jeugdbescherming voor vluchtelingen

Versie 0.4 25-08-2025

Informatiebeveiliging

Beleidsdocument

Voor je ligt het informatiebeleid van Nidos

Informatiebeveiliging is veel meer dan alleen een kwestie van ICT

INHOUD

Versie historie

Nr	Datum	Auteur(s)	Status	Opmerking
0.1	17-03-2025	Jeroen Rams Marco Ebbers	Initiële versie	
0.2	09-05-2025	Jeroen Rams		Bijgewerkt nav opmerkingen Hubert Jan
0.3	06-08-2025	Jeroen Rams		Bijgewerkt na input Bart en Peter
0.4	25-08-2025	Jeroen Rams		Bijgewerkt na review

1 MANAGEMENT-SAMENVATTING

Voor je ligt het informatieveiligheidsbeleid van Nidos. Het beschrijft het te voeren beveiligingsbeleid binnen Nidos. Hieraan gerelateerd zijn de meer gedetailleerde procedures, maatregelen en richtlijnen die voor het uitvoeren van het beleid van toepassing zijn. Dit beleid beschrijft de richting en ondersteuning zoals deze door de directie van Nidos is bepaald voor informatiebeveiliging in overeenstemming met de bedrijfsmatige eisen voor effectieve en efficiënte bedrijfsprocessen, betrouwbare financiële verslaggeving en naleving van wet- en regelgeving. De directie van Nidos stelt daarom het volgende vast:

- Het informatiebeveiligingsnormenkader NEN7510 wordt beschouwd als uitgangspunt voor het ontwikkelen van richtlijnen die specifiek op de organisatie zijn toegesneden. Op sommige punten kan -gemotiveerd - worden afgeweken van de voorgestelde maatregelen en/of zijn er wellicht aanvullende maatregelen nodig.
- Het uit te dragen informatiebeveiligingsbeleid is vastgelegd in dit document.
- Alle medewerkers van Nidos, ZZP'ers en andere externe medewerkers handelen overeenkomstig en passend bij dit Informatiebeveiligingsbeleid.
- Alle medewerkers zijn gehouden gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht.
- Nidos bevordert actief het beveiligingsbewustzijn van haar medewerkers.
- Indien nodig zijn onderdelen van dit beleid uitgewerkt in concrete richtlijnen en maatregelen, toegesneden op de taken en verantwoordelijkheden van de betrokken medewerkers.
- Periodiek beoordeelt de organisatie of voor specifieke gegevens of de informatiesystemen aanvullende maatregelen noodzakelijk zijn.
- De naleving van genomen maatregelen wordt periodiek getoetst, passend bij het risiconiveau van de gegevens waarop de maatregelen van toepassing zijn. De frequentie van deze beoordeling is opgenomen in de auditplanning.
- Het beleid wordt eens per drie jaar herzien en indien nodig tussentijds aangepast.

De directie van Nidos

2 INFORMATIE-BEVEILIGINGS DOELSTELLING

De informatiebeveiligingsdoelstelling is afgeleid van de missie uit het meerjarenbeleidsplan van Nidos en dan het strategische thema “Naar een professionele organisatie”.
Op basis van deze missie is het mogelijk een (strategische) doelstelling voor Informatiebeveiliging te definiëren. Nidos wil met het informatiebeveiligingsbeleid de volgende doelstelling realiseren:

Het beheersen van de informatiebeveiliging binnen Nidos zodat zowel voor de jongeren, opvanggezinnen, contractpartners als medewerkers de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening wordt geborgd.

Dit wordt bereikt door, op basis van een uitgevoerde risicoanalyse, een set van maatregelen vast te stellen en te toetsen tegen de NEN7510. Om de implementatie van informatiebeveiliging in de organisatie te initiëren en te beheersen is een Information Security Managementsysteem (afgekort ISMS) ingericht. Het beleid is vastgesteld door de directie, met vaststelling van de rollen, de coördinatie en de uiteindelijke beoordeling van de implementatie van het beleid.

Deze strategische doelstelling wordt later in dit document verder uitgewerkt in operationele en meetbare doelstellingen.

