRTG.
Via PRTG wordt, door middel van meer dan 21.000 sensoren, veel gemonitord zoals: het netwerk, back-up-/restoretest, stroomverbruik, updates, certificaten, etc. Voor bepaalde problemen zijn alerts ingesteld.
Een alert kan bestaan uit:

- Een e-mailbericht richting de Servicedesk;
- Een melding op het monitoringscherm op de afdeling System Administration (deze meldingen worden tevens getoond op de smartphones van de medewerkers van deze afdeling).

Bescherming tegen malware

Er zijn op verschillende niveaus maatregelen tegen malware genomen:

- Door middel van ESA (E-Mail Security Appliance) wordt binnenkomend en uitgaand e-mail verkeer gescand;
- Door middel van Trendmicro Scanmail scant de Exchange server e-mails;
- Alle Windows machines bevatten antivirussoftware (Microsoft System Center Endpoint Protection);
- Op basis van file masks van cryptoware extensies worden alerts naar de servicedesk en een selectieve groep gestuurd;
- Bij bepaalde extensies wordt de gebruiker automatisch afgemeld;
- Daarnaast wordt door middel van Windows Firewall Rules (ACL's) verkeer tussen klanten geblokkeerd zodat malware zich niet tussen klanten kan verspreiden.

Overig

Binnen de omgeving van Missing Piece is de volgende wachtwoordpolicy van toepassing:
Een wachtwoord dient aan de volgende voorwaarden te voldoen (dit wordt door het systeem afgedwongen):

- Tenminste zeven tekens gebruiken (maak bij voorkeur een password aan van 12 posities of meer);
- De vorige 24 wachtwoorden mogen niet opnieuw worden gebruikt;
- De inlog-, voor- en achternaam mogen geen deel uitmaken van het wachtwoord;

- Een wachtwoord moet een of meerder karakters uit drie van de volgende vier categorieën bevatten:
    - Hoofdletters
    - Kleine letters
    - Getallen
    - Niet alfanumerieke karakters zoals leestekens

- Bij het vijf maal intoetsen van een foutief wachtwoord wordt het account een half uur geblokkeerd, waarna er opnieuw in inlogpoging kan worden gedaan. Er kan ook een verzoek aan de Servicedesk worden gedaan voor een wachtwoord reset;
- Wachtwoorden moeten elke 120 dagen worden gewijzigd. Hierover krijgt de gebruiker een melding per e-mail. Inloggen is pas weer mogelijk nadat het wachtwoord is gewijzigd;
- Screensaver instellingen binnen de omgeving.

1.4. Procedure bij Datalek

1.4.1. Constatering datalek

Er wordt door Missing Piece, Cliënt of een derde een datalek geconstateerd. Missing Piece zal overeenkomstig het crisismanagementplan het datalek als grote crisis behandelen. Missing Piece zal direct een crisisteam samenstellen en Cliënt binnen 1 werkdag op de hoogte stellen van het datalek.

Cliënt dient zelf binnen uiterlijk 72 uur na het ontstaan, of na redelijkerwijs kunnen ontdekken van het datalek een melding te doen bij de Autoriteit Persoonsgegevens (AP).

1.4.2. Acties crisisteam

Het samengestelde crisisteam van Missing Piece zal primair de reden van het datalek achterhalen om vervolgens direct maatregelen te treffen om het verder lekken van data te voorkomen. Vervolgens dient er vastgesteld te worden welke data (gegevens) er is gelekt, waarna Cliënt door Missing Piece op de hoogte zal worden gesteld.

Het crisisteam zal vervolgens controleren of er sprake is van meerdere datalekken, eventueel bij andere Cliënten van Missing Piece.

Het crisisteam zal alle uitgevoerde acties en communicatie vastleggen als incident. Nadat het datalek is verholpen zal het crisisteam het incident evalueren en besluiten of, en zo ja welke maatregelen er getroffen dienen te worden om dit voor in de toekomst te voorkomen.

1.4.3. Acties cliënt

Cliënt is zelf verantwoordelijk voor het melden van het datalek binnen 72 uur bij de Autoriteit Persoonsgegevens (AP) en dient in het geval van een datalek alle medewerking te verlenen aan Missing Piece om maatregelen te treffen om het verder lekken van data te

voorkomen en mee te werken aan maatregelen om eventuele nieuwe incidenten te voorkomen.

