Informatiebeveiligingsplan

Eljakim Information Technology BV
Winthontlaan 200
3526 KV Utrecht
KvK: 09096808

Versie: 2.1
11-07-2018

Algemeen Statement Informatiebeveiliging – Eljakim IT

Eljakim Information Technology BV (hierna: Eljakim IT) is een softwarebedrijf dat zoekt naar creatieve oplossingen voor technische uitdagingen, en voert projecten uit die een maatschappelijke betekenis hebben. Het hecht dan ook grote waarde aan innoverende, uitdagende projecten en verricht veel maatwerk naar de wens van klant. Hierdoor heeft het bedrijf verschillende klanten die allemaal een eigen uitdaging met zich meebrengen en veel waarde hechten aan de bescherming van de informatie die zij aan Eljakim IT toevertrouwen.

Dit informatiebeveiligingsplan beschrijft de maatregelen die Eljakim IT heeft genomen om de gegevens die zij onder haar beheer heeft te waarborgen. Deze maatregelen vinden diens grondslag onder de eisen die aan de informatiebeveiliging worden gesteld vanuit de ISO 27001:2013 (Managementsysteem voor Informatiebeveiliging) en NEN 7510:2017 (Informatiebeveiliging in de zorg), twee normen waar Eljakim IT respectievelijk sinds 6 maart 2018 en 4 juni 2018 in is gecertificeerd.

Deze maatregelen zijn genomen om:

- De veiligheid en betrouwbaarheid van data, bedrijfsinformatie en middelen te waarborgen.
- Op een effectieve en verantwoorde manier tegen verwachte en onverwachte dreigingen en/of gevaren op te treden die de veiligheid en integriteit van informatie kunnen schaden.
- Data, informatie en middelen te beschermen tegen misbruik en ongeautoriseerde toegang waardoor het bedrijf en haar klanten geschaad kunnen worden.

Verder zijn er processen en richtlijnen aanwezig voor:

- Het identificeren, analyseren en beheersen van risico's die de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatie onder het beheer van Eljakim IT kunnen schaden.
- Het continu evalueren en behandelen van deze risico's.
- Het aanpassen van het eigen informatiebeveiligingsbeleid op basis van veranderingen in technologie, de gevoeligheid van de informatie, de beschikbaarheid van middelen, en interne of externe dreigingen voor de informatiebeveiliging.

Inhoudsopgave

1. Organisatie van de informatiebeveiliging

Om haar informatiebeveiligingsbeleid uit te voeren, verbeteren en controleren heeft Eljakim IT specifieke verantwoordelijkheden onder haar eigen personeel verdeeld. Deze personeelsleden dragen gezamenlijk de verantwoordelijkheid voor het functioneren en in stand houden van haar informatiebeveiligingsbeleid, en alle zaken die daarmee verband houden.

De rol van de directie, bestaande uit de directeur en de projectleider, bestaat uit het bepalen van de strategische richting van het bedrijf en het vrijmaken van voldoende middelen voor een effectief managementsysteem voor informatiebeveiliging. Verder fungeert zij als sparringpartner voor de Information Security Officer / Data Protection Officer. Daarnaast is de directeur nauw betrokken bij het onderzoeken en analyseren van beveiligingsincidenten (wanneer deze zich voordoen).

De Information Security Officer is binnen Eljakim IT verantwoordelijk voor:

- Het opstellen en implementeren van het managementsysteem voor informatiebeveiliging.
- De periodieke uitvoering van metingen, audits en andere controles.
- Het opstellen dan wel aanpassen van nieuwe procedures.
- Het beheren van het risicomanagementproces.
- Het onderzoeken, analyseren en registreren van beveiligingsincidenten en datalekken.
- Het schrijven van beleid dat gerelateerd is aan informatiebeveiliging, evenals alle bijbehorende documentatie.
- Ervoor zorgen dat het geldende beleid wordt nageleefd door alle medewerkers.
- Het monitoren van technologische en juridische ontwikkelingen en deze met de directie bespreken indien het gevolgen heeft voor het eigen beleid.
- Het voordragen van potentiële verbeteringen van het managementsysteem aan de directie.
- Het ontwerpen, implementeren en uitvoeren van het bewustwordingsbeleid.
- Het ondersteunen van de systeembeheerder bij het monitoren van de serveractiviteiten.