3 DOEL VAN HET BELEIDSDOCUMENT

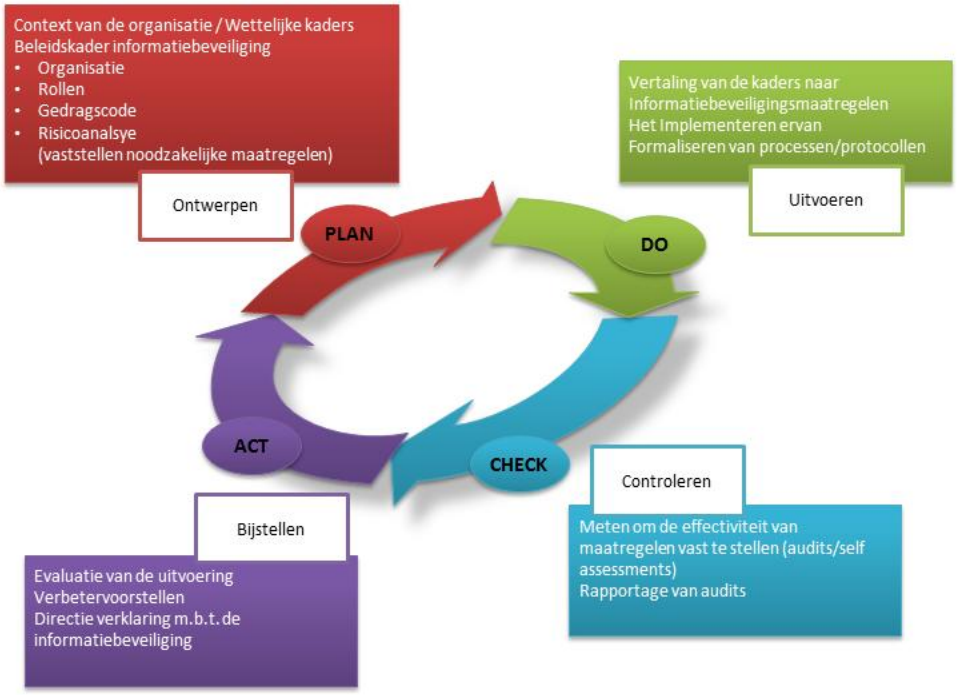
De in dit beleidsdocument beschreven uitgangspunten zijn er op gericht Nidos de informatie beveiligingsrisico's voor haar bedrijfsvoering te kennen en beheersen.
Het beleid is bedoeld voor alle medewerkers (inclusief ZZP'ers, uitzendkrachten).
Daarnaast wordt het beleid beschikbaar gesteld aan die organisaties waarmee Nidos een overeenkomst heeft en aan externe organisaties die namens NIdos persoonsgegevens verwerken.
Het beleid wordt door Nidos beschikbaar gesteld aan alle medewerkers van Nidos en belanghebbenden en wordt verstrekt aan externe belanghebbenden indien hiertoe aanleiding bestaat.
Bij het opzetten van dit beleid is aansluiting gezocht met de geldende internationale normen op het gebied van informatiebeveiliging. Hierdoor is Nidos in staat om bewuste keuzes te maken en passende maatregelen te nemen. Op deze wijze worden de risico's met betrekking tot haar dienstverlening beheerst.
Dit beleid beschrijft het te voeren beveiligingsbeleid en geeft richting aan de meer gedetailleerde maatregelen en richtlijnen die van toepassing zijn binnen Nidos.

4 REIKWIJDTE

Het beleid heeft betrekking op alle door Nidos gebruikte gegevens en hieraan gerelateerde informatiesystemen, de fysieke aspecten met betrekking tot deze gegevens, welke zijn aangesloten op het netwerk van Nidos (bijvoorbeeld laptops van medewerkers) én op software in eigendom van Nidos, via licentie verkregen of afgenomen via een SaaS (Software as a Service) dienst.
De gehanteerde norm is NEN 7510.

4.1 BEHEERSING VAN INFORMATIEBEVEILIGING BINNEN NIDOS

De informatiebeveiliging van Nidos is een cyclisch proces. Via de zogenaamde Plan-Do-Check-Act cyclus wordt gestreefd om de informatiebeveiliging steeds naar een hoger niveau te krijgen. Hiervoor heeft Nidos een management systeem ingericht. De tussentijdse controles of constateringen kunnen aanleiding zijn bij te sturen op de bestaande maatregelen.



De cyclus wordt jaarlijks minimaal één keer doorlopen.