Bijlagen bij dit document:

i. Versie geschiedenis
ii. Lijst van sub verwerkers;
iii. ISO certificaat;
iv. Security Audit Rapportage Reqon Security BV
v. Verklaring van toepasselijkheid.

2. Bijlagen

B-I. Versie geschiedenis

v.1.0 ; januari 2020 ; Initiële uitgifte Informatie Beveiligingsbeleid Document (IBB)
- Samenvoeging documentatie ISMS binnen 1 document ter distributie

v.1.1 ; juni 2020 ; Revisie initiële documentatie inclusief nieuwe toevoegingen
- Toevoeging pentest rapportage Reqon Security
- Herindeling en samenvoeging hoofdstukken datacenter informatie en back-up/restore procedures
- Uitbreiding lijst van sub verwerkers

v.1.3 ; januari 2021 ; Revisie documentatie
- Invoegen nieuwe certificering ISO27001

B-II. Lijst van sub-verwerkers

Bedrijfsnaam sub verwerker	Doel
BIT	Datacenter Services
Equinix	Datacenter Services
VMWARE	Platform infrastructuur
Veeam	Platform back-up
Bittitan	E-mailmigraties
Zivver	Secure E-mail services
SmartLockr	Secure E-mail services
Spotler	E-mailcommunicatie
Microsoft	Operating System /Office Intergratie/Skype for Business
Cisco	End Point Security
Panas	SVB
Voicedata	VoIP Services
Codelathe	Filecloud Services
Worksteampeople	Anywhere365
Code Two	Office365 Migratie
Thinkscape	Office365 Migratie
CloudAlly	Office365 Cloud Backup
AA-Express	Hardware distributie
IRentsystems	Tijdelijke inzet hardware
OneTrust	Privacy Management SaaS
ANVA	Software verzekerings PaaS
OptiTune	Cloud werkplek/client beheer

B-III. Kopie certificaat ISO27001

DNV·GL

MANAGEMENTSYSTEEM CERTIFICAAT

Certificaat nr.:	Initiële certificatie datum:	Geldig:
241221-2017-AIS-NLD-UKAS	17 januari 2018	16 januari 2021 – 16 januari 2024

Dit is ter bevestiging dat het managementsysteem van

Missing Piece B.V.
Frankenweg 2, 3962 CE Wijk bij Duurstede, Nederland

voldoet aan de eisen gesteld in de Informatie Beveiliging Management Systeem norm:

ISO/IEC 27001:2013

Dit certificaat is geldig voor de volgende scope:

Leveren van hardware, consultancy, hosting-, applicatie-, beheer- en supportdiensten in overeenstemming met de verklaring van toepasselijkheid versie 2.2 van 10-09-2020.

B-IV. Security Audit Reqon Security B.V.

Publieke samenvatting IT-beveiligingsonderzoek

19-05-2020

Missing Piece ontzorgt ondernemers op het gebied van ICT. Zo bieden zij hun klanten de mogelijkheid om te werken binnen een VDI-omgeving. Binnen deze VDI-omgeving verwerken de klanten vertrouwelijke gegevens. Om de beschikbaarheid, integriteit en vertrouwelijkheid van deze gegevens te waarborgen is het van belang dat de omgeving adequaat is beveiligd.

Om meer zicht te krijgen op de mogelijke kwetsbaarheden binnen de IT-beveiliging van de VDI-omgeving heeft Missing Piece aan REQON de opdracht gegeven om een onafhankelijk beveiligingsonderzoek uit te voeren. REQON is gespecialiseerd in het uitvoeren van onafhankelijke technische beveiligings-onderzoeken in de vorm van penetratietesten (pentesten). De uitkomsten van dit onderzoek zullen ondersteuning bieden bij het verhogen van het beveiligingsniveau.

Er is vanuit drie verschillende perspectieven onderzoek gedaan, namelijk zonder authenticatie/autorisatie, met autorisatie en vanaf het klantennetwerk. De testperspectieven zijn uitgevoerd in de vorm van:

- een blackbox perspectief op de VDI-omgeving en het login mechanisme;
- een greybox perspectief op de klantomgeving VDI 2.0 & 3.0;
- een on-site perspectief bij een klant van Missing Piece (ter beoordeling van het netwerk).