De Data Protection Officer:

- Zorgt ervoor dat het bedrijf te allen tijde compliant is met geldende wet- en regelgeving op het gebied van privacy en informatiebeveiliging.
- Adviseert en informeert de directie, klanten en collega's met betrekking tot juridische vraagstukken.
- Stelt alle benodigde documentatie op ten opzichte van de Algemene Verordening Gegevensbescherming (AVG).
- Ontwikkelt en beoordeelt beleid, procedures en overeenkomsten op het gebied van privacy.
- Begeleidt het management bij het uitvoeren van Data Protection Impact Assessments (DPIA's).
- Identificeert en mitigeert privacy-gerelateerde risico's.
- Fungeert als eerste aanspreekpunt voor vragen over privacy-recht van de directie, klanten en collega's.
- Draagt zorg voor het analyseren van de privacy-impact van incidenten en datalekken, en het verwerken van de bevindingen in een rapport.
- Zorgt voor een algemene bewustwording binnen Eljakim IT op het gebied van privacyrecht en de geldende wet- en regelgeving.
- Registreert alle incidenten en datalekken, en houdt deze registraties bij.

De systeembeheerder draagt zorg voor het alledaagse functioneren van de informatiesystemen van Eljakim IT, monitort het functioneren van al haar servers, en zorgt ervoor dat alle back-ups tijdig gemaakt worden en dat deze werken voor de gevallen dat er gebruik van moet worden gemaakt. Verder houdt deze persoon alle bedrijfssystemen en -software up-to-date, en beheert de toegangsrechten van de medewerkers die binnen de organisatie werkzaam zijn.

Programmeurs en andere personeelsleden zijn, met betrekking tot de data waar zij eigenaar van zijn, zelf verantwoordelijk om de desbetreffende informatie en data te beschermen binnen het kader dat door de directie en Information Security Officer gesteld is.

2. Risico Management

Vanwege de aard van haar bedrijfswerkzaamheden heeft Eljakim IT een grote hoeveelheid gevoelige gegevens onder haar beheer, waarbij de gevolgen groot kunnen zijn indien hier niet zorgvuldig mee wordt omgegaan. Daarnaast dient de organisatie ook rekening te houden met meerdere interne en externe risico's ten opzichte van haar informatiebeveiliging en alle zaken die daaraan gerelateerd zijn.
Daarnaast erkent de organisatie dat, aangezien er constant nieuwe technologische ontwikkelingen plaatsvinden, er regelmatig nieuwe risico's zijn terwijl eerder vastgestelde risico's kunnen komen te vervallen. Deze veranderlijkheid van risico's dient dan ook in haar informatiebeveiligingsbeleid te worden opgenomen.

Om de risico's in kaart te brengen en zo goed mogelijk te beheersen hanteert Eljakim IT een risicomanagementproces waarin de risico's die voor haar zelf en haar klanten worden geïdentificeerd, geanalyseerd, en behandeld. Per risico wordt bepaald wat de

kans en impact ervan is, welke maatregelen genomen moeten worden om dit te reduceren, en hoe eventuele restrisico's kunnen worden opgevangen. De risicoanalyse wordt tenminste eens per jaar herzien en waar nodig aangepast.

3. Naleving van de gestelde richtlijnen

Alle werknemers dienen het gevoerde informatiebeveiligingsbeleid van Eljakim IT na te leven, evenals alle wettelijke verplichtingen die op hen van toepassing zijn vanuit de eigen functie-uitoefening. Iedere werknemer waarvan wordt bevonden dat die zich bezighoudt met ongeautoriseerd gebruik, verspreiden, wijzigen of vernietigen van vertrouwelijke informatie dan wel persoonsgegevens, zal aan gepaste disciplinaire maatregelen onderworpen worden. Afhankelijk van de ernst van de schending zal er onder meer worden overgegaan tot een boete, ontslag en/of juridische stappen.

4. Classificatie van informatie

Om het juiste beschermingsniveau van alle soorten informatie objectief te kunnen bepalen, classificeert Eljakim IT alle data en andere informatie onder haar beheer in drie verschillende niveaus: Publiek, Vertrouwelijk en Bedrijfsgeheim. Doordat de vertrouwelijkheid van veel persoonsgegevens vaak contextgevoelig is, is bij het classificeren van deze informatie rekening gehouden met de aard van de gegevens, wettelijke eisen en verplichtingen, en geldend intern beleid. Door hierbij de juiste afwegingen te maken wordt er op verantwoorde wijze gezorgd voor een passend beschermingsniveau.