5 CONTEXT VAN DE ORGANISATIE

Nidos voert als gecertificeerde instelling de voogdij uit voor alleenstaande minderjarige vreemdelingen (ongeacht het verblijf). Ook voert Nidos op dezelfde grondde ondertoezichtstelling voor kinderen voor wie een asielaanvraag is ingediend én die in verband daarmee verblijven in een opvangcentrum van het COA.
Deze jeugdbeschermingsmaatregelen worden uitgevoerd door professionals die met respect voor de culturele achtergrond van de jongere, vanuit betrokkenheid en met specifieke deskundigheid het belang van de individuele jongere centraal stellen. De professional voert de regie over de ontwikkeling naar zelfredzaamheid van de jongere en grijpt in wanneer die ontwikkeling op enigerlei wijze dreigt te stagneren.
Nidos is een organisatie die snel moet kunnen inspelen op veranderingen. In de afgelopen jaren zijn we flink gegroeid, onder andere door een hoge instroom van jongeren, maar die instroom is nu teruggelopen.

Het “typische” IT landschap van Nidos bestaat uit een Virtual Private Cloud waarbinnen verschillende servers draaien, Microsoft Office/ Office 365 omgeving en (SaaS) applicaties in de Cloud. Het aantal gebruikte applicaties is vrij overzichtelijk.
Tussen Nidos en andere instanties/bedrijven kunnen door middel van koppelingen gegevens uitgewisseld worden, bijvoorbeeld ten behoeve van diensten die vanuit Nidos aan andere bedrijven worden geleverd, financieel af te kunnen handelen.
Binnen Nidos wordt IT ondersteund door de IM/ICT afdeling, een deel van de dienstverlening is ondergebracht bij externe IT-leveranciers.

6 ORGANISATIE VAN DE INFORMATIE-BEVEILIGING

In onderstaande paragrafen wordt ingegaan op de verschillende rollen binnen Nidos in het kader van informatiebeveiliging. Omdat er een overlap bestaat tussen informatiebeveiliging en (data) privacy, wordt in onderstaande ingegaan op beide onderwerpen.
De verschillende beleidsmatige aandachtsgebieden zijn verdeeld binnen de organisatie.

6.1 INBEDDING VAN INFORMATIEBEVEILIGING & PRIVACY OP STRATEGISCH NIVEAU

6.1.1 IM/ICT

Informatiebeveiliging en Privacy zijn zo sterk als de zwakste schakel. Indien binnen de organisatie één onderdeel niet “in control” is op het gebied van informatiebeveiliging en privacy, kan dat een negatieve impact hebben op de andere organisatieonderdelen. Het is daarom van belang dat beide onderwerpen centraal worden aangestuurd. Om deze reden is de IM/ICT richtinggevend voor informatiebeveiliging en privacy binnen de organisatie.

6.2 CENTRALE FUNCTIES BIJ NIDOS

6.2.1 Risk & Compliance

Onderdeel van de Governance is dat aan alle soorten risico’s en hun onderlinge verwevenheid passende aandacht geschonken wordt. Het is om die reden dat bij Nidos op strategisch niveau diverse risico categorieën bestuurd worden. Hieronder vallen frauderisico en financiële
risico’s, risico’s omtrent informatiebeveiliging en privacy. De verschillende risico categorieën worden in samenhang gemanaged door de afdeling planning en control.

6.2.2 Portefeuillehouder Informatiebeveiliging

De Bestuurder is eindverantwoordelijk voor alle activiteiten binnen Nidos en dus ook voor informatiebeveiliging. Binnen het directieteam heeft de directeur bedrijfsvoering de portefeuille informatiebeveiliging toegewezen aan manager IM&ICT. De portefeuillehouder is vanuit het bestuur verantwoordelijk voor de uitvoering van het informatiebeveiligingsbeleid.
De bestuursverantwoordelijkheid voor informatiebeveiliging omvat:

- het vaststellen van dit informatiebeveiligingsbeleid;
- het toezien op de naleving van het informatiebeveiligingsbeleid door de organisatieonderdelen;
- het evalueren van de toepassing en werking van het informatiebeveiligingsbeleid op basis van rapportages over informatiebeveiliging.

