Informatiebeveiliging Beleid Techni Team ICT BV

Versie 5.7

29 september 2022

Techni Team ICT B.V. – Schietboom 2, 3905 TD Veenendaal
0318 57 43 85 – info@techniteam.nl – www.techniteam.nl

Techni Team
ICT zonder zorgen

Inhoudsopgave

1. Versiebeheer

1.1 Versie, Recensenten, Distributielijst

Eigenaar		Ardin M.C. Vlot		
Vertrouwelijkheid		I. Intern vertrouwelijk		
Geldig tot (review voor:)		1 juni 2023		
Versie	Status	Aangepast	d.d.	Door
5.0	Draft	Algehele revisie	10-10-17	Ardin M.C. Vlot
5.1	Finaal	Algehele revisie met Menzo Bomhof	17-05-18	Ardin M.C. Vlot
5.1	Goedgekeurd	Goedkeuring	18-06-18	Directie
5.2	Update	Bijlage Doelstellingen toegevoegd	24-10-18	Ardin M.C. Vlot
5.3	Update	Enkele tekstuele aanpassingen	29-10-18	Ardin M.C. Vlot
5.4	Update	VOG na 01-01-2015	19-06-19	Menzo Bomhof
5.5	Update	Algehele actualisering	16-03-21	Ardin M.C. Vlot
5.6	Update	Toevoegen norm hoofdstuk 2	31-03-22	Menzo Bomhof
5.7	Update	VOG Beleid in lijn met RAA	15-09-22	Menzo Bomhof

2. Norm ISO 27001 en NEN 7510

A.5 IB-beleid				
A.5.1 Aansturing door Directie van de IB				
Doelstelling: Het verschaffen van Directie aansturing van en -steun voor IB in overeenstemming met bedrijfseisen en relevante wet- en regelgeving.				
Norm	**Omschrijving**	**Beheersmaatregel**	**Zorg specifieke maatregelen**	**VVT**
A .5.1.1	Beleidsregels voor IB	Ten behoeve van IB moet een reeks beleidsregels worden gedefinieerd, goedgekeurd door Directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	Organisaties moeten beschikken over een schriftelijk informatiebeveiligingsbeleid dat door het management wordt goedgekeurd, wordt gepubliceerd en vervolgens wordt gecommuniceerd aan alle werknemers en relevante externe partijen.	j
A.5.1.2	Beoordelen van het IB-beleid	Het beleid voor IB moet met geplande tussenpozen of als zich significante veranderingen voordoen, worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	Het informatiebeveiligingsbeleid moet aan voortdurende, gefaseerde beoordelingen worden onderworpen zodat het volledige beleid ten minste eenmaal per jaar wordt beoordeeld. Het beleid moet worden beoordeeld als er zich een ernstig beveiligingsincident heeft voorgedaan.	j

3. Inleiding

Dit document geeft algemene beleidsuitgangspunten over informatiebeveiliging van Techni Team ICT BV. Het managementsysteem moet passend zijn voor de organisatie. De inrichting van het Information Security Management System (ISMS) is gebaseerd op de eisen uit de ISO27001 norm en de NEN7510.
In de ISO27001 staat in hoofdstuk 0;

> *"Het vaststellen en implementeren van een managementsysteem voor informatiebeveiliging wordt beïnvloed door de behoeften en doelstellingen van de organisatie, de beveiligingseisen, de procedures die de organisatie toepast en de omvang en structuur van de organisatie."*

En in hoofdstuk 5;

> *"De Directie moet een informatiebeveiligingsbeleid vaststellen dat passend is voor het doel van de organisatie".*

De NEN7510 biedt een gemeenschappelijk kader voor het inrichten van de informatiebeveiliging in de gezondheidszorg. Dit gemeenschappelijke kader is nodig met het oog op de samenwerking binnen en tussen verschillende organisaties in de zorg.
Dit document is daarvoor het uitgangspunt. Minimaal jaarlijks (of bij grote veranderingen die impact hebben op het ISMS) wordt dit Informatiebeveiligingsbeleid (IB) herzien en goedgekeurd door de directie in haar rol van beleidsbepaler in het ISMS volgens de NEN7510 standaard. Zodoende blijft het IBB passend voor Techni Team ICT BV en krijgt een formele status.

3.1 Doel en doelstellingen

Dit document biedt de handvatten aan onze medewerkers bij de inrichting van de organisatie, procedures, werkwijze en informatiesystemen. Doel van het Informatiebeveiligingsbeleid is om de **vertrouwelijkheid, integriteit en beschikbaarheid** van de gegevens die door ons verwerkt worden te garanderen. De Directie is eindverantwoordelijk voor het up to date zijn en de naleving van dit Informatiebeveiligingsbeleid.
Vertrouwen is voor Techni Team ICT BV een groot goed. We vertrouwen medewerkers, klanten, leveranciers en andere stakeholders waarbij we leunen op het wederkerigheidsprincipe. Techni Team ICT BV gaat ervan uit, dat afspraken m.b.t. integriteit, vertrouwelijkheid en continuïteit van de informatievoorziening worden nagekomen zoals zij deze zelf ook nakomt.

In 2006 is Techni Team ICT BV gestart met het uitrollen van een fullservice dienstverlening op het gebied van kantoorautomatisering binnen het MKB. Door een terugkerende en groeiende vraag naar deze dienstverlening binnen de eerstelijnszorg, heeft Techni Team ICT BV haar dienstenpakket doorontwikkeld op basis van de trends en ontwikkelingen in de markt van de gezondheidszorg. Werken voor en in de zorg maakt het noodzakelijk om inzage te geven in het beleid van informatiebeheer. Daarnaast heeft Techni Team zich sinds 2021 toegelegd op het distribueren en implementeren van Security Tools & Services. Zij richt zich daarbij op collega-ICT bedrijven en MKB-bedrijven die behoefte hebben aan deze additionele dienstverlening.
Binnen ICT-dienstverlening is veel digitale communicatie nodig, waarvoor diverse verbindingen en voorzieningen in de infrastructuur van het bedrijf aanwezig zijn. Medewerkers hebben door hun kennis toegang tot alle informatie van opdrachtgevers. Tevens is deze toegang noodzakelijk voor het uitoefenen van de beheerfunctie. Deze openheid zal als een gegeven geaccepteerd moeten worden. Maatregelen zijn daarom noodzakelijk om de privacygevoelige informatie en vertrouwelijkheid te waarborgen.
Door de communicatie met de buitenwereld en de aansluitingen van de interne op de externe infrastructuur is er risico voor inbraken en virussen van buitenaf. Tevens is er risico dat mensen die het bedrijf bezoeken (ook onuitgenodigd) pogingen ondernemen om via systemen van Techni Team ICT BV toegang te krijgen tot informatie.