Alle classificaties zijn gebaseerd op het BIV-model: (B)eschikbaarheid, (I)ntegriteit en (V)ertrouwelijkheid. Deze punten houden respectievelijk in dat (1) informatie toegankelijk moet zijn voor de personen wanneer zij dit nodig hebben, (2) ongeautoriseerde aanpassing of vernietiging van informatie voorkomen moet worden, en (3) gegarandeerd moet kunnen worden dat de informatie enkel leesbaar is voor degenen die daarvoor geautoriseerd zijn.

4.1 Publieke informatie

Publieke informatie is niet vertrouwelijk en kan zonder nadelige gevolgen toegankelijk worden gemaakt voor het algemene publiek. Inzage is daarmee niet voorbehouden aan specifieke groepen, en beperkte beschikbaarheid hiervan naar aanleiding van bijvoorbeeld downtime is acceptabel. Hierbij kan gedacht worden aan de informatie die wordt vermeld op de website van Eljakim IT, de al publieke contactgegevens van klanten en openbare aanbestedingsdocumenten.

4.2 Vertrouwelijke informatie

Informatie van dit niveau is beperkt tot degenen die het nodig hebben voor het vervullen van de eigen werkzaamheden. Toegang door onbevoegden kan de operationele effectiviteit van de organisatie schaden, evenals het vertrouwen van de klanten. Deze informatie dient altijd goed te worden beschermd tegen onrechtmatige wijziging, vernietiging of andere onrechtmatige verrichtingen. Voorbeelden van informatie die in deze categorie vallen zijn algemene en bijzondere persoonsgegevens, backups, logbestanden, intellectueel eigendom en broncode.

4.3 Bedrijfsgeheime informatie

Deze categorie van informatie is van cruciaal belang voor het operationeel en financieel functioneren van de organisatie. Onbevoegde inzage, publicatie of wijziging dan wel vernietiging van deze informatie leidt tot grote schade voor de organisatie, haar personeel en/of haar klanten. Personeelsdossiers, financiële bedrijfsinformatie en de salarisadministratie zijn voorbeelden van informatie die deze classificatie kennen.

Eljakim IT voert regelmatig controles uit om ervoor te zorgen dat alle medewerkers op zorgvuldige wijze met informatie omgaan en te voorkomen dat informatie door onbevoegden, zowel intern als extern, wordt ingezien.

5. Omgang met vertrouwelijke informatie en geheimhouding

Om ervoor te zorgen dat er voor het personeel een duidelijk kader is rondom de omgang met en bescherming van informatie, en te voorkomen dat informatie met onbevoegden wordt gedeeld, hanteert Eljakim IT voor elk lid van haar organisatie een geheimhoudingsplicht. Deze plicht heeft zij in alle arbeidsovereenkomsten opgenomen in een aparte clausule.

Daarnaast wordt binnen de organisatie, ten behoeve van de informatiebeveiliging, een addendum op de arbeidsovereenkomst gehanteerd waarin de rechten en plichten van de medewerkers uiteen worden gezet. Dit addendum dient bij de indiensttreding door elke medewerker te worden getekend.

De geheimhoudingsplicht geldt voor onbepaalde tijd, en betreft daarom zowel de periode gedurende als na het dienstverband. Deze is van toepassing op alle kennis die de medewerker binnen Eljakim IT opdoet, los van het feit of deze kennis vanuit de functie noodzakelijk is. Bij overtreding van de geheimhoudingsplicht volgt een boete en mogelijk ontslag op staande voet.

Zodra Eljakim IT constateert dat er een redelijke kans is dat de geheimhouding van de gegevens is geschaad wordt direct contact opgenomen met de klant. Verder wordt er van alle betrokken servers direct een volledige back-up van de logbestanden veiliggesteld die bij later onderzoek gebruikt kan worden.

Indien het onduidelijk is hoe verstrekkend de toegang tot gegevens is geweest kan in overleg met de klant worden besloten om tot een of meerdere van de volgende maatregelen over te gaan:

- De servers worden losgekoppeld van het netwerk.
- De applicatie wordt volledig stilgelegd voor gebruikers.
- De toegang tot de applicatie wordt geblokkeerd voor gebruikers die vanaf een onbekend IP-adres komen of toegang proberen te verkrijgen.

Verder maakt Eljakim IT ook gebruik van een externe partij (‘arbeidscoach’) die periodiek alle medewerkers individueel spreekt om zo vroeg mogelijk te signaleren indien er problemen zijn in de persoonlijke sfeer die van invloed zouden kunnen zijn op het geheimhouden van de gegevens.