6.2.3 Security Officer (SO)

Bij Nidos is de Security Officer (SO) de spin in het web met betrekking tot informatiebeveiliging. Op hoofdlijnen omvat deze rol de volgende verantwoordelijkheden:

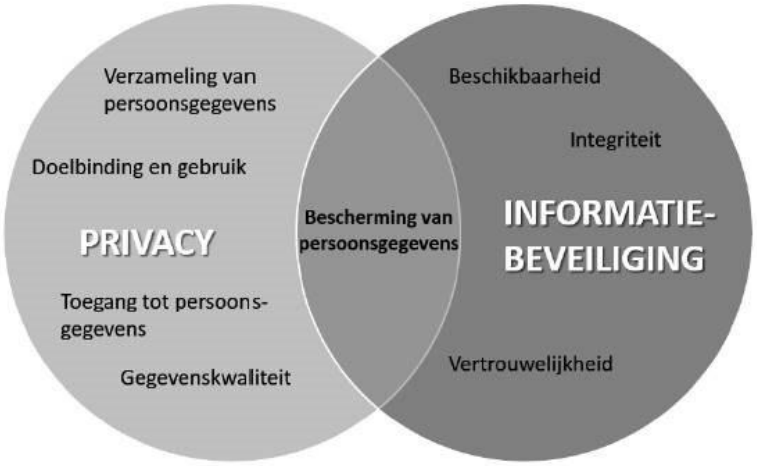
- toezicht houden op de naleving van de wet- en regelgeving, normen en standaarden met betrekking tot informatieveiligheid binnen Nidos;
- beleidsvorming, het beheren van het Nidos-brede informatiebeveiligingsbeleid en de hieruit voortvloeiende Nidos-brede richtlijnen en procedures, waaronder het informatiebeveiligingshandboek;
- controle en registratie, het bewaken van de uniformiteit en het niveau van de informatiebeveiliging binnen Nidos;
- aanspreekpunt voor incidenten, de afhandeling, registratie en evaluatie hiervan;
- communicatie en voorlichting, het coördineren van de implementatie van het gewenste niveau van informatiebeveiliging en het stimuleren van het beveiligingsbewustzijn bij management en (tijdelijke) medewerkers (in duidelijke en begrijpelijke taal);
- evaluatie en advies, het (gevraagd en ongevraagd) adviseren van de Bestuurder en andere leidinggevenden over informatiebeveiliging en het rapporteren over de status van informatiebeveiliging binnen Nidos.

6.2.4 Privacy Officer (PO)

De PO heeft een controlerende en adviserende taak op het gebied van privacy en is vanuit de Algemene Verordening Gegevensbescherming (AVG) verplicht gesteld. De PO is de interne toezichthouder op de Verwerking van Persoonsgegevens bij Nidos het aanspreekpunt op het gebied van AVG gerelateerde issues voor de Autoriteit Persoonsgegevens en rechthebbenden.
De PO heeft:

- toezicht op de toepassing en naleving van de AVG
- de rol van interne toezichthouder
- een adviserende rol op het gebied van AVG.
- een ondersteunde rol voor de directie bij het voldoen aan de AVG, bijvoorbeeld door het begeleiden van een DPIA of het afhandelen van een potentieel datalek.

Schematische weergave van de verdeling van het werkveld van de PO en de SO;



6.2.5 Interne Audit

Interne Audit is een rol die is ingericht binnen de Nidos.
Elk jaar stelt "Interne Audit" binnen Nidos een managementreview op waarin wordt teruggeblikt op het voorgaande jaar waarbij de directie vaststelt of we als organisatie nog in control zijn of niet.
Dit aan de hand van verschillende processen waaronder het proces rond informatieveiligheid waarbij een risico-inventarisatie wordt gedaan.
Ook van de informatiebeveiliging willen we weten of we de kwaliteit leveren die we beogen te halen en waar nodig bij te sturen.

6.3 DECENTRALE FUNCTIES EN ROLLEN IN DE AFDELINGEN

6.3.1 Directeur

De Directeuren hebben een sturende rol voor informatiebeveiliging en privacy. De Directeuren zijn eindverantwoordelijk voor het identificeren en beheersen van de risico's binnen het domein waarvoor ze verantwoordelijk zijn. De Directeur wordt op het gebied van informatiebeveiliging en privacy gerelateerde onderwerpen ondersteund door de SO en PO met gevraagd en ongevraagd advies. Om medewerkers in staat te stellen zich te ontwikkelen op het gebied van privacy en informatiebeveiliging, stelt de Directie middelen beschikbaar. De Directie wordt ondersteund door de PO en de SO bij het selecteren van deze middelen.

6.3.2 Manager IM&ICT

De manager IM&ICT is de portefeuillehouder en verantwoordelijk voor de uitvoering van het informatiebeveiligingsbeleid. Daarnaast is de manager IM&ICT verantwoordelijk voor het aansturen van de medewerkers binnen IM&ICT. De manager IM&ICT legt als portefeuillehouder verantwoording af over informatiebeveiliging en privacy gerelateerde IT-onderwerpen. Binnen deze scope valt ook het aansturen van IT-leveranciers; met andere woorden het uitvoering geven aan leveranciersmanagement.