De belangen die Techni Team ICT BV heeft bij informatiebeveiliging zijn als volgt te rangschikken, in volgorde van preventief naar curatief:

- Het waarborgen van de continuïteit van het primaire proces
- Het beschermen van vertrouwelijke en/of gevoelige informatie in het primaire proces
- Het voorkomen van imagoschade en het behouden van een professionele uitstraling
- Het voorkomen van bedrijfsschade
- Het beschermen van vitale bedrijfsinformatie
- Het voldoen aan wettelijke voorschriften

Met nadruk wordt gesteld dat het preventieve aspect van het grootste belang is. Voorkomen is in het algemeen beter dan genezen. De inzet tot het waarborgen van de continuïteit van processen zal betekenen dat de continuïteit ook daadwerkelijk op een hoog niveau blijft.
Het informatiebeveiligingsbeleid geldt voor alle medewerkers, bezoekers, partners en leveranciers van Techni Team ICT B.V.

Techni Team heeft de volgende IBB doelstellingen geformuleerd:

Doelstelling	Wanneer is de doelstelling gehaald (welke uitkomst van de meting?	Vastlegging
De veilige omgang met gegevens van klanten en hun klanten is van kritiek belang voor de dienstverlening en voortbestaan van Techni Team, zij treft de passende technische en organisatorische maatregelen toe om de veiligheid hiervan te kunnen borgen. De mate van beveiliging en naleving wordt bepaald door de directie, die deze afweging maakt en verifieert op passendheid op strategisch niveau, door stakeholder- en risicoanalyse. En op basis van beschikbare middelen. Dit is altijd een bedrijfseconomische afweging.	Beleid moet zijn opgesteld, goedgekeurd, gedistribueerd, gepubliceerd en communiceerd. Het personeel moet zich bewust zijn van het beleid en hiernaar handelen.	Directiebeoordeling Informatiebeveiligingsbeleid
Verantwoordelijkheden voor de bescherming van gegevens en voor het uitvoeren van beveiligingsprocedures zijn expliciet gedefinieerd en vallen onder de eindverantwoordelijkheid van de directie. De rollen en verantwoordelijkheden rondom Informatiebeveiligingsbeleid zijn vastgelegd en geïmplementeerd.	Alle rollen en verantwoordelijkheden zijn vastgelegd en toegewezen.	Interne organisatie I.B. en competenties Informatiebeveiliging
De doelstellingen en beheersmaatregelen van de norm NEN-ISO/IEC 27001:2013, de richtlijnen volgend uit de AVG (2018), gedefinieerde stakeholderseisen en contractuele verplichtingen van klanten, vormen de basis voor ons Informatiebeveiligingsbeleid op de dienstverlening in scope. Vertrouwen is voor Techni Team een groot goed. We hanteren het wederkerigheidsprincipe medewerkers, klanten, leveranciers en andere stakeholders: Techni Team gaat ervan uit, dat zij afspraken nakomen m.b.t. integriteit, vertrouwelijkheid en continuïteit van de informatievoorziening. Dit is de grondslag voor elke	Jaarlijks wordt een risico assessment uitgevoerd. Daarnaast worden op basis van controles, geconstateerde afwijkingen, of incidenten eventuele nieuwe risico's gedocumenteerd en gemitigeerd.	Risico assessment en behandelmethodiek Stakeholderanalyse
Techni Team ziet toe op risicoveranderingen, Informatiebeveiligings- en privacyaspecten bij nieuwe initiatieven (privacy by design). Afwijkingen, veranderingen en mogelijke risico(veranderingen) worden opgemerkt, vastgelegd, verwerkt en geëvalueerd.	IBB-Wijzigingen worden altijd in EBS vastgelegd, ook als ze geen risico inpliceren. Dit wordt steekproefsgewijs gecontroleerd.Deze worden afgehandedl volgens een vast procedee, overeenkomstig de norm.	Kwartaaloverleg Informatiebeveiligingsbeleid
Afwijkingen van afspraken en procedures, mogelijke kwetsbaarheden en schendingen van integriteit, vertrouwelijkheid en beschikbaarheid van gegevens worden opgemerkt, geanalyseerd, vastgelegd en geclassificeerd Indien een incident de continuïteit van de dienstverlening in gevaar brengt treedt het Continuïteitsplan in werking.	IBB-Incidenten worden altijd in EBS vastgelegd. Deze worden afgehandeld volgens een vast procedee, overeenkomstig de norm.	incidentmanagement continuiteitsbeheer documentbeheer

Doelstelling	Wanneer is de doelstelling gehaald (welke uitkomst van de meting?	Vastlegging
Techni Team treft de passende organisatorische en technische maatregelen voor veilige gegevensverwerking. Techni Team respecteert daarbij de drie regels van logische informatiebeveiliging: 1. Niet hebben: Techni Team slaat geen onnodige (categorieën van) gegevens op. 2. Niet slepen: data worden verwerkt op één plek, afwijkingen alleen in overleg 3. Scheiden van data/omgevingen: middels dataclassificatie en toegangsbeheer.	Uitsluitend gebruik van crypto-USB, alle klantdata achter slot en grendel, vervoer van data alleen op uitneembere HD	Documentbeheer Beheer middelen
Informatiebeveiligingsbeleid is bij Techni Team een continu verbeterproces. Afwijkingen en veranderingen worden geanalyseerd. Middels in- en externe audits beoordeelt directie periodiek de werking van het beleid.	Acties en evaluaties worden voor minmaal 90% uitgevoerd	Auditplan Informatiebeveiligingsbeleid
De Security Officer ondersteunt Techni Team vanuit een onafhankelijke positie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover periodiek -en wanneer noodzakelijk- aan de directie.	Acties en evaluaties worden voor minmaal 90% uitgevoerd	Directiebeoordeling operationele planning continuiteitsbeheer
De directie ziet toe op naleving van de beleidsuitgangspunten voor die gegevensbewerkingen, waarvoor Techni Team wettelijk en/of contractueel verantwoordelijk is. Zij laat periodiek de werking van het beleid en de naleving van deze maatregelen intern en extern beoordelen om te borgen, dat het IB-managementsysteem blijvend adequaat werkt en waar nodig verbeterd wordt.	Directiebeoordeling en kwartaalmeetings functioneren naar behoren	Informatiebeveiligingsbeleid directiebeoordeling
Medewerkers, contractanten, partners en leveranciers die werken met de aan ons toevertrouwde gegevens zijn op de hoogte van ons Informatiebeveiligingsbeleid en de betekenis daarvan voor hun werkzaamheden. Om de continuïteit te waarborgen is dit vastgelegd in overeenkomsten, wordt er gelogd en gemonitord, periodiek gecontroleerd en gerapporteerd. Disciplinaire maatregelen worden waar nodig getroffen.	Opzetten van KPI-structuur zodat het functioneren van het IBB kwantitatief gemeten kan worden.	Informatiebeveiligingsbeleid uitbestedingsbeleid directiebeoordeling

4. Toepassingsgebied

Dit beleid is van toepassing op alle klantinformatie die we verwerken. Het beleid en de uitwerking hiervan geldt voor alle medewerkers en inhuur/contractanten van Techni Team ICT BV. Deze zijn middels de ethische code gehouden aan de naleving. Afwijkingen hierop moeten gemeld worden, zodat het managementsysteem continu verbeterd kan worden.

