Overzicht wet- en regelgeving

Het volgende overzicht bevat wetten en regelgeving die van toepassing zijn op [ORGANISATIE] en die mogelijk raakvlakken hebben met informatiebeveiliging. Er wordt hier ook bijgehouden op welke processen het van toepassing is, en in hoeverre eraan voldaan wordt. Dit document is een invulling van ISO 27001 normeis A18.1.1 (ISO 27001:2017) of A5.31 (ISO 27001:2022).

# Privacy

|  |  |  |  |
| --- | --- | --- | --- |
| **Wet/regelgeving/contract** | **Processen** | **Concrete eis aan het ISMS** | **Status implementatie** |
| Algemene verordening gegevensbescherming (AVG)  Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) | Bijna alle processen, [SECTOR SPECIFIEKE PROCESSEN] en HR bevatten bijzondere en gevoelige gegevens, veel ondersteunende processen gebruiken ook persoonsgegevens |  | Geïmplementeerd. [GENOMEN ACTIES]. Ook is er een privacyverklaring:  [LINK PRIVACYVERKLARING] |
| Telecommunicatiewet (Tw) | Externe websites waar gebruik gemaakt wordt van cookies of andere methodes om bezoekers te tracken. |  | Geïmplementeerd. Bijvoorbeeld door toevoegen cookieverklaring  [LINK COOKIEVERKLARING] |
|  |  |  |  |

# (eventueel) Zorg

|  |  |  |  |
| --- | --- | --- | --- |
| **Wet/regelgeving/contract** | **Processen** | **Concrete eis aan het ISMS** | **Status implementatie** |
| Wet op de geneeskundige behandelingsovereenkomst (WGBO)  Wet op de beroepen in de individuele gezondheidszorg (Wet BIG)  Wet kwaliteit, klachten en geschillen zorg (Wkkgz)  Uitvoeringsbesluit Wkkgz  Wet verplichte geestelijke gezondheidszorg (Wvggz)  Wet zorg en dwang (Wzd)  Wet forensische zorg (Wfz)  Burgerlijk Wetboek (BW) boek 1 (m.n. bepalingen curatorschap en mentorschap)  Gezondheidswet  Zorgverzekeringswet (Zvw)  Wet langdurige zorg (Wlz)  Wet maatschappelijke ondersteuning (Wmo 2015)  Jeugdwet  Wet medisch-wetenschappelijk onderzoek met mensen  Wet op de medische hulpmiddelen  Wet op de orgaandonatie  Wet publieke gezondheid  Mededingingswet  Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz)  Wet marktordening gezondheidszorg (Wmg)  Wet medezeggenschap cliënten zorginstellingen 2018 (Wmcz)  Geneesmiddelenwet  Wet toelating zorginstellingen (Wtzi) | Zorgverleningsprocessen | Bewaartermijn medische informatie, medisch beroepsgeheim (beperkt delen informatie) | Al deze wetten zijn geïmplementeerd en worden nageleefd. Over het algemeen is dit niet per wet gedaan maar met een integrale aanpak die ontwikkeld is om aan de eisen van de Nederlandse wet te voldoen.  Waar nodig is er advies gegeven door de bedrijfsjurist. |

# Arbeid/ personeel

|  |  |  |  |
| --- | --- | --- | --- |
| **Wet/regelgeving/contract** | **Processen** | **Concrete eis aan het ISMS** | **Status implementatie** |
| Arbeidsrecht, onder andere:   * Wet op de ondernemingsraden * Arbeidsovereenkomst, artikel 7:610 e.v. BW * Arbowet, -besluit en -regeling * Wet werk en zekerheid * Arbeidstijdenwet * Wet transitievergoeding arbeidsongeschikte medewerkers * Wet verbetering poortwachter * Wet DBA | HR-processen |  | Geïmplementeerd. De afdeling HR zorgt voor de integriteit, beschikbaarheid en betrouwbaarheid van personeelsgegevens. [ORGANISATIE] verwerkt gegevens van personeel wanneer daar een wettelijke basis voor is. Er is gekozen voor een systeem ([SYSTEEM]) dat ontwikkeld is om aan de Nederlands wetgeving te voldoen. |