Tot slot geldt voor alle medewerkers van Eljakim IT dat er binnen een maand na indiensttreding een Verklaring Omtrent het Gedrag (VOG) overlegd moet worden. Het screeningsprofiel bij de VOG is:

- Bevoegdheid hebben tot het raadplegen en/of bewerken van systemen (11);
- Met gevoelige/vertrouwelijke informatie omgaan (12);
- Kennis dragen van veiligheidssystemen, controlemechanismen en verificatieprocessen (13).

Alleen medewerkers van Eljakim IT die voor de uitvoer van hun functie toegang nodig hebben tot de applicatie zijn geautoriseerd om persoonsgegevens in te zien.

6. Bewustwording van het personeel

Ter bevordering van een effectieve informatiebeveiliging, evenals een verantwoorde omgang met vertrouwelijke informatie door alle leden van de organisatie, voert Eljakim IT een actief bewustwordingsbeleid. Zo wordt er maandelijks een nieuwsbrief via de interne mail rondgestuurd, en worden er periodieke gesprekken met de medewerkers gevoerd over de inhoud ervan.

De topics, en daarmee de inhoud van het bewustwordingsbeleid, wordt zoveel mogelijk gebaseerd op recente ontwikkelingen binnen het domein van cybersecurity en/of de informatiebehoeften van de medewerkers. De planning van de topics wordt per periode van 6 maanden geschreven en uitgevoerd, zodat er altijd een actueel onderwerp wordt behandeld.

7. Identiteits- en Toegangsbeheer

Eljakim IT heeft meerdere maatregelen genomen om de eigen organisatie en haar klanten ervan te kunnen verzekeren dat medewerkers enkel bij de data en informatie kunnen komen waarvoor zij daadwerkelijk geautoriseerd zijn, en daarbij alleen de benodigde rechten hebben zodat deze personen naar behoren kunnen functioneren.

Zo zijn er met betrekking tot de logische toegang tot applicaties, netwerken, code en documentatie (onder meer) de volgende maatregelen getroffen:

- Voor de eigen informatiesystemen wordt altijd gebruik gemaakt van een gebruikersnaam en wachtwoord.
- De database servers zijn niet rechtstreeks van buitenaf benaderbaar.
- Alle informatie die wordt uitgewisseld tussen systemen onderling wordt versleuteld verzonden. Dit betreft SSH-tunnels dan wel HTTPS-verbindingen.
- Voor alle sleutels geldt dat deze minimaal 2048-bits beveiliging verzorgen.
- Voor applicaties waarin persoonlijke gezondheidsinformatie wordt verwerkt wordt twee-factor authenticatie gehanteerd. Daarnaast kan twee-factor authenticatie ook ingebouwd worden voor andere applicaties indien de klant dat wenst.
- Toegang tot de back-ups, logbestanden en andere elementen van systeembeheer is beperkt tot de medewerkers die zich daarmee vanuit hun functie bezigen.
- Alle ontwikkel-, test- en productieomgevingen zijn te allen tijde van elkaar gescheiden.
- Eljakim IT maakt gebruik van meerdere gescheiden netwerken.
- Back-ups worden versleuteld opgeslagen op aparte servers.

- Alle activiteiten op de databaseservers van Eljakim IT worden gelogd door middel van het rsyslog-protocol.
- Alle werkstations en laptops worden beschermd door anti-virus software.

Met het oog op de fysieke beveiliging van alle data en informatie zijn de volgende maatregelen getroffen:

- De primaire servers staan in een beveiligd co-locatie centrum in Amsterdam. De beveiliging van dit center wordt geregeld door KPN Telecom. Een deel van de servers staat in een uitwijkcentrum waarvoor dezelfde maatregelen gelden.
- Alle servers zijn eigendom van Eljakim IT. Er worden geen gegevens in 'de cloud' opgeslagen.
- Toegang tot het colocenter kan alleen door vooraf aangemelde en geautoriseerde personen die beschikken over een speciale pas en legitimatie. In het colocenter zijn alle deuren beveiligd zodat alleen geautoriseerde personen toegang hebben tot ruimtes. Slechts een beperkt aantal medewerkers van Eljakim IT heeft een pas waarmee het pand van KPN betreden kan worden.
- De servers van Eljakim IT hangen in een apart afgesloten kast waarvan de code alleen bij bevoegde medewerkers van Eljakim IT bekend is. Op de kast staan permanent camera's gericht zodat altijd te achterhalen is welke personen in de buurt van de kast zijn gekomen.