4.1 Houderschap en reikwijdte van het beleid

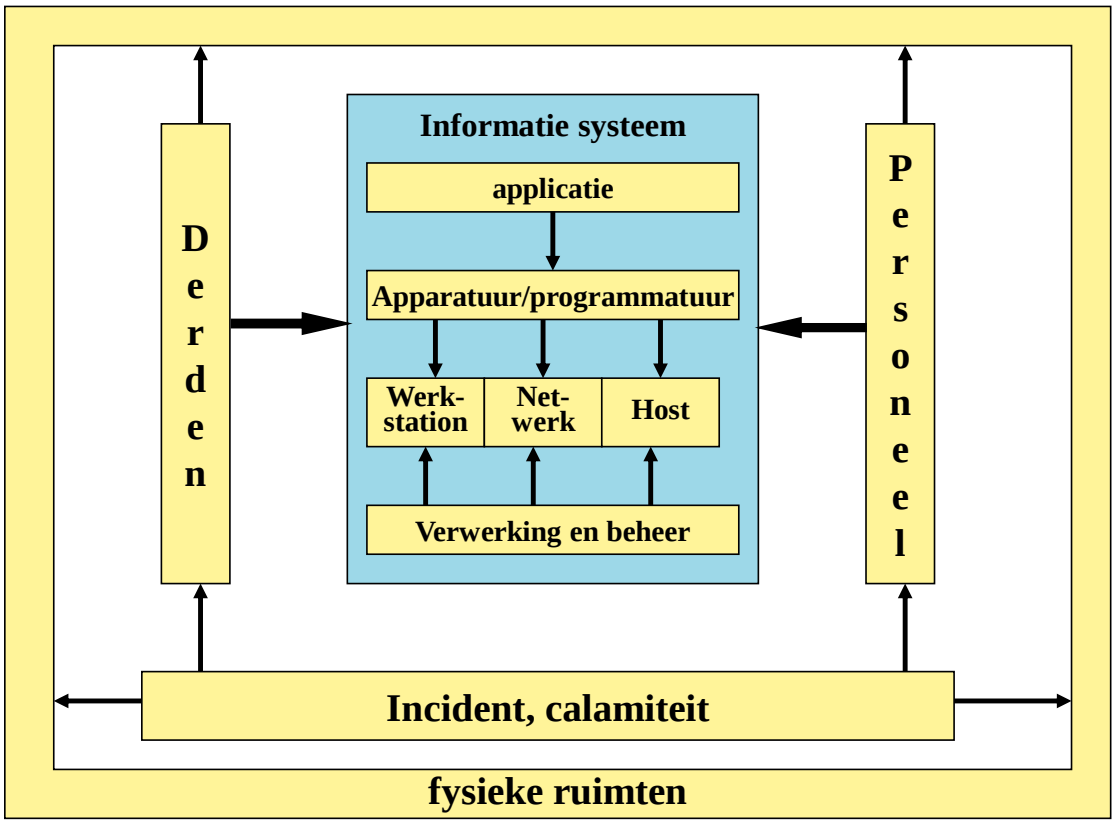
Dit document is een uitwerking van alle maatregelen, afspraken en sancties die tot doel hebben de veiligheid en de vertrouwelijkheid van informatie – voor zover vereist en relevant – te waarborgen.
De scope van het hier beschreven informatiebeveiligingsbeleid is het beveiligen van de informatie die zich op ICT-systemen bevindt en de informatie die via de ICT-systemen en de daaraan gekoppelde verbindingen te benaderen is.
De klanten van Techni Team ICT BV zijn en blijven eindverantwoordelijk voor de beveiliging van de gegevens die zij ter verwerking deelt met Techni Team ICT BV. Techni Team ICT BV is verantwoordelijk voor het beschikbaar stellen van haar diensten met voldoende beveiligingsopties, zodat haar klanten kunnen voldoen aan de geldende IB-normen en andere wet- en regelgeving. Zij is verwerker in de zin van de AVG (GDPR).
Elk bedrijfsmiddel, informatiesysteem en daarbij behorende gegevens, heeft een eigenaar. Tenzij anders vermeld, is de Manager Team Beheer eigenaar van elk van de assets/informatiesystemen.
De benoemde eigenaar is verantwoordelijk voor het betreffende systeem, inclusief;

- Het bepalen van de bij het systeem te onderkennen risico's,
- Het classificeren van het systeem en de daarbij behorende gegevens, en;
- Het (laten) ontwikkelen van adequate beveiligingsmiddelen en interne controlemaatregelen.

Naast de applicatie zelf betreft dit ook;

- De juiste inzet van de infrastructurele componenten (werkstations, servers en het interne en externe netwerk),
- De juiste verwerking,
- Het adequate beheer,
- Het goed functioneren van het personeel,
- Het maken van afspraken met derden,
- Fysieke beveiliging en
- Voorzieningen om incidenten en calamiteiten te voorkomen of af te handelen.

In onderstaand figuur zijn alle genoemde deelgebieden van een informatiesysteem opgenomen:



We gebruiken de term eindverantwoordelijk, omdat een aantal aspecten van het informatiesysteem uitbesteedt worden aan sub bewerkers. We streven daarbij nadrukkelijk een maximaal beveiligingsniveau na, binnen de context van beheerste risico's, beheerste kosten en flexibiliteit.