Uit het onderzoek zijn 7 bevindingen gekomen. De risico's van deze bevindingen zijn volgens het Common Vulnerability Scoring System (CVSS) geclassificeerd. Twee bevindingen zijn daarbij geclassificeerd als 'Kritiek', twee als 'Hoog' en drie als 'Midden'. De kwetsbaarheden zijn voornamelijk te wijten aan misconfiguraties of 'vergeten' tijdelijke implementaties. Missing Piece heeft tijdens het onderzoek direct maatregelen genomen om de kritieke kwetsbaarheden te mitigeren.

Missing Piece heeft aangegeven om, naar aanleiding van het onderzoek, haar interne IB-beleid en de change-procedures te verscherpen, om zo de kans op misconfiguraties te verkleinen. Daarbij zullen aanvullende controls worden geïmplementeerd die automatisch kwetsbare configuraties detecteren. Tenslotte zullen zij periodiek beveiligingsonderzoeken uit laten voeren ter controle en verbetering van het beveiligingsniveau.

Risico- en aanbevelingsmodel

Aanbevolen maatregelen

Aanbevelingsscore Schaal 1-10	Maatregel	Complexiteit van de implementatie*	Te mitigeren kwetsbaarheden
10	Segmenteer het netwerk	2	001/004/006
5	Versleutel back-ups	2	001
4	Stel een beleidsplan op voor het managen van wachtwoorden	2	004
3	Beperk het aantal Domain-Admin-Accounts	2	007
3	Waarborg juiste permissies	5	002/003
3	Implementeer autorisatie en authenticatie op vertrouwelijke services	5	001/006
2	Koppel de IP-whitelist aan specifieke klant	2	005
1	Volg de Microsoft 'best-pracices' op voor het inrichten van de Active Directory	5	007

*De classificatie van de complexiteit is naar inschatting van de onderzoekers en kan afwijken van de werkelijke complexiteit.

B-V. Verklaring van toepasselijkheid (versie 2.1 d.d. 02-10-2018)

		Wijze van implementatie	Van toepassing?
A.5 Informatiebeveiligingsbeleid			
A.5.1 Aansturing door de directie van de informatiebeveiliging			
A.5.1.1	Beleidsregels voor informatiebeveiliging	ISMS	Ja
A.5.1.2	Beoordeling van het informatiebeveiligingsbeleid	ISMS	Ja
A.6 Organiseren van informatiebeveiliging			
A.6.1 Interne organisatie			
A.6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging	ISMS, Functieprofielen	Ja
A.6.1.2	Scheiding van taken	Functieprofielen, Gebruikers toegangsbeleid, Personeelshandboek Gedragslijnen Autorisaties, Autorisatiematrix	Ja
A.6.1.3	Contact met overheidsinstanties	Lijst van relevante overheidsinstanties	Ja
A.6.1.4	Contact met speciale belangengroepen	Lijst van speciale belangengroepen	Ja
A.6.1.5	Informatiebeveiliging in projectbeheer	Beleid informatiebeveiliging in Projecten	Ja

A.6.2 Mobiele apparatuur en telewerken			
A.6.2.1	Beleid voor mobiele apparatuur	Beleid voor BYOD, Beleid voor aanvaardbaar gebruik	Ja
A.6.2.2	Telewerken	Beleid voor BYOD, Beleid voor aanvaardbaar gebruik	Ja
A.7 Veiligheid personeel			
A.7.1 Voorafgaand aan het dienstverband			
A.7.1.1	Screening	Algemeen informatie beveiligingsbeleid, Procedure medewerker aannemen	Ja
A.7.1.2	Arbeidsvoorwaarden	Verklaring van goedkeuring van het ISMS	Ja
A.7.2 Tijdens het dienstverband			
A.7.2.1	Directieverantwoordelijkheden	Verklaring van goedkeuring van het ISMS	Ja
A.7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	ISMS, Algemeen informatiebeveiligingsbeleid, Procedure medewerker aannemen	Ja
A.7.2.3	Disiplinaire procedure	Sanctiebeleid, Procedure medewerker indienst	Ja
A.7.3 Beëindiging en wijziging van dienstverband			
A.7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	Arbeidsovereenkomst, Procedure medewerker functiewijziging, Procedure medewerker uitdienst	Ja
A.8 Beheer van bedrijfsmiddelen			
A.8.1 Verantwoordelijkheid voor bedrijfsmiddelen			