Voor de gegevens die zich binnen het kantoorpand van Eljakim IT bevinden is er sprake van de volgende beveiligingsmaatregelen:

- Toegang tot het bedrijfsverzamelgebouw wordt bewaakt door een centrale receptie die met camera's is beveiligd.
- Toegang tot de vleugels van Eljakim IT is alleen mogelijk na het verwijderen van het individuele alarm van deze gangen en het fysiek van het slot draaien van de sloten. Hiernaast zijn overdag de deuren permanent beveiligd door een elektronisch slot. De toegangscode hiervoor wordt periodiek gewijzigd.
- Op de voordeuren van de gangen staan camera's gericht.
- Eljakim IT heeft enkele ruimten aangemerkt als "beveiligde zone". Dit houdt in dat toegang tot deze ruimten beperkt wordt tot degenen die daarvoor geautoriseerd zijn. Specifiek gaat het hier om de kamer van de directie, de office manager en de serverruimte.
- De lokale servers zijn in een aparte afgesloten ruimte geplaatst. Deze ruimte is met een apart geschakeld alarm en deurslot beveiligd. Slechts een beperkt aantal medewerkers kan dit aparte alarm uitschakelen.
- Medewerkers worden getraind om geen vertrouwelijke informatie af te drukken. Indien dit toch noodzakelijk is, is een shredder aanwezig voor de vernietiging van het papier.
- In meerdere ruimten, waaronder de serverruimte, zijn rookmelders geïnstalleerd.
- De fysieke omgeving van het bedrijfsverzamelgebouw is beveiligd met camera's, een hekwerk en een alarmsysteem.
- Gegevensdragers, zoals laptops en tablets, worden op een beveiligde ruimte opgeslagen zolang deze niet in gebruik zijn.
- Vertegenwoordigers van klanten, derden en leveranciers worden altijd begeleid door ten minste één medewerker van Eljakim IT zolang deze zich in het kantoorpand van de organisatie bevinden.

Tot slot worden de benodigde rechten en accounts altijd afgegeven door de systeembeheerder, en deze worden periodiek gecontroleerd. De medewerkers van Eljakim IT kunnen vanaf afstand met de servers verbinding maken via VPN, en medewerkers met "privileged access" worden tot een absoluut minimum beperkt.

8. Netwerkbeheer, -beveiliging & monitoring

Eljakim IT beheert haar eigen netwerken – hier is geen externe partij bij betrokken. Via speciale monitoring software worden de servers 24-uur per dag gemonitort, waarbij onder meer de servercapaciteit, -activiteiten en het algehele functioneren ervan worden gecontroleerd. Indien er aanwijzingen bestaan van afwijkend functioneren wordt er, afhankelijk van het issue, direct actie op ondernomen. Daarnaast wordt elke vijf minuten de verbinding met de servers in Amsterdam automatisch opgevraagd om er zeker van te zijn dat de servers in goede gezondheid verkeren.

Er worden afzonderlijke procedures gehanteerd om grootschalige, kritieke of anderzijds risicovolle wijzigingen aan de eigen systemen te beheersen. Onderhoud aan de eigen systemen, waaronder software- en systeemupdates, wordt altijd verricht door gekwalificeerde personen en aan de klanten gecommuniceerd die hier mogelijke nadelige gevolgen van kunnen ondervinden.

Verder maakt Eljakim IT iedere nacht automatisch een back-up van alle gegevens op de dataservers naar een andere server. Een kopie van de back-up blijft altijd achter op de server zelf. Hierdoor kan in geval van gebruikersfouten snel teruggegrepen worden naar de back-up van 'afgelopen nacht'. Indien gewenst is het ook mogelijk om elke nacht een automatische back-up te maken naar een derde locatie die door de klant aangewezen wordt. Hierdoor wordt gegarandeerd dat de klant altijd een kopie van de eigen gegevens in huis heeft.

In geval van calamiteiten worden back-upwerkzaamheden binnen 4 uur uitgevoerd. Het terugplaatsen van de back-up wordt wekelijks getest en geëvalueerd.

9. Bescherming van Bedrijfsmiddelen

Alle bedrijfsmiddelen worden enkel door de systeembeheerder (laptops, werkstations) dan wel de Office Manager (sleutels en druppel tot het pand) afgegeven, en zijn alleen bedoeld voor intern gebruik.
Alle gegevensdragers worden in een beveiligde ruimte opgeslagen zolang deze niet worden gebruikt.