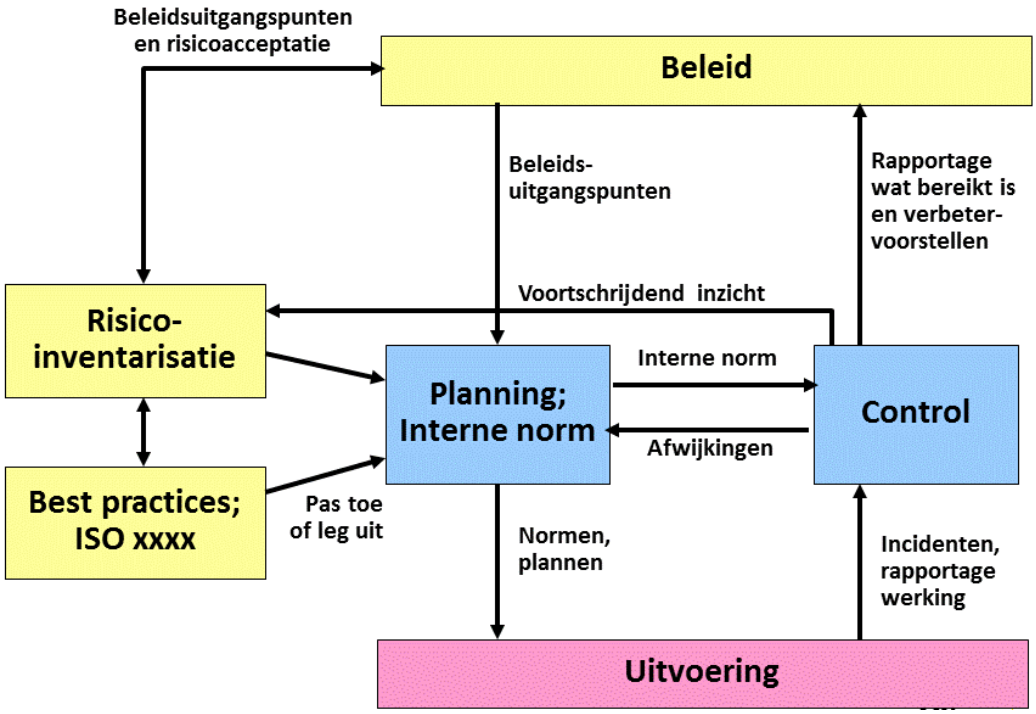
4.2 Uitwerking en naleving

Dit Informatiebeveiligingsbeleid vormt met de jaarlijkse risicoanalyse de basis voor een set van maatregelen en control, gezamenlijk gedefinieerd als het basisbeveiligingsniveau, zoals vastgelegd in het ISMS. Dit geldt als minimum voor de dienstverlening. Op verzoek van stakeholders kan ook een hoger niveau van beveiliging worden overeengekomen, na vastlegging in wijzigingsprocedure en overeenkomsten.

4.3 Controle werking en naleving van het beleid

Eens per kwartaal wordt de werking en de naleving van het beleid intern geëvalueerd in het kwartaaloverleg informatiebeveiliging. Vaste onderdelen van dit overleg zijn

- Doorlopen mogelijke veranderingen risico's
- Check voortgang verbeterplan
- Periodieke beoordeling uitvoering operationele planning
- Beoordeling of beheersmaatregelen nog kloppen.
- Voortgang interne audits


Beleidsuitgangspunten
en risicoacceptatie
Beleid
Beleids-
uitgangspunten
Rapportage
wat bereikt is
en verbeter-
voorstellen
Voortschrijdend inzicht
Risico-
inventarisatie
Planning;
Interne norm
Interne norm
Control
Afwijkingen
Best practices;
ISO xxxx
Pas toe
of leg uit
Normen,
plannen
Incidenten,
rapportage
werking
Uitvoering

5. Verantwoording

Dit hoofdstuk beschrijft de uitgangspunten die Techni Team ICT BV hanteert bij het opstellen en handhaven van een informatiebeveiligingsbeleid.

5.1 Statement

Techni Team ICT BV voert een expliciet en daadkrachtig beleid voor de beveiliging van de informatie die in informatiesystemen wordt beheerd.
De informatiebeveiliging is daarbij geen doel op zich, maar dient uitsluitend het belang van Techni Team ICT BV, haar opdrachtgevers en diens cliënten/relaties. De continuïteit, kwaliteit en vertrouwelijkheid van bedrijfsprocessen staan centraal, evenals respect voor de privacy van alle betrokkenen. De uitgangspunten en organisatie zijn vastgelegd en worden gedragen door de directie en, afgeleid daarvan, door de hele organisatie. Er worden enerzijds duidelijke keuzes gemaakt in beveiligingsmaatregelen, en anderzijds wordt de toepassing daarvan ook gecontroleerd ter verbetering van zowel beleid als uitvoering.

5.2 Uitgangspunten

De beveiliging dient in ieder geval te voldoen aan de eisen van:

- de Algemene Verordening Gegevensbescherming of General Data Protection Regulation (AVG/GDPR).
- de “Wet Computercriminaliteit” (vernieuwd: 1 september 2006) (ref: 5)
- de Telecommunicatiewet (1998, diverse aanpassingen sindsdien) (ref: 6).
- De stakeholders (belanghebbenden)

De contacten met deze organisaties (AP, BIT, RoutIT) worden onderhouden door de directie. Jaarlijks wordt bij RoutIT een informatie-event gehouden die door verschillende medewerkers wordt bezocht. Rondom de AVG worden we op de hoogte gehouden door de nieuwsbrief van Duthler Associaties. Zij hebben ook jaarlijks een event.
Verder zal de beveiliging continu worden geactualiseerd naar de geldende juridische eisen op zowel landelijk als Europees niveau.
De beveiliging wordt dusdanig ingericht dat in elk geval de volgende aspecten gewaarborgd worden:

- **Beschikbaarheid**: informatie en systemen zijn beschikbaar wanneer ze nodig zijn en voldoen aan de eisen die gesteld worden.
- **Integriteit**: informatie (verwerking) is volledig, juist en tijdig
- **Vertrouwelijkheid**: informatie en systemen zijn alleen toegankelijk voor hen die daartoe geautoriseerd zijn

Bij opzettelijke schendingen van beveiligingsmaatregelen volgen in alle gevallen disciplinaire maatregelen – zie het hoofdstuk over Sancties.
Het informatie beveiliging beleid zal jaarlijks geëvalueerd worden en indien noodzakelijk aangepast.

5.3 Algemene Verordening Gegevensbescherming (AVG)

De AVG geeft regels voor een zorgvuldige omgang met persoonsgegevens. Vanaf mei 2018 is deze van kracht. De wet geeft aan wat de rechten zijn van iemand van wie gegevens worden gebruikt en wat de plichten zijn van de instanties of bedrijven die deze gegevens gebruiken. Ook worden eisen gesteld aan de verwerking van persoonsgegevens.
Een organisatie:

- mag persoonsgegevens alleen verzamelen en verwerken als daar een goede reden voor is (gerechtvaardigd doel), of als de betrokken burger toestemming heeft gegeven voor het gebruik van zijn gegevens.