# Financieel

|  |  |  |  |
| --- | --- | --- | --- |
| **Wet/regelgeving/contract** | **Processen** | **Concrete eis aan het ISMS** | **Status implementatie** |
| Belastingwet | Financiële processen |  | Geïmplementeerd. De financiële processen worden ook door [AFDELING/ORGANISATIE] gecontroleerd |
| Archiefwet | Financiële processen |  | Binnen de financiële systemen is ervoor gezorgd dat de wettelijke bewaartermijn wordt nageleefd. |

# (eventueel) Vastgoed

|  |  |  |  |
| --- | --- | --- | --- |
| **Wet/regelgeving/contract** | **Processen** | **Concrete eis aan het ISMS** | **Status implementatie** |
| Bouwbesluiten (deze bevatten eisen die raken aan continuïteit, bijvoorbeeld brandmelders) | Alle processen die binnen [ORGANISATIE] locaties plaatsvinden |  | [STATUS] [UITLEG STATUS] |

# Contractuele eisen

|  |  |  |  |
| --- | --- | --- | --- |
| **Wet/regelgeving/contract** | **Processen** | **Concrete eis aan het ISMS** | **Status implementatie** |
| Afspraken met [TYPE LEVERANCIER/DERDE PARTIJ] | [HOOFDPROCES] |  | [STATUS] [UITLEG STATUS] |
| (eventueel) Afspraken gedeelde locaties | [HOOFDPROCES] als een locatie (bijvoorbeeld een gedeeld restaurant/lobby) met andere organisaties gedeeld wordt. |  | De [ROL PERSOON] houdt een overzicht van afspraken bij en onderhoudt contact met deze organisaties |

# Intellectueel eigendom

Toepasselijke wetten en regelingen:

* Auteurswet (Aw)

[ORGANISATIE] prefereert het inkopen van standaardpakketten voor software boven maatwerkoplossingen. Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectuele-eigendomsrechten en het gebruik van eigendomssoftwareproducten te waarborgen wordt het reguliere inkoopproces gevolgd. Contractuele voorwaarden zijn leidend voor omgang met intellectueel eigendom.

***Over dit template:***

*Dit template is gemaakt door de mensen van ICT Institute.*

*Het template mag gratis worden gebruikt, onder een creative commons licentie*

[*https://creativecommons.org/licenses/by/4.0/*](https://creativecommons.org/licenses/by/4.0/)

*De nieuwste versie staat op:*

[*https://softwarezaken.nl/2022/01/gratis-27001-avg-templates/*](https://softwarezaken.nl/2022/01/gratis-27001-avg-templates/)

*Je mag het template uitbreiden, aanpassen en bewerken zoveel je wilt*

*Je mag het template en documenten gemaakt met het template doorgeven en delen zoveel je wilt*

*Als je het template doorgeeft, dan moet je "gemaakt door de mensen van ICT Institute" laten staan*

*Als je een document maakt met dit template en je bent geen opdrachtgever van ons, zet dat "gemaakt met template van ICT Institute" ergens in het document*

*Als je een opdrachtgever bent van ICT Institute, dan mag je alles doen met dit template wat je wilt*

*Let op dat je de ISO 27001 norm moet kopen bij NEN of een andere organisatie voordat je de norm gaat gebruiken. De norm is auteursrechtelijk beschermd*

*Lees vooral ook deze artikelen als je aan de slag gaat:*

[*https://softwarezaken.nl/2017/03/samenvatting-iso-27001-informatie-beveiliging/*](https://softwarezaken.nl/2017/03/samenvatting-iso-27001-informatie-beveiliging/)

[*https://softwarezaken.nl/2021/12/iso-27001-certificatie-aanvraag/*](https://softwarezaken.nl/2021/12/iso-27001-certificatie-aanvraag/)

[*https://softwarezaken.nl/2018/01/gdpr-avg-in-10-stappen/*](https://softwarezaken.nl/2018/01/gdpr-avg-in-10-stappen/)

[*https://softwarezaken.nl/security-verified/*](https://softwarezaken.nl/security-verified/)