6.3.3 IM&ICT medewerkers

IM&ICT medewerkers hebben de verantwoordelijkheid voor het ontwerpen, inrichten en beheren van de binnen Nidos gebruikte applicaties conform het informatiebeveiliging en Privacy beleid.
Voorbeelden van taken die hieronder vallen zijn het beheren van applicatie inloggegevens en bijbehorende autorisaties, het beheren van informatiebeveiliging gerelateerde parameters (zoals bijvoorbeeld wachtwoord complexiteit) en het ondersteunen bij informatiebeveiligingsincidenten. De medewerkers worden daarbij voorzien van gevraagd en ongevraagd advies door de SO en de PO.

6.3.4 Medewerkers

Informatiebeveiliging en Privacy is ieders verantwoordelijkheid. Er wordt van medewerkers verwacht dat ze zich integer gedragen. Niet acceptabel is dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies van Nidos of van individuen. Het is om deze reden dat er gedragscodes worden geformuleerd en toegepast. Ook in jaargesprekken en werkoverleg zijn dit gespreksonderwerpen die periodiek aan de orde komen. Medewerkers worden door de Directie gestimuleerd en in staat gesteld zich te ontwikkelen op het gebied van privacy en informatiebeveiliging.

7 PLANNING VAN INFORMATIE-BEVEILIGING.

Om vast te stellen welke maatregelen een organisatie moet nemen op het gebied van informatiebeveiliging, moeten eerst de risico's worden geïdentificeerd. Daarom wordt jaarlijks een risicoanalyse en een risicobehandelplan opgesteld/bijgewerkt voor Nidos. Daarnaast wordt voor sommige applicaties een DPIA met risicoanalyse uitgevoerd voordat ze in gebruik worden genomen door Nidos.
Risico's die onvoldoende worden beheerst kunnen worden gemitigeerd, geaccepteerd, vermeden of overgedragen. Afwegingen die gemaakt worden dienen te worden vastgelegd en gerapporteerd aan de Directie zodat het totale risicoprofiel van Nidos kan worden vastgesteld.
Voor het beheersen van de risico's wordt een risicobehandelplan opgesteld, waarin de te implementeren maatregelen worden beschreven en gepland.
Bij het vaststellen van de te implementeren maatregelen is het Nidos informatiebeveiligingsbeleid leidend en wordt de NEN 7510, Annex A gebruikt als referentiekader. De maatregelen worden altijd risico gebaseerd geselecteerd, hetgeen inhoudt dat alleen de maatregelen die een bestaand risico afdekken worden geselecteerd.

In het volgende hoofdstuk staan de richtlijnen die het kader van het informatiebeveiligingsbeleid vormen. Waar nodig wordt het beleid op onderdelen in detail uitgewerkt in separate documentatie.
De SO bewaakt de voortgang van de risicobehandelplannen, rapporteert over de voortgang en adviseert bij het uitvoeren van de risicobehandelplannen.

8 RICHTLIJNEN INFORMATIE-BEVEILIGINGSBELEID NIDOS

Om de omvang van dit beleid zo beperkt mogelijk te houden, zijn voor de volgende onderdelen separate richtlijnen opgesteld:

- Thuiswerkbeleid
- Gedragscode

De volgende onderwerpen zijn onderdeel van de uitbesteding ICT:

- Logging en monitoring
- Bedrijf continuïteit
- Operations
- Security Incidenten
- Herstel

8.1 BORGEN VAN SECURITY IN PROJECTEN

In dit onderdeel wordt er van uitgegaan dat Nidos niet zelf IT applicaties/ toepassingen ontwikkelt.

- Voordat een applicatie/ toepassing in gebruik genomen gaat worden, worden de eisen omtrent informatiebeveiliging vastgesteld. Hierbij wordt de SO betrokken.
- Voordat een applicatie/ toepassing in gebruik genomen wordt, moet een DPIA worden uitgevoerd. Hier wordt de SO en PO bij betrokken
- Voordat een applicatie/ toepassing in gebruik genomen wordt, wordt een applicatie security scan uitgevoerd. Hier wordt de SO bij betrokken.
- De PO en de SO worden zo vroeg als nodig betrokken door het project, maar niet later dan het moment waarop een keuze voor een applicatie/toepassing gemaakt wordt.