Laptops en PC's die gebruik maken van de informatiesystemen van Eljakim IT dienen altijd up-to-date te zijn, een anti-virus programma te bevatten en beveiligd te zijn met gebruikersnaam en wachtwoord.

Voor alle medewerkers wordt een Clear Desk & Clear Screen Policy gehanteerd.

10. Verwijdering van data

Voor alle soorten gegevensdragers en media, waaronder hardcopy en elektronische documenten, zijn specifieke regels en procedures opgesteld met betrekking tot het veilig verwijderen van informatie op media. Deze zijn vastgelegd naar het SOP-model (Standard Operating Procedure) om ervoor te zorgen dat de procedure zo goed mogelijk wordt geborgd.

Wanneer gegevensdragers of gegevensdragende componenten geformatteerd en/of vernietigd worden, wordt de daadwerkelijke uitvoering daarvan in een apart logboek vastgelegd.

Bij de verwijdering van media die grote hoeveelheden en/of vertrouwelijke informatie bevatten wordt de goedkeuring van de directie gevraagd voordat er tot daadwerkelijke vernietiging over wordt gegaan.

Bij defecte of oude hardware worden alle gegevensdragende componenten verwijderd, zoals de harde schijven, evenals de geheugenmodules. De hardware wordt daarna als standaard afval afgevoerd. De verwijderde componenten worden op een beveiligde plaats opgeslagen binnen het kantoorpand van Eljakim IT.

Hardcopy documenten worden bij vernietiging door een papierversnipperaar gehaald, waarna de resten worden afgevoerd.

11. Leveranciers en derden

Met uitzondering van de partij die het datacenter beheert waarin de servers van Eljakim IT staan, heeft de organisatie geen verbanden met andere leveranciers of derden die zich direct verhouden tot de eigen informatiebeveiliging. De beheerder van het datacenter stuurt de organisatie jaarlijks een ISAE 3000 Type II-rapport, waarmee wordt aangetoond dat deze partij voldoet aan de eisen die Eljakim IT aan haar stelt rondom de bescherming van haar servers.

Hardware die vanuit de vaste leveranciers wordt besteld en aangeleverd, wordt altijd gecontroleerd en getest.

Geen enkele leverancier heeft directe toegang tot de informatie of kantoorruimte van Eljakim IT.

Het functioneren van de leveranciers wordt tenminste elke 6 maanden besproken tijdens de directiebeoordeling. Indien hierover een negatief oordeel wordt gegeven, zal de organisatie de geleverde diensten met de desbetreffende leverancier bespreken, dan wel mogelijkheden onderzoeken om naar een betere leverancier over te stappen.

12. Beveiligingsincidenten en Datalekken

Om ervoor te zorgen dat eventuele beveiligingsincidenten en datalekken op een effectieve en verantwoorde wijze worden afgehandeld heeft Eljakim IT verschillende procedures opgezet en geïmplementeerd. Hierbij is onder meer een Respons Team aangesteld, dat bepaalt wat als een incident of datalek beschouwd dient te worden, wie welke verantwoordelijkheden heeft, welke stappen dienen te worden gezet tijdens een dergelijk voorval en welke informatie verzameld moet worden voor een juiste opvang en afhandeling. Aansluitend hierop bestaat er tevens een aparte procedure voor het verzamelen, beschermen en bewaren van bewijsmateriaal.

Alle beveiligingsincidenten en datalekken worden in een apart overzicht vastgelegd. Specifiek wordt hier (niet noodzakelijk in de getoonde volgorde) de volgende informatie in vastgelegd:

- Datum van het voordoen van het incident.
- Datum waarop het incident is opgelost.
- De desbetreffende klant.

- Samenvatting van het incident, inclusief de aard.
- De oorzaak van het incident.
- Aantal getroffen personen.
- De genomen dan wel te nemen correctieve maatregelen.
- Het soort gegevens dat bij het incident betrokken is.
- Welke mogelijke nadelige gevolgen kunnen worden ondervonden door de betrokkenen.
- Hoe de informatie is beveiligd tegen onbevoegde inzage.

Per beveiligingsincident en/of datalek wordt tevens een onderzoek uitgevoerd waarvan de bevindingen in een afzonderlijk rapport worden vastgelegd. Hierbij wordt per geval eveneens een analyse verricht van de (potentiële) impact op de eigen informatiesystemen dan wel op de privacy van alle personen die bij het incident betrokken zijn. Dit laatste geldt in het bijzonder bij datalekken.