A.8.1.1	Inventariseren van bedrijfsmiddelen	Bedrijfsmiddelen inventarisatie risicoanalyse, CMDB	Ja
A.8.1.2	Eigendom van bedrijfsmiddelen	Bedrijfsmiddelen inventarisatie risicoanalyse, Beleid voor aanvaardbaar gebruik	Ja
A.8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen	Beleid voor aanvaardbaar gebruik	Ja
A.8.1.4	Teruggeven van bedrijfsmiddelen	Procedure medewerker uit dienst, Beleid voor aanvaardbaar gebruik	Ja
A.8.2 Informatieclassificatie			
A.8.2.1	Classificatie van informatie	Beleid voor geclassificeerde informatie	Ja
A.8.2.2	Informatie labelen	Beleid voor geclassificeerde informatie	Ja
A.8.2.3	Behandelen bedrijfsmiddelen	Beleid voor geclassificeerde informatie	Ja
A.8.3 Behandelen van media			
A.8.3.1	Beheer van verwijderbare media	Beleid voor geclassificeerde informatie	Ja
A.8.3.2	Verwijderen van media	Beleid voor geclassificeerde informatie	Ja
A.8.3.3	Media fysiek overdragen	Beleid voor geclassificeerde informatie	Ja
A.9 Toegangsbeveiliging			
A.9.1 Bedrijfseisen voor toegangsbeveiliging			
A.9.1.1	Beleid voor toegangsbeveiliging	Gebruikers toegangsbeleid, Klant account beleid	Ja
A.9.1.2	Toegang tot netwerken en netwerkdiensten	Gebruikers toegangsbeleid, Klant account beleid	Ja
A.9.2 Beheer van toegangsrechten van gebruikers			

A.9.2.1	Registratie en afmelden van gebruikers	Procedure medewerker uit dienst, Klant account beleid	Ja
A.9.2.2	Gebruikers toegang verlenen	Gebruikers toegangsbeleid, Klant account beleid	Ja
A.9.2.3	Beheren van speciale toegangsrechten	Gebruikers toegangsbeleid,	Ja
A.9.2.4	Beheer van geheime authenticatie-informatie van gebruikers	Klant account beleid	Ja
A.9.2.5	Beoordeling van toegangsrechten van gebruikers	Gebruikers toegangsbeleid	Ja
A.9.2.6	Toegangsrechten intrekken of aanpassen	Gebruikers toegangsbeleid, Procedure medewerker uit dienst, Procedure medewerker functie wijziging	Ja
A.9.3 Verantwoordelijkheden van gebruikers			
A.9.3.1	Geheime authenticatie-informatie gebruiken	Beleid voor aanvaardbaar gebruik	Ja
A.9.4 Toegangsbeveiliging van systeem en toepassing			
A.9.4.1	Beperking toegang tot informatie	Gebruikers toegangsbeleid	Ja
A.9.4.2	Beveiligde inlogprocedures	Beleid voor aanvaardbaar gebruik	Ja
A.9.4.3	Systeem voor wachtwoordbeheer	Beleid voor aanvaardbaar gebruik.	Ja
A.9.4.4	Speciale systeemhulpmiddelen gebruiken	Beleid voor aanvaardbaar gebruik	Ja
A.9.4.5	Toegangsbeveiliging op programmabroncode	Missing Piece ontwikkelt zelf geen software	Nee
A.10 Cryptografie			
A.10.1 Cryptografische beheersmaatregelen			
A.10.1.1	Beleid inzake het gebruik van	Technisch informatiebeveiligingsbeleid	Ja

	cryptografische beheersmaatregelen		
A.10.1.2	Sleutelbeheer	Technisch informatiebeveiligingsbeleid	Ja
A.11 Fysieke beveiliging en beveiliging van de omgeving			
A11.1 Beveiligde gebieden			
A.11.1.1	Fysieke beveiligingszone	Fysieke beveiliging	Ja
A.11.1.2	Fysieke toegangsbeveiliging	Fysieke beveiliging, Bezoekersbeleid	Ja
A.11.1.3	Kantoren, ruimten en faciliteiten beveiligen	Fysieke beveiliging, Bezoekersbeleid	Ja
A.11.1.4	Beschermen tegen bedreigingen van buitenaf	Fysieke beveiliging	Ja
A.11.1.5	Werken in beveiligde gebieden	Fysieke beveiliging	Ja
A.11.1.6	Laad- en loslocatie	Fysieke beveiliging	Ja
A11.2 Apparatuur			
A.11.2.1	Plaatsing en bescherming van apparatuur	Fysieke beveiliging	Ja
A.11.2.2	Nutsvoorzieningen	Technisch informatiebeveiligingsbeleid	Ja
A.11.2.3	Beveiliging van bekabeling	Technisch informatiebeveiligingsbeleid	Ja
A.11.2.4	Onderhoud van apparatuur	Onderhoudscontracten CMDB	Ja
A.11.2.5	Verwijdering van bedrijfsmiddelen	Beleid voor aanvaardbaar gebruik	Ja
A.11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	Beleid voor aanvaardbaar gebruik	Ja
A.11.2.7	Veilig verwijderen of hergebruiken van apparatuur	Beleid voor geclassificeerde informatie	Ja