8.2 VEILIGE WERKOMGEVING

- In arbeidsovereenkomsten met alle medewerkers is een bepaling opgenomen met betrekking tot geheimhouding. Deze bepaling geldt ook nadat de medewerker uit dienst is getreden.
- Bij overtreding van deze bepaling volgen sancties
- Alle medewerkers worden bij hun aanstelling en gedurende hun verdere loopbaan binnen Nidos op de hoogte gehouden van het geldende informatiebeleid, voor zover dat voor hen relevant is. Het is bijvoorbeeld niet nodig een jeugdzorgmedewerker kennis te laten nemen van het backup en restore beleid. De Directie bepaalt welke onderwerpen voor welke (groep van) medewerkers relevant is.

8.3 BEHEER VAN BEDRIJFSMIDDELEN

- Er wordt een overzicht bijgehouden van IT middelen (bv applicaties, websites en IT middelen zoals laptops en tablets).
- Alle (groepen van) IT middelen hebben een eigenaar
- IT middelen worden up to date gehouden (patches, firmware updates etc.)
- Er is een procedure voor het uitgeven, beheren en weer innemen van IT middelen aan medewerkers. Bij het uitreiken van IT middelen worden afspraken gemaakt over aanvaardbaar gebruik
- Datadragers (bv Laptops, Telefoons, Tablets, Domotica) worden voor ze worden afgevoerd/ hergebruikt, gewist
- Indien voor het gebruik van middelen licenties benodigd zijn, worden procedures opgesteld voor het uitgeven, intrekken en controleren op gebruik en geldigheid van licenties

8.4 INFORMATIECLASSIFICATIE

Alle informatie binnen Nidos wordt geclassificeerd naar één van de drie niveaus van vertrouwelijkheid, zoals hieronder vermeld.

Gegevens-classificatie	Kenmerken van informatie
Publiek	Deze informatie kent veelal lage eisen ten aanzien van de vertrouwelijkheid en beschikbaarheid en is daardoor voor **iedereen** binnen en buiten Nidos beschikbaar en toegankelijk (maar is niet te wijzigen).
Intern Nidos	Dit betreft de informatie die toegankelijk mag of moet zijn voor een groot deel van de **medewerkers / ZZP-ers** van Nidos maar is niet bedoeld dat deze informatie publiek toegankelijk is. De eisen ten aanzien van vertrouwelijkheid zijn beperkt maar aanwezig.
Vertrouwelijk (Nidos)	Dit betreft de informatie die toegankelijk mag of moet zijn voor een **beperkt** deel van de **medewerkers / ZZP-ers** van Nidos. Indien deze informatie publiek toegankelijk wordt kan dit leiden tot schade voor de medewerker of organisatie.
Vertrouwelijk (klantdata)	Dit betreft informatie die alleen toegankelijk mag zijn voor een **beperkte** groep **medewerkers / ZZP-ers**. De informatie wordt beschikbaar gesteld op basis van het "*need to know*" principe[1]. Schending van deze classificatie kan direct of indirecte schade toebrengen aan de klantorganisatie en haar medewerkers en/of Nidos.

8.5 VEILIG OPSLAAN EN DELEN VAN GEGEVENS

- Koppelingen tussen systemen zijn beveiligd door middel van encryptie
- Voor het uitwisselen van vertrouwelijke gegevens tussen personen wordt een secure email oplossing gebruikt waarbij ten minste twee factor authenticatie wordt toegepast voor zowel de zendende als ontvangende partij
- Voor het uitwisselen van grote bestanden (zowel eenmalig als structureel zoals bij langdurige projecten) wordt gebruik gemaakt van de faciliteiten die door Nidos worden aangeboden. Te denken valt aan Office365 in combinatie met Zivver. Toepassingen zoals Dropbox en WeTransfer zijn niet toegestaan.
- Het gebruik van datadragers zoals USB sticks, is niet toegestaan
- Het opslaan van vertrouwelijke gegevens buiten de daarvoor bedoelde toepassing (bv PRS, EPD, EGD, ADP en de koppeling daartussen) is niet toegestaan

[1] Need to know principe. Dit principe houdt in dat functionarissen slechts toegang hebben tot die informatie die zij nodig hebben voor het uitoefenen van hun functie.