- mag niet meer gegevens verwerken dan strikt noodzakelijk is voor het doel waarvoor ze zijn verzameld
- mag de gegevens niet langer bewaren dan noodzakelijk,
- moet passende technische en organisatorische maatregelen treffen om de gegevens te beschermen
- moet de verwerking in veel gevallen melden (zie hieronder)
- moet de betrokken burger in principe altijd informeren over de gegevensverwerking

Het Autoriteit Persoonsgegevens (AP) controleert zo nodig of bedrijven en instanties zich aan de AVG houden.

5.4 Wet Computercriminaliteit

Onder computercriminaliteit wordt vaak verstaan: misdrijven die met een computer gepleegd worden, waarbij het gebruik van ICT een wezenlijke rol speelt bij het misdrijf. In het Wetboek van strafrecht (Sr) (ref: 5) zijn vele artikelen opgenomen met betrekking tot computercriminaliteit. Hieronder vallen: vernieling en onbruikbaar maken, aftappen van gegevens, denial-of-service (verstikkingsaanval), computervredebreuk, diensten afnemen zonder betalen en zogenoemde malware (kwaadaardige software). Artikel 138a lid 1 Sr gaat specifieker in op het onderwerp computervredebreuk. Hierin worden genoemd: het doorbreken van een beveiliging, gebruik maken van een technische ingreep, valse signalen of een valse sleutel en het aannemen van een valse hoedanigheid als voorbeelden van computervredebreuk. Deze categorieën zijn niet bedoeld als volledige taxonomie, er kan best overlap tussen zitten.

5.5 Telecommunicatiewet

De Telecommunicatiewet (ref: 6) heeft als doel het beschermen van de rechten van de burger betreffende elke vorm van digitale communicatie. Allereerst mogen aanbieders van elektronische communicatienetwerken en/of –diensten informatie die voor of tijdens onderhandelingen of uitvoeren van een overeenkomst aan hen is verstrekt, uitsluitend gebruiken voor het doel waarvoor deze informatie is verstrekt (volgens artikel 6.1 lid 2 van de Telecommunicatiewet). De verkregen of opgeslagen informatie wordt vertrouwelijk behandeld en wordt niet doorgegeven aan andere partijen.

In artikel 11.2 van de Telecomwet wordt beschreven dat de aanbieders in het belang van de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers, passende technische en organisatorische maatregelen moeten nemen ten behoeve van de veiligheid en beveiliging van de door hen aangeboden netwerken en diensten. Abonnees moeten hierover worden geïnformeerd. Daarbij dient vermeld te worden welke risico's het bedrijf eventueel kan lopen en hoe deze worden tegengegaan. Wanneer een aanbieder een abonneelijst uitgeeft of een abonnee-informatiedienst verzorgt, moet hij de abonnee voor opname van de persoonsgegevens in de lijst op de hoogte stellen van de doeleinden van deze abonneelijst en/of de desbetreffende abonnee-informatiedienst.

In de abonneelijst en het abonneebestand van de aanbieder worden uitsluitend persoonsgegevens van een abonnee opgenomen als de abonnee daarvoor toestemming heeft verleend. Aan het niet opgenomen zijn in een abonneelijst mogen geen kosten worden verbonden.
De abonnee heeft het recht om kosteloos de betreffende persoonsgegevens in een abonneelijst te verifiëren, te laten verbeteren of te laten verwijderen.

5.6 Beleidsuitgangspunten informatiebeveiliging

Aan de hand van de context van de organisatie en de risico's die Techni Team ICT BV heeft geïnventariseerd zijn beleidsuitgangspunten geformuleerd. Hierin geeft de directie aan, op welke wijze zij wil dat de informatiebeveiliging passend vorm gegeven wordt bij Techni Team ICT BV.
In de bijlage staat de verwijzing naar de documenten waarin de beleidsuitgangspunten zijn uitgewerkt.

Deze beleidsuitgangspunten gelden voor die gegevensbewerkingen, waarvoor Techni Team ICT BV wettelijk en/of contractueel verantwoordelijk is.

Beleidsuitgangspunt
I. Techni Team ICT BV is gehouden aan haar Informatiebeveiligingsbeleid
II. Rollen en verantwoordelijkheden Informatiebeveiligingsbeleid zijn gedefinieerd
III. Toepassingsgebied Informatiebeveiligingsbeleid is gebaseerd op strategie van Techni Team ICT BV, risico's en eisen stakeholders en wetgeving. En op vertrouwen.
IV. Nieuwe projecten en veranderingen
V. Omgaan met incidenten
VI. Toepassen van de logische beveiligingsprincipes
VII. Plan do check adjust: lerende organisatie
VIII. Planning en naleving I.B. geborgd
IX. Directie is en blijft eindverantwoordelijk
X. Actieve monitoring naleving Informatiebeveiligingsbeleid en sancties

6. Organisatie en bewustwording

Dit hoofdstuk beschrijft de organisatie van Techni Team ICT BV voor zover relevant voor het informatiebeveiligingsbeleid.
De uitwerking van de organisatie rond informatiebeveiliging is gerelateerd aan de gekozen scope van het hier uitgewerkte beveiligingsbeleid. Deze is, dat naar die informatie wordt gekeken welke via ICT-systemen beschikbaar moet zijn voor de primaire en secundaire processen van Techni Team ICT BV. Belangrijk daarbij is het bewust zijn van de gebruikers van de systemen dat zij voor de continuïteit van deze processen qua beveiliging een cruciale rol spelen.

6.1 Organisatie

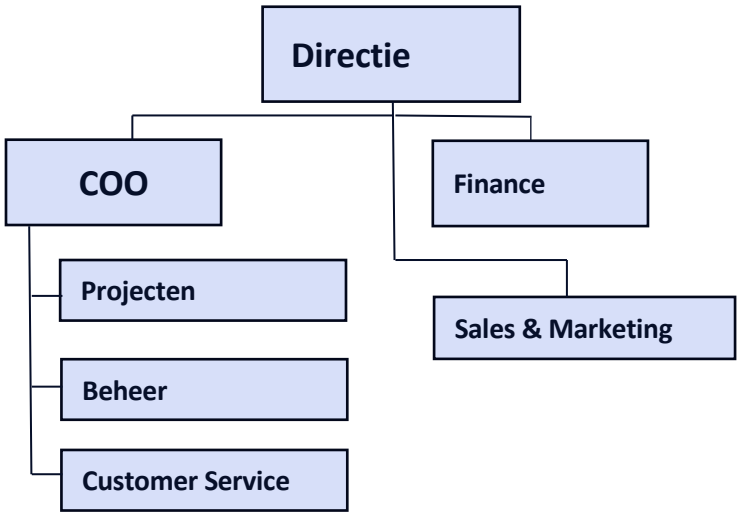
Techni Team ICT BV is georganiseerd in 5 afdelingen:

- Sales & Marketing
- Projecten
- Beheer
- Customer Service
- Finance

De directie is direct verantwoordelijk voor Sales & Marketing en Finance.
De COO is verantwoordelijk voor Beheer, Projecten en Customer Services. Het zijn vooral de afdelingen Beheer en Projecten waarop ISO2700 en NEN7510 van toepassing zijn.