A.11.2.8	Onbeheerde gebruikersapparatuur	Beleid voor aanvaardbaar gebruik	Ja
A.11.2.9	Clear desk- en clear screen-beleid	Beleid voor aanvaardbaar gebruik	Ja

A.12 Beveiliging bedrijfsvoering

A.12.1 Bedieningsprocedures en verantwoordelijkheden

A.12.1.1	Gedocumenteerde bedieningsprocedures	Gedocumenteerde procedures kennisbank Scienta	Ja
A.12.1.2	Wijzigingsbeheer	Technisch informatiebeveiligingsbeleid	Ja
A.12.1.3	Capaciteitsbeheer	Technisch informatiebeveiligingsbeleid	Ja
A.12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen	Missing Piece ontwikkelt zelf geen software, test omgeving geregeld via Releasemanagement, omgang met test VM's via beleid voor aanvaardbaar gebruik	Nee

A.12.2 Bescherming tegen malware

A.12.2.1	Beheersmaatregelen tegen malware	Technisch informatiebeveiligingsbeleid	Ja

A.12.3 Back-up

A.12.3.1	Back-up van informatie	Technisch informatiebeveiligingsbeleid	Ja

A.12.4 Verslaglegging en monitoren

A.12.4.1	Gebeurtenissen registreren	Technisch informatiebeveiligingsbeleid	Ja
A.12.4.2	Beschermen van informatie in logbestanden	Technisch informatiebeveiligingsbeleid	Ja

A.12.4.3	Logbestanden van beheerders en operators	Technisch informatiebeveiligingsbeleid	Ja
A.12.4.4	Kloksynchronisatie	Technisch informatiebeveiligingsbeleid	Ja
A.12.5 Beheersing van operationele sotware			
A.12.5.1	Software installeren op operationele systemen	Technisch informatiebeveiligingsbeleid	Ja
A.12.6 Beheer van technische kwetsbaarheden			
A.12.6.1	Beheer van technische kwetsbaarheden	Lijst contact met speciale belangengroepen, Issue management	Ja
A.12.6.2	Beperkingen voor het installeren van software	Beleid voor aanvaardbaar gebruik	Ja
A.12.7 Overwegingen betreffende audits van informatiesystemen			
A.12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen	ISMS	Ja
A.13 Communicatiebeveiliging			
A.13.1 Beheer van netwerkbeveiliging			
A.13.1.1	Beheersmaatregelen voor netwerken	Technisch informatiebeveiligingsbeleid	Ja
A.13.1.2	Beveiliging van netwerkdiensten	Technisch informatiebeveiligingsbeleid	Ja
A.13.1.3	Scheiding in netwerken	Technisch informatiebeveiligingsbeleid	Ja
A.13.2 Informatietransport			
A.13.2.1	Beleid en procedures voor	Beleid voor geclassificeerde informatie, BYOD	Ja

	informatietransport		
A.13.2.2	Overeenkomsten over informatietransport	Bewerkersovereenkomsten met leveranciers	Ja
A.13.2.3	Elektronische berichten	Beleid voor geclassificeerde informatie	Ja
A.13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	Arbeidsovereenkomst, Bewerkersovereenkomst	Ja
A.14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen			
A.14.1 Beveiligingseisen voor informatiesystemen			
A.14.1.1	Analyse en specificatie van informatiebeveiligingseisen	Technisch informatiebeveiligingsbeleid	Ja
A.14.1.2	Toepassingen op openbare netwerken beveiligen	Technisch informatiebeveiligingsbeleid	Ja
A.14.1.3	Transacties van toepassingen beschermen	Technisch informatiebeveiligingsbeleid	Ja
A.14.2 Beveiliging in ontwikkelings- en ondersteunende processen			
A.14.2.1	Beleid voor beveiligd ontwikkelen	Missing Piece ontwikkelt zelf geen software	Nee
A.14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen	Technisch informatiebeveiligingsbeleid	Ja
A.14.2.3	Technische beoordeling van toepassingen na wijzigingen bedieningsplatform	Technisch informatiebeveiligingsbeleid	Ja
A.14.2.4	Beperkingen op wijzigingen aan softwarepakketten	Technisch informatiebeveiligingsbeleid	Ja