Beveiligingsincidenten en datalekken die betrekking hebben op de dienstverlening aan de klanten van Eljakim IT worden altijd binnen een periode van 24 uur gemeld. Onderzoek naar de oorzaken en het vastleggen van de bevindingen zal plaatsvinden binnen 72 uur, waarna er (indien noodzakelijk) in overleg wordt getreden met de desbetreffende klant.
Mocht er sprake zijn van een datalek waarbij Eljakim IT van oordeel is dat er een melding gemaakt moet worden bij de Autoriteit Persoonsgegevens op grond van de Meldplicht Datalekken, zal zij de klant hierover zo spoedig mogelijk informeren.

13. Bedrijfscontinuïteitsbeheer

13.1 Organisatorische maatregelen.

Risico's met betrekking tot de continuïteit van de door Eljakim IT geleverde diensten zijn geïdentificeerd in drie categorieën: Externe risico's, voorzieningsrisico's en IT-risico's. De risico's in elke categorie zijn geanalyseerd en daaropvolgend zijn de benodigde maatregelen genomen om de kans van voordoen en de impact ervan waar mogelijk te reduceren. Hierbij is ook rekening gehouden met de rollen die centrale leveranciers hierbij spelen, zoals de beheerder van het datacenter en de eigenaar van het bedrijfsverzamelpand waar het kantoor van Eljakim IT gevestigd is.

Er is een communicatieplan aanwezig voor wanneer calamiteiten zich voordoen. Daarnaast bestaat er een los escalatieplan waarin de voorwaarden gesteld zijn voor wanneer er tot evacuatie over dient te worden gegaan, en zijn er verschillende crisismanagementplannen aanwezig die het handelen van alle leden van Eljakim IT voorschrijven tijdens bijvoorbeeld een brand.

Continuïteitsplannen worden jaarlijks getest en geëvalueerd. De resultaten hiervan worden in een apart document vastgelegd, en aan de hand daarvan wordt bestaand beleid en de daarbij behorende procedures verbeterd.

13.2 Technische maatregelen

Om de continuïteit en stabiliteit van het systeem en netwerk te waarborgen, gebruikt Eljakim IT meerdere servers voor gebruik en back-ups. Het datacentrum in Amsterdam, waar de primaire servers zich bevinden, beschikt over de volgende faciliteiten die de continuïteit en stabiliteit van de infrastructuur waarborgen:

- Meerdere redundante netwerkverbindingen met alle grote internetproviders uit Nederland.
- Redundante stroomvoorzieningen indien de stroom onverwachts uitvalt.

De servers in Amsterdam vormen de centrale servers waarop applicaties draaien. De andere serverlocaties fungeren als back-up en noodvoorzieningen. Op de centrale locatie wordt gebruik gemaakt van een firewall die alle internet verkeer van en naar de server controleren. Op het moment van schrijven van dit document wordt gebruik gemaakt van Fortigate 200D firewalls.

Omdat er meerdere omgevingen gehost worden op het netwerk van Eljakim IT, wordt er gebruik gemaakt van meerdere servers. De databases staan op de verschillende databaseservers, die niet rechtstreeks benaderbaar zijn vanaf het internet. Deze servers kunnen niet automatisch worden overgenomen door een andere server.

Alle databases houden een transactielog bij waarin van seconde tot seconde alle transacties op de databases worden opgeslagen. De transactielog wordt gedurende minimaal 5 dagen en maximaal 14 dagen bewaard.

Van alle databases wordt elke nacht een back-up gemaakt. Deze back-up wordt minimaal 14 dagen bewaard. De exacte termijn is afhankelijk van individuele afspraken die met elke klant worden gemaakt.

14. Compliance, Audits en Metingen

Eljakim IT voert periodiek audits en metingen uit om het functioneren van het eigen informatiebeveiligingsbeleid te kunnen beoordelen.

Om zowel de naleving van het geldende beleid als ook de effectiviteit ervan te controleren en beheersen, voert de Information Security Officer elke 6 maanden een interne audit uit. Hierbij wordt er naar de geïmplementeerde beveiligingsmaatregelen gekeken of deze nog steeds voldoen aan het normenkader zoals deze uiteen is gezet in de ISO 27001:2013 en NEN 7510:2017-normen. Alle bevindingen, evenals de reikwijdte van de audit en de geauditeerde risico's, worden in een afzonderlijk rapport vastgelegd en bewaard. Indien uit deze audit naar voren komt dat de bestaande maatregelen niet toereikend zijn, worden de benodigde verbeteringen of andere aanpassingen bepaald en vervolgens doorgevoerd. Op een later tijdstip wordt de effectiviteit van de genomen maatregelen beoordeeld.