In de zorg is NEN7510 steeds vaker een voorwaarde voor relaties en dat daarom is gekozen om de werkwijze te laten auditen. Daarnaast behoort een certificaat en de daarbij behorende auditing bij de ambitie van de directie om een eerste klasse speler in de eerstelijnsgezondheidszorg te zijn. Daarbij is gekozen voor een inrichting die past bij de omvang van de organisatie en het volwassenheidsstadium waarin die zich bevindt.

Techni Team ICT organisatie



6.2 Taken en bevoegdheden

De directie van Techni Team ICT BV is eindverantwoordelijk voor de vaststelling en het wijzigen van het informatiebeveiligingsbeleid.

De directeur is verantwoordelijk voor de uitvoering en handhaving van de technische aspecten van het beleid.
De directeur laat een technische risicoanalyse uitvoeren door technisch specialisten van Techni Team ICT BV.
De directeur is eveneens verantwoordelijk voor uitvoering en handhaving van alle andere aspecten.
De directie kan besluiten door een externe organisatie een audit uit te laten voeren.

6.3 Bewustwording

Het handhaven van maatregelen en het realiseren van de doelstellingen om informatie correct te beveiligen en beheren, staat of valt met de inzet en goede wil van alle betrokkenen. De directie zal daarom een actief beleid voeren om medewerkers, bezoekers, leveranciers en anderen die met Techni Team ICT BV en haar producten/diensten in aanraking komen, bewust te maken van de vertrouwelijkheid van de beheerde informatie.

Belangrijkste middel voor het kweken van bewustwording is communicatie. In bilateraal overleg en in afdelingsoverleg zullen medewerkers geïnformeerd worden. Bij aanname van nieuw personeel zal de vertrouwelijkheid van de beheerde informatie expliciet besproken worden.
Leveranciers en partners zullen nadrukkelijk gewezen worden op hun verplichtingen inzake geheimhouding en vertrouwelijkheid, hetgeen ook contractueel vastgelegd zal worden in overeenkomsten.
Bezoekers worden middels een gedragscode geïnformeerd bij binnenkomst.

7. Risico analyse

Dit hoofdstuk beschrijft de risico's op informatieverlies vanuit verschillende invalshoeken.
Risico's voor verlies van informatie en/of schending van vertrouwelijkheid is op te delen in verschillende categorieën, waarvoor een verschillende benadering vereist is:

- vanuit de interne organisatie
- via openbare netwerken
- via leveranciers
- via bezoekers
- via klanten

7.1 Vanuit de interne organisatie

Medewerkers van Techni Team ICT BV, in vast dienstverband of ingeleend, hebben door hun kennis te allen tijde de mogelijkheid om inzage te verkrijgen in alle technische informatie welke door Techni Team ICT BV beheerd wordt. Tevens is deze mogelijkheid een vereiste om hun werkzaamheden als "een goed huisvader" te kunnen uitvoeren. Dit is derhalve een onvermijdbare situatie.
Slordig gebruik van ter beschikking gestelde middelen, diefstal of het laten slingeren of achterlaten van computerapparatuur en/of informatiedragers kan leiden tot onbedoeld verlies van informatie. Hiervan zijn in het algemeen voldoende voorbeelden bekend.

7.2 Via openbare en/of besloten netwerken

Zie het document dat handelt over de technische architectuur.

7.3 Leveranciers

Wat gesteld is in paragraaf 4.2 m.b.t. personeel, geldt in veel gevallen evenzo voor leveranciers van diensten en partners waarmee wordt samengewerkt. Voor leveranciers van materialen is het risico nihil.

7.4 Bezoekers

Reguliere bezoekers van Techni Team ICT BV en de Techni Team ICT BV datacenters, kunnen met en door hun aanwezigheid onbedoeld inzage krijgen in informatie. Tevens kunnen bezoekers in de gelegenheid komen informatie te ontvreemden.
Dat laatste is zeker het geval indien ongewenste bezoekers in een pand weten binnen te dringen, zowel binnen als ook buiten kantoortijd.

7.5 Klanten

Het onkundig gebruik van de ICT middelen zou kunnen leiden tot verlies of beschadiging van informatie. Daarom worden ook klanten bewust gemaakt van de gevaren hiervan en de manier om deze risico's te vermijden.

8. Maatregelen en sancties

Het doel van informatiebeveiliging binnen Techni Team ICT BV is om te allen tijde een adequate set van maatregelen te hebben getroffen om de risico's die de hiervoor genoemde risicobronnen met zich meebrengen te beperken c.q. de gevolgschade te beperken.

8.1 Interne Organisatie

Voorafgaand aan de indiensttreding vindt een zorgvuldige screening van de kandidaat plaats. Een voorwaarde om bij werkgever in dienst te kunnen treden en blijven is het zijn van onbesproken gedrag. Werknemer heeft verklaard van onbesproken gedrag te zijn op het gebied van databeveiliging. Voor de datum indiensttreding overlegt werknemer aan werkgever een Verklaring Omtrent Gedrag (VOG), gericht op functieaspecten 11, 12 en 13. Deze verklaring mag op datum indiensttreding niet ouder zijn dan zes maanden. De arbeidsovereenkomst komt eerst tot stand nadat werknemer de VOG heeft overlegd (opschortende voorwaarde). Werknemer zal op verzoek van werkgever iedere drie jaar opnieuw een VOG overleggen. Het niet kunnen overleggen van een geldige VOG maakt werknemer ongeschikt voor het uitoefenen van zijn functie en vormt een grond voor ontbinding.

Alle medewerkers zijn bekend gemaakt met het informatiebeveiligingsbeleid en ook met de risico's die hun positie en functie met zich mee brengt. De plicht tot geheimhouding en bewaren van de vertrouwelijkheid worden vastgelegd en gesanctioneerd in de arbeidsovereenkomst en RAA (incl. geheimhoudingsverklaring). Individuele medewerkers wordt gevraagd deze te ondertekenen. Elke medewerker krijgt bij aanvang van het dienstverband een presentatie van het interne informatiebeveiligingsbeleid.

Apparatuur die medewerkers gebruiken t.b.v. een goede functie-uitoefening zal ten allen tijde verstrekt worden door Techni Team ICT BV. BYOD (Bring Your Own Device) is toegestaan maar is wel onder strikte voorwaarden (zie document 15 "Beheer bedrijfsmiddelen").