8.6 LOGISCHE TOEGANGSBEVEILIGING

- Medewerkers hebben een uniek user id
- Toegang tot gegevens is altijd te herleiden tot een natuurlijk persoon
- Er is een proces waarmee wordt geborgd dat de toegang tot systemen, mappen en mailboxen is gekoppeld aan de instroom/doorstroom/uitstroom van medewerkers. Hier wordt een registratie van bijgehouden
- Autorisaties worden regelmatig (minimaal 1x per kwartaal) gecontroleerd
- Toegang tot systemen vindt plaats op basis van functie/rol/bevoegdheden en/of locatie
- Toegang tot systemen is beveiligd met een sterk wachtwoord
- Toegang tot systemen waarin cliënt informatie wordt verwerkt is op basis van twee factor authenticatie.
- Wachtwoorden mogen niet opgeschreven worden of worden bewaard in niet beveiligde bestanden
- Wachtwoorden voldoen aan de volgende eisen (Microsoft default):
    - Minimaal 8 karakters
    - Minimaal 1 leesteken
    - Minimaal 1 letter
    - Minimaal 1 cijfer
    - Maximaal 3 maanden geldig; deze eis vervalt indien twee factor authenticatie wordt toegepast
    - Initiële wachtwoorden moeten direct aangepast worden
    - Na 5 x verkeerd aanloggen moet het user ID voor minimaal 15 minuten geblokkeerd worden. Daarna bij iedere verkeerde poging
- Beheerders met admin rechten gebruiken altijd twee factor authenticatie bij beheerwerkzaamheden

8.7 EISEN AAN WEBSITES

In dit onderdeel wordt er van uitgegaan dat Nidos al het beheer van de website (deels) uitbesteedt aan derde partijen.

- De leverancier is ISO 27001 gecertificeerd of voldoet aantoonbaar aan ISO 27001
- De leverancier kan aantonen dat de website is gemaakt en wordt onderhouden conform de OWASP top 10
- Websites maken gebruik van een geldig SSL-certificaat dat minimaal een A scoort volgens SSL Labs
- Voor het gebruik van cookies wordt vooraf toestemming gevraagd aan de bezoeker van de website: Bij weigeren van de Cookies door de bezoeker, moet toegang tot de website voor die bezoeker wel mogelijk blijven
- Er is een geldige privacyverklaring op de website beschikbaar
- De leverancier laat regelmatig (minimaal 1 x per jaar of na iedere grote wijziging) de site onderwerpen aan een pentest.
- Er is een proces ingericht voor het tijdig vervangen en veilig opslaan de private key van Certificaten voor websites

8.8 LEVERANCIERSMANAGEMENT

- In de overeenkomsten met leveranciers die mogelijk toegang hebben tot vertrouwelijke data van Nidos worden bepalingen met betrekking tot informatiebeveiliging opgenomen
- Met leveranciers die mogelijk toegang hebben tot persoonsgegevens, wordt een verwerkersovereenkomst afgesloten
- De leverancier is ISO 27001 gecertificeerd of voldoet aantoonbaar aan ISO 27001
- In de overeenkomst wordt het recht op het uitvoeren van een audit opgenomen.
- Leveranciers worden voorafgaande aan contracteren, door de SO getoetst of ze voldoen aan het Nidos Informatie Beveiligingsbeleid
- De contracteigenaar monitort en beoordeelt de leverancier op het naleven van de contracteisen op het gebied van informatiebeveiliging.
  Bij de beoordeling van de leverancier op het naleven van de afspraken op het gebied van IB, wordt een document
  “Leveranciersbeoordelingsformulier” gebruikt.

8.9 NALEVING VAN WET- EN REGELGEVING

Nidos dient zich te houden aan alle relevante wet- en regelgeving die van toepassing is op het uitvoeren van de dagelijkse werkzaamheden. De relevante wet- en regelgeving is vertaald naar richtlijnen en gedragscodes die van toepassing zijn op alle medewerkers van Nidos en voor het overige van toepassing zijn op inhuurpersoneel, stagiaires van Nidos of derden (zoals leveranciers) die gebruik maken van informatievoorzieningen van Nidos. In het bijzonder gelden in dit verband de volgende richtlijnen en codes:
Op te volgen wettelijke voorschriften en normen:

- Jeugdwet; zie wetten.nl - Regeling - Jeugdwet - BWBR0034925
- Pivacyreglement; zie Privacy
- Wet op computercriminaliteit (30 mei 2016).
- Arbeidsrecht. Burgerlijk Wetboek bevat de belangrijkste regels van het arbeidsrecht (boek 7 titel 10) gericht op de eisen voor de arbeidsovereenkomst.
- Algemene Verordening Gegevensbescherming2 (AVG) Europese richtlijn (24 mei 2016).
- Auteurswet (11 oktober 2018, De wet van 23 september 1912, houdende nieuwe regeling van het auteursrecht)
- Meldplicht datalekken, gebaseerd op de AVG 24 mei 2016) .
- NIS2 (per 1 oktober 2024)
- ISAE 3402 type 2.
- Personeelsgids; zie Voor nieuwe medewerkers

Daarnaast gelden de afspraken die contractueel gelden met leveranciers waarmee Nidos afspraken heeft gemaakt.
Indien Nidos schade ondervindt door nalatigheid bij het gebruik of het opzettelijke misbruik van informatievoorzieningen (plichtsverzuim) zal de vigerende wet- en regelgeving worden toegepast en op basis daarvan neemt de directie van Nidos aanvullende maatregelen.

[2] De AVG is de Europese privacy verordening die per24 mei 2016 in werking is getreden en vanaf 25 mei 2018 van toepassing is.

9 EVALUATIE & CONTROLE

Onder controle wordt verstaan zowel interne controle door de eigen organisatie als toetsing door een onafhankelijke derde. De toetsing richt zich hierbij zowel op het beveiligingsbeleid als op de maatregelen die uit dit beleid voortvloeien. De toetsing daarom gericht op de volgende onderwerpen:

1. De juiste naleving van het beleid en de interne werkafspraken;
2. Een correcte werking van de beveiligingsorganisatie;
3. De beoordeling van de toereikendheid van de vastgestelde beveiligingsmaatregelen gedurende een bepaalde periode

Onder evaluatie wordt verstaan het nagaan of de kaders van de beveiliging inhoudelijk nog toereikend zijn. Hierbij worden twee niveaus onderscheiden: de evaluatie van het beleid en de evaluatie van het beheer.
De evaluatie van het beleid is een heroriëntatie op de beleidsuitgangspunten. Bij de evaluatie van het beheer wordt nagegaan of het vastgestelde beleid nog toereikend is. De periodieke controle op de informatieveiligheid is opgenomen in het auditjaarplan.

10 BIJLAGE 1 – DEFINITIES

In deze bijlage worden enkele definities nader toegelicht.

Algemene Verordening Gegevensbescherming
De AVG is de Europese privacy verordening die per24 mei 2016 in werking is getreden. De Verordening is per vanaf 25 mei 2018 van toepassing. De AVG vervangt de huidige privacy wetten van de verschillende EU-lidstaten.

R&C Risk & Compliance
Risk & Compliance is verantwoordelijk voor de controle op naleving van de richtlijnen waarbij ze binnen afgesproken grenzen coaching en begeleiding aan de bedrijven aanbiedt.

SO Security Officer
De functionaris binnen Nidos welke is belast met het coördineren van de informatiebeveiligingsactiviteiten.

PO Privacy Officer
De PO is de interne toezichthouder op de Verwerking van Persoonsgegevens bij Nidos en primair aanspreekpunt op het gebied van AVG gerelateerde issues voor de Autoriteit Persoonsgegevens en rechthebbenden

Interne Audit
Interne Audit is een rol voor het voeren van audits
op informatiebeveiliging en/of privacy.

Continuïteitsplan
Een plan om bij (ernstige) verstoringen de informatievoorziening gericht op het primaire proces, binnen de door Nidos aangegeven tijd, weer beschikbaar te hebben.

Compliant
Compliance betekent dat de organisatie moet (en wil) voldoen aan de wet- en regelgeving. Het niet voldoen aan compliance-eisen brengt risico's met zich mee zoals:

- imagoschade die kan worden opgelopen;
- financiële schade in de vorm van boetes of claims.

Fysieke en digitale informatiesystemen
Informatiesystemen met het doel vanuit gegevensbronnen voor een gebruiker relevantie informatie te generen. Dit kan een digitaal systeem (bijvoorbeeld: een applicatie) zijn of een fysiek systeem (bijvoorbeeld: het HRM-dossier in een kast)

Incidentenregistratie
Een systeem, bij voorkeur digitaal, waar meldingen over de informatiebeveiliging in worden geregistreerd zodat de organisatie adequaat kan reageren en de opvolging kan worden gemonitord.

ISMS
Het Information Security Management System. Door het inrichten van een ISMS behoudt de organisatie grip op het onderwerp Informatiebeveiliging.