Het uitvoeren van de metingen heeft meerdere doelen, afhankelijk van het soort meting dat plaatsvindt. Het kan hier namelijk gaan om een meting van de bestaande geïdentificeerde risico's, maar ook of het geldende Clear Desk & Clear Screen Policy voldoende door het eigen personeel wordt gevolgd. Een ander voorbeeld van een meting die periodiek plaatsvindt, is die van de effectiviteit van het bewustwordingsbeleid, en of de kennis onder het eigen personeel inderdaad groeiende is.

15. Continue Verbetering en Evaluaties

Vanuit het normenkader van de ISO 27001:2013 en NEN 7510:2017 draagt Eljakim IT er zorg voor dat het eigen informatiebeveiligingsbeleid, inclusief de technische aspecten ervan, zoveel mogelijk geëvalueerd en waar mogelijk verbeterd wordt. Aan de hand van elke directiebeoordeling, meting, audit en overige controles worden de benodigde verbetermaatregelen bepaald en door de Information Security Officer vastgelegd. Wanneer nodig worden deze gezamenlijk met de directie en andere partijen binnen de organisatie doorgevoerd.

16. Relevante Wet- en Regelgeving

Binnen het kader van de informatiebeveiliging worden in ieder geval de volgende wetten genoemd:

-	Algemene Verordening Gegevensbescherming	(AVG)	Vanaf 25-05-2018
-	Meldplicht Datalekken		Vanaf 01-01-2016
-	Wet Basisregistratie Personen	(Wet BRP)	Vanaf 03-07-2013

Eljakim IT zal de gegevens die zij onder haar beheer krijgt van een verantwoordelijke, in overeenstemming met de bovengenoemde wetten, altijd op een behoorlijke en zorgvuldige wijze verwerken. Om haar te helpen om te allen tijde compliant te zijn met geldende wet- en regelgeving, wordt Eljakim IT rondom ICT-recht geadviseerd door een speciaal kenniscentrum.

16.1 Functionaris voor de Gegevensbescherming

Sinds November 2017 heeft Eljakim IT intern een Functionaris voor de Gegevensbescherming (ook wel Data Protection Officer genoemd) aangesteld, die tot taak heeft om naleving van de AVG binnen de organisatie te waarborgen. Verder functioneert deze persoon als het aanspreekpunt voor privacy vraagstukken, levert hij of zij advies aan de medewerkers en klanten van de organisatie, verzorgt de nodige documentatie (zoals het verwerkingsregister) en assisteert de directie bij het ontwikkelen van benodigde interne regelingen en processen ten opzichte van privacy.

17. Revisiegeschiedenis

Datum	Versie	Opmerking	Door
25-02-2014	1.0	Eerste versie.	E. Schrijvers
31-03-2014	1.1	Verduidelijkingen backupprocedure.	E. Schrijvers
05-02-2015	1.2	Plaatjes vergroot op verzoek van een klant.	E. Schrijvers
10-02-2015	1.3	• Actief aangegeven dat het onveilige protocol SSL niet meer ondersteund wordt, en in plaats daarvan TLS wordt gebruikt. • Backupprocedure aangepast aan wat momenteel de werkelijkheid is (backups naar Utrecht worden niet meer gemaakt).	E. Schrijvers
30-09-2015	1.4	Inleiding volledig herschreven.	E. Schrijvers
26-10-2015	1.5	Alle applicatiespecifieke zaken zijn verwijderd.	D. Blokhuis
10-02-2018	1.6	• Document geüpdatet naar aanleiding van het ISO 27001:2013 en NEN 7510:2017 traject. • Inleiding uitgebreid. • Vermeldingen van de Wbp aangevuld met dan wel vervangen door de AVG. • Compliance met wet- en regelgeving toegevoegd.	S. van der Velden
01-03-2018	1.7	Inleiding uitgebreid met informatie over certificering in de ISO 27001:2013 en NEN 7510:2017 normen (cursieve tekst).	S. van der Velden
15-06-2018	2.0	Nieuwe versie van het Informatiebeveiligingsplan opgesteld die beter is aangesloten op de recente certificering van Eljakim IT BV in de ISO 27001:2013 en NEN 7510:2017 -normen. De oude versie is hierdoor vervallen.	S. van der Velden
11-07-2018	2.1	Enkele taalfouten hersteld en de inhoudsopgave gecorrigeerd.	S. van der Velden S. Nagelhout