Datadragers die het eigendom zijn Techni Team ICT BV zullen extra worden beveiligd middels encryptie.

Iedere medewerker krijgt unieke gebruikersidentificaties zodat hij/zij kan worden gekoppeld aan en verantwoordelijk kan worden gesteld voor de uitgevoerde acties. Alle handelingen van iedere medewerker worden in logfiles vastgelegd, welke onder alle omstandigheden geraadpleegd kunnen worden. Het gebruik van groepsidentificaties is alleen toegelaten als deze om bedrijfs- of operationele redenen noodzakelijk zijn. Dit moet worden goedgekeurd en gedocumenteerd.

Bij beëindiging van dienstverband wordt de gebruikersidentificatie van de betreffende medewerker onmiddellijk ongeldig gemaakt.

Informatie wordt fysiek beheerd in datacenters. Deze datacenters worden in dit verband gezien als een interne organisatie. Voor het informatie beveiligingsbeleid van de datacenters wordt verwezen naar de beleidsstukken van de betreffende datacenters.

Medewerkers dienen hun gereedschappen die zij ter beschikking krijgen gesteld als "een goed huisvader" te beheren. Dat wil zeggen dat zij hun middelen niet onbeheerd c.q. uit hun directe toezicht mogen verliezen en dus deze niet mogen achterlaten in hun auto. Indien deze situaties niet te vermijden zijn, dan dient de gebruiker compleet uit te loggen, zodat geen ongewenste toegang via de middelen mogelijk is.

De door Techni Team ICT BV ter beschikking gestelde middelen mogen niet worden gebruikt voor privé doeleinden of voor andere bezigheden die niet tot de Techni Team ICT BV-activiteiten behoren.

Wanneer een medewerker zijn/haar werkplek voor kortere of langere tijd verlaat, dient de pc of laptop te allen tijde vergrendeld te worden. Hierbij inbegrepen is niet alleen de interne werkplek, maar ook een externe

werkplek, hetzij bij een klant of leverancier, hetzij een thuiswerkplek. Dit vergrendelen geschiedt door het indrukken van de volgende toets combinatie:  +L (Windowstoets + L)

Sancties
De plicht tot geheimhouding is vastgelegd in de arbeidsovereenkomst. Een schending van deze plicht is gesanctioneerd met een boete van € 2.500 per gebeurtenis, vermeerderd met € 500 voor elke dag dat de overtreding voortduurt.

Indien geconstateerd wordt dat een medewerker onzorgvuldig omgaat met de regels zal de betreffende medewerker hierop worden aangesproken in een functioneringsgesprek, wat direct na het constateren zal plaatsvinden. De inhoud van het gesprek zal in het personeelsdossier worden vastgelegd. Een eerste overtreding wordt vastgelegd als een waarschuwing. Een tweede als een laatste waarschuwing. Na een derde constatering zal het dienstverband worden beëindigd op grond van herhaaldelijke weigeren van het opvolgen van bedrijfsvoorschriften in het kader van het informatiebeveiligingsbeleid.

Indien er sprake is van een bewuste, al of niet geslaagde poging, informatie te verspreiden of aan derden ter beschikking te stellen, zal dit in beginsel worden gezien als een strafbaar feit en zal aangifte worden gedaan.

Bewustwording
Alle medewerkers worden middels een intake op de hoogte gebracht van het Techni Team ICT BV informatie beveiligingsbeleid. Tijdens deze intake wordt het volledige beleid doorgenomen met nadruk op de positie en de plichten van de individuele medewerker bij het handhaven en uitvoeren van de maatregelen.

Tijdens het wekelijks MT is het informatiebeveiligingsbeleid een vast agendaonderdeel. Daarbij worden volgende onderwerpen besproken:

- Incidenten in de afgelopen week
- Wijzigingen in het IBB
- Ervaringen medewerkers en voorstellen voor verbetering
- Algemene evaluatie

8.2 Openbare en/of besloten netwerken

Zie het document dat handelt over de technische architectuur (ref: 7).

8.3 Leveranciers

Voor leveranciers van materialen worden geen maatregelen genomen. Voor samenwerking met leveranciers van diensten is een betreffende overeenkomst opgesteld, welke voorafgaand aan iedere vorm van samenwerking door beide partijen ondertekend dient te worden en waarin geheimhouding en vertrouwelijkheid wordt geregeld.
Aanvullend daarop zullen individuele medewerkers gevraagd worden een geheimhoudingsovereenkomst te ondertekenen, indien zij in verband met de door hen uitgevoerde werkzaamheden inzage kunnen verkrijgen in vertrouwelijke informatie.

Sancties
Beide overeenkomsten zijn passend gesanctioneerd. Voor het bedrijf is een boete vastgesteld per overtreding van € 100.000, te vermeerderen met € 2.000 voor elke dag dat de overtreding voortduurt.
Voor medewerkers van leveranciers en partners geldt een boete van € 2.500 per gebeurtenis, te vermeerderen met € 500 voor elke dag dat de overtreding voortduurt.

8.4 Bezoekers

Toegang tot het pand is geregeld middels een toegangsautorisatiesysteem. Bezoekers kunnen het pand alleen betreden nadat zij zich gemeld hebben via de receptie. Bij de aanmelding dient de bezoeker zich te legitimeren, worden aankomsttijd en ontvangende medewerker genoteerd. Er wordt geen identificatie (zoals ID, paspoort of rijbewijs) van de bezoeker genoteerd. Bij vertrek wordt de vertrektijd genoteerd.

Medewerkers dienen erop toe te zien dat bezoek zich alleen onder begeleiding in het pand bevindt. Zonder toestemming van de directie hebben bezoekers geen toegang tot de werkruimtes.

Leveranciers van materialen hebben alleen toegang tot de afleverlocatie goederen en worden niet als bezoekers gezien.
Buiten kantooruren is het pand gesloten en met een alarmsysteem met doormelding aanvullend beveiligd. Inbraak is echter niet te voorkomen, daarom dienen medewerkers bij het verlaten van het pand op systemen uit te loggen en alarmsystemen in te schakelen. Beveiliging tegen informatie verlies in een dergelijke situatie is gelijk beschreven in paragraaf 5.3.

Voor bezoekers in de datacenters wordt verwezen naar het beleid van de datacenters.