A.14.2.5	Principes voor de engineering van beveiligde systemen	Technisch informatiebeveiligingsbeleid	Ja
A.14.2.6	Beveiligde ontwikkelomgeving	Missing Piece ontwikkelt zelf geen software	Nee
A.14.2.7	Uitbestede ontwikkelomgeving	Missing Piece ontwikkelt zelf geen software	Nee
A.14.2.8	Testen van systeembeveiliging	Missing Piece ontwikkelt zelf geen software	Nee
A.14.2.9	Systeemacceptatietests	Technisch informatiebeveiligingsbeleid	Ja
A.14.3 Testgegevens			
A.14.3.1	Bescherming van testgegevens	Beleid voor aanvaardbaar gebruik	Ja
A.15 Leveranciersrelaties			
A.15.1 Informatiebeveiliging in leveranciersrelaties			
A.15.1.1	Informatiebeveiligingsbeleid voor leveranciersrelaties	Beveiligingsbeleid toeleveranciers	Ja
A.15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	Beveiligingsbeleid toeleveranciers	Ja
A.15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	Beveiligingsbeleid toeleveranciers	Ja
A.15.2 Beheer van dienstverlening van leveranciers			
A.15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	Beveiligingsbeleid toeleveranciers	Ja

A.15.2.2	Beheer van veranderingen in dienstverlening van leveranciers	Beveiligingsbeleid toeleveranciers	Ja
A.16 Beheer van informatiebeveiligingsincidenten			
A.16.1 Beheer van informatiebeveiligingsincidenten en -verbeteringen			
A.16.1.1	Verantwoordelijkheden en procedures	ISMS, Issuemanagement	Ja
A.16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	Incident registratie Cherwell, Issuemanagement	Ja
A.16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging	Issuemanagement, medewerkers beoordeling, nieuwsbrief klanten	Ja
A.16.1.4	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	Issuemanagement	Ja
A.16.1.5	Respons op informatiebeveiligingsincidenten	Issuemanagement, Bedrijfscontinuïteitsplan, Bedrijfsnoodplan, Crisismanagementplan	Ja
A.16.1.6	Lering uit informatiebeveiligingsincidenten	Issuemanagement	Ja
A.16.1.7	Verzamelen van bewijsmateriaal	Issuemanagement	Ja
A.17 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer			
A.17.1 Informatiebeveiligingscontinuïteit			
A.17.1.1	Informatiebeveiligingscontinuïteit plannen	Bedrijfsccontinuïteitsplan, Bedrijfsnoodplan, Crisismanagementplan	Ja
A.17.1.2	Informatiebeveiligingscontinuïteit implementeren	Bedrijfsccontinuïteitsplan, Bedrijfsnoodplan, Crisismanagementplan	Ja
A.17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	ISMS	Ja

A.17.2 Redunante componenten			
A.17.2.1	Beschikbaarheid van informatieverwerkende faciliteiten	Technisch informatiebeveiligingsbeleid	Ja
A.18 Naleving			
A.18.1 Naleving van wettelijke en contractuele eisen			
A.18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen	ISMS	Ja
A.18.1.2	Intellectuele-eigendomsrechten	ISMS, Beleid voor aanvaardbaar gebruik	Ja
A.18.1.3	Beschermen van registraties	Gebruikers toegangsbeleid, Beleid voor geclassificeerde informatie	Ja
A.18.1.4	Privacy en bescherming van persoonsgegevens	Gebruikers toegangsbeleid, Beleid voor geclassificeerde informatie, Technisch informatiebeveiligingsbeleid	Ja
A.18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	Technisch informatiebeveiligingsbeleid	Ja
A.18.2 Informatiebeveiligingsbeoordelingen			
A.18.2.1	Onafhankelijke beoordeling van informatiebeveiliging	ISMS	Ja
A.18.2.2	Naleving van beveiligingsbeleid en -normen	ISMS	Ja
A.18.2.3	Beoordeling van technische naleving	ISMS	Ja