Gedragscode bezoekers
Bezoekers worden bij binnenkomst en registratie op de hoogte gesteld dat zij zich dienen te houden aan de door Techni Team ICT BV ingestelde gedragscode. Deze luidt als volgt:

> *Bezoeker dient zich ervan bewust te zijn dat Techni Team ICT BV onder andere werkzaam is voor de Zorgsector. Daardoor kan er gewerkt worden met vertrouwelijke informatie.*
> *De bezoeker wordt geacht te verblijven in de voor de afspraak aangewezen ruimte en zich ongevraagd geen toegang te verschaffen tot enig andere ruimte. Tevens is het de bezoeker niet toegestaan pogingen te ondernemen om via een computersysteem of via het netwerk van Techni Team ICT BV toegang te verkrijgen tot internet, data of programmatuur.*

Sancties
Bij constatering van enige overtreding van de regels zal de bezoeker direct de toegang tot het pand worden ontzegd, c.q. uit het pand worden verwijderd.
Indien er sprake is van een bewuste, al of niet geslaagde poging, informatie te ontvreemden, zal dit in beginsel worden gezien als een strafbaar feit en zal aangifte worden gedaan.

8.5 Klanten

Middels nieuwsbrieven en email-updates worden klanten bewust gemaakt van de gevaren van onkundig gebruik van ICT middelen. Om dit te onderstrepen en om te voldoen aan de vigerende regelgeving wordt met klanten een zogenaamde bewerkers- of verwerkersovereenkomst gesloten.

9. Rapportage en evaluatie

Ieder kwartaal wordt de directie geïnformeerd welke incidenten zich hebben voorgedaan ter aanzien van het informatie beveiligingsbeleid. Incidenten met een hoge impact worden direct bij de directie gemeld.
Jaarlijks zal het informatie beveiligingsbeleid geëvalueerd worden om naleving en effectiviteit van het beleid te toetsen.

9.1 Rapportage

Incidenten worden direct na constateren vastgelegd in het interne ERP-systeem (EBS) van Techni Team ICT BV. In dit systeem worden incidenten geclassificeerd voor het verzamelen van statistische data. Ieder moment is online een rapportage opvraagbaar welke incidenten in een bepaalde periode hebben plaatsgevonden, in welke klasse deze vallen en welke maatregelen zijn genomen op elk geconstateerd incident.
Incidenten worden in drie categorieën verdeeld:

1. **Beschikbaarheid**: De mate waarin een informatiesysteem in bedrijf is op het moment dat de organisatie het nodig heeft.
2. **Integriteit**: De mate waarin een informatiesysteem zonder fouten is.
3. **Vertrouwelijkheid**: De mate waarin toegang tot en de kennisname van een informatiesysteem en de informatie daarin is beperkt tot een gedefinieerde groep van gerechtigden.

9.2 Technische evaluatie

Jaarlijks wordt in het vierde kwartaal een risicoscan uitgevoerd door een van de technisch specialisten van Techni Team ICT BV. De technische directie van Techni Team ICT BV heeft de verantwoording over deze actie. Uit deze scan moet naar voren komen in hoeverre de technische systemen afdoende afgeschermd zijn voor pogingen het systeem te benaderen (indringerstest). Indien hieruit blijkt dat het onvoldoende is, zullen per direct aanvullende maatregelen genomen worden.
De directie kan eveneens besluiten de scan door een externe specialist te laten uitvoeren indien zij daartoe aanleiding denkt te hebben.
Van de scan wordt een rapport gemaakt met beschrijving werkwijze, bevindingen en eventuele aanbevelingen.

9.3 Algemene evaluatie

Jaarlijks wordt in vierde kwartaal een evaluatie gedaan op het informatie beveiligingsbeleid. Evaluatie vindt o.a. plaats op basis van de interne norm en onze beleidsuitgangspunten.

Input voor de evaluatie zijn rapportages op basis van ondermeer de informatiebeveiligingsincidenten, de interne audits en het auditplan, de resultaten van de risicoanalyse en de bijbehorende verbeterplannen, de resultaten van de technische evaluatie.
Voor deze meeting is een standaard agenda (TechniTeam Agenda Directiebeoordeling 1.3)

De directie laat zich informeren door de Security Officer (sinds 2018 een combinatie van de directiebeoordeling en de managementreview.
Te beoordelen zijn de effectiviteit en mate van naleving van het informatie beveiligingsbeleid. Er wordt rapportage opgesteld van de bevindingen en er worden aanbevelingen gedaan voor eventuele verbeteringen.

Bijlage 1: Overzicht beleidsuitgangspunten en de uitwerking in beleidsstukken en registraties

NR	Beleidsuitgangspunt	Document referentie	ISO27001/ NEN7510
I	**Techni Team ICT BV is gehouden aan haar Informatiebeveiligingsbeleid**	• *Risicobeoordelingen behandelmethodiek* • *Informatiebeveiligingsbeleid* • *Directiebeoordeling*	*A.5.1* *A6.1*
II	**Rollen en verantwoordelijkheden werking Informatiebeveiligingsbeleid zijn gedefinieerd**	• *Interne organisatie I.B. en competenties Informatiebeveiliging* • *Directiebeoordeling*	*A.6.1.2* *A.6.1.3*
III	**Toepassingsgebied Informatiebeveiligingsbeleid is gebaseerd op de strategie van Techni Team ICT BV, haar risico's en eisen stakeholders en wetgeving. En op vertrouwen.**	• Risicobeoordelingen behandelmethodiek • Stakeholderanalyse • Wetgeving en contracten • Interne Norm	*A.12* *A.14* *A.18*
IV	**Nieuwe projecten en veranderingen worden gecontroleerd uitgevoerd**	• Changemanagement • Incidentmanagement	*A.6* *A.12* *A.14*
V	**Omgaan met incidenten volgens protocollen**	• Informatiebeveiligingsbeleid • Changemanagement • Incidentmanagement • Continuïteitsplan	*A.16*
VI	**Toepassen van logische beveiligingsprincipes: niet hebben, scheiden en niet slepen**	• Documentbeheer • Beheer middelen • Toegangsbeheer en authenticatie • Beheer bedrijfsmiddelen	*Hs 4-10*
VII	**Plan do check adjust: continue verbetering en een lerende organisatie**	• Verbeterplan • Operationele planning • Directiebeoordeling • Auditplan	*HS 4-10*
VIII	**Planning, inrichting en naleving I.B. geborgd**	• Interne organisatie Informatiebeveiliging en competenties sleutelmedewerkers	*A.6.1.4*
IX	**Directie is en blijft eindverantwoordelijk**	• Informatiebeveiligingsbeleid • Directiebeoordeling	*A.7*
X	**Actieve monitoring naleving Informatiebeveiligingsbeleid en sancties**	• Ethische code • Awareness training • Communicatieplan • Uitbestedingsbeleid • Continuïteitsbeheer • Arbeidsovereenkomst en geheimhoudingsverklaring • Opname in functioneringsgesprekken	*A.6.2* *A7.*