Informatiebeveiligingsbeleid

Stichting Werken in Gelderland

Versiebeheer

Eigenaar: **Review:**	Bestuur juni 2019			
Versie	**Status**	**Aangepast**	**Datum**	**Door**
0.1	Concept	Versiebeheer	31-5-2018	Privacyzaken, Michel Rijnders
1.0	Vastgesteld	Vastgesteld	8-6-2018	Bestuur

Inleiding

Aangesloten werkgevers bij Stichting Werken in Gelderland laten hun gegevens in vertrouwen verwerken door (aangeboden oplossingen van) Werken in Gelderland. Zij zijn voor een deel van hun bedrijfsvoering afhankelijk van hoe Werken in Gelderland met de beveiliging van informatie omgaat. Daarnaast is Werken in Gelderland verantwoordelijk voor de verwerking van Persoonsgegevens.

Voor Werken in Gelderland is een adequate beveiliging van informatie van essentieel belang om aan de toenemende (beveiligings)behoefte van aangesloten werkgevers te kunnen voldoen en voor de continuïteit van de bedrijfsvoering van Werken in Gelderland.

Vereisten vanuit wet- en regelgeving en bedreigingen voor de informatievoorziening maken het noodzakelijk om gerichte maatregelen te treffen om de risico's tot een aanvaardbaar niveau te reduceren. Daarbij rekening houdend met behoeften en doelstellingen van de organisatie, de beveiligingseisen, de procedures die de organisatie toepast en de omvang en structuur van de organisatie.

Dit document is het uitgangspunt van Werken in Gelderland voor het formuleren van dit informatiebeveiligingsbeleid.

Het bestuur van Stichting Werken in Gelderland is verantwoordelijk voor dit informatiebeveiligingsbeleid. Dit beleid wordt jaarlijks beoordeeld, herzien en vastgesteld door het bestuur zodat het passend is en blijft voor Werken in Gelderland en de aangesloten werkgevers.

Definitie informatiebeveiliging

Informatiebeveiliging wordt als volgt gedefinieerd:
Het samenhangend stelsel van maatregelen dat zich richt op het blijvend realiseren van een optimaal niveau van beschikbaarheid, integriteit en vertrouwelijkheid van informatie en informatiesystemen.

Werken in Gelderland stelt zich met het informatiebeveiligingsbeleid specifiek tot doel om passende technische en organisatorische maatregelen te nemen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen zullen passend zijn, rekening houdend met de stand van de techniek en de kosten die ermee gemoeid zijn en zullen er mede op gericht zijn onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

Werkingsgebied

De werkgever is en blijft verantwoordelijk voor de beveiliging van de gegevens die zij ter verwerking deelt met Poolz. Werken in Gelderland is verantwoordelijk voor het beschikbaar stellen van haar diensten met voldoende beveiligingsopties, zodat haar klanten kunnen voldoen aan de geldende Informatiebeveiligingsnormen en andere wet- en regelgeving. Werken in Gelderland is tevens

verantwoordelijk voor adequate beveiliging van de gegevens die zij als Verwerkingsverantwoordelijke verwerkt.

Het informatiebeveiligingsbeleid is van toepassing op de gehele organisatie van Werken in Gelderland en alle informatie verwerkt wordt. Het informatiebeveiligingsbeleid is ook van toepassing op de gegevensuitwisseling met andere organisaties. Het beleid richt zich op onze eigen medewerkers, tijdelijk personeel en op personeel dat door derden wordt ingezet om diensten te verlenen aan onze organisatie. Deze worden gehouden aan de naleving.

Werken in Gelderland legt in overeenkomsten met klanten (aangesloten werkgevers) vast welke informatieverwerkingen op welke wijze plaatsvinden. Werken in Gelderland neemt de verantwoordelijkheid om medewerkers en haar leveranciers aan dezelfde afspraken te houden.

Uitwerking en naleving

Dit Informatiebeveiligingsbeleid vormt met de periodieke risicoanalyses de basis voor een set van maatregelen. Dit geldt als minimum voor de dienstverlening aan klanten. Op verzoek van klanten kan ook een hoger niveau van beveiliging worden overeengekomen, na vastlegging in SLA en wijzigingsprocedure.

Controle werking en naleving van het beleid

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

- Doorlopen mogelijke veranderingen risico’s
- Check voortgang verbeterplan
- Periodieke beoordeling uitvoering operationele planning
- Algemene passendheid van de beheersmaatregelen

Beleidsuitgangspunten informatiebeveiliging

Aan de hand van de context van de organisatie en de risico’s die Werken in Gelderland heeft geïnventariseerd zijn beleidsuitgangspunten geformuleerd. Hierin geeft het bestuur aan, op welke wijze zij wil dat de informatiebeveiliging passend vorm wordt gegeven bij Werken in Gelderland.

Verwijzing naar de documenten waarin de beleidsuitgangspunten zijn uitgewerkt staan in het overzicht opgenomen.

Nr	Beleidsuitgangspunt	Beschrijving	Documenten
1	**Werken in Gelderland is gehouden aan haar Informatiebeveiligingsbeleid**	De veilige omgang met gegevens van klanten is van kritiek belang voor de dienstverlening en voortbestaan van Werken in Gelderland, 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 het bestuur, die deze afweging maakt en verifieert op passendheid op strategisch niveau door de risicoanalyse.	● Risicobeheersing ● Informatiebeveiligings beleid
2	**Toepassingsgebied Informatiebeveiligingsbeleid is gebaseerd op strategie Werken in Gelderland, risico's en eisen stakeholders en wetgeving. En op vertrouwen.**	Wet- en regelgeving, waaronder de Algemene Verordening Gegevensbescherming (AVG), gedefinieerde eisen van stakeholders en contractuele verplichtingen van klanten vormen de basis voor ons Informatiebeveiligingsbeleid op de dienstverlening. Vertrouwen is voor Werken in Gelderland een groot goed en zij hanteert naar medewerkers, klanten, leveranciers en andere stakeholders het wederkerigheidsprincipe. Werken in Gelderland gaat ervan uit, dat zij afspraken nakomen m.b.t. integriteit, vertrouwelijkheid en continuïteit van de informatievoorziening. Dit is de grondslag voor elke bedrijfseconomische afweging.	● Risicobeheersing ● Stakeholder analyse ● Wetgeving en contracten
4	**Nieuwe projecten en veranderingen**	Werken in Gelderland 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.	● Change management ● Incident management
5	**Omgaan met incidenten**	Afwijkingen van afspraken en procedures, mogelijke kwetsbaarheden en schendingen	● Informatiebeveiligingsbeleid ● Changemanagement

		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.	● Incidentmanagement ● Continuïteitsplan
6	**Continue verbetering**	Informatiebeveiligingsbeleid is bij Werken in Gelderland een continu verbeterproces. Het bestuur beoordeelt periodiek de werking van het beleid.	● Verbeterplan ● Operationele planning ● Bestuursbeoordeling
7	**Actieve monitoring naleving Informatiebeveiligingsbeleid en sancties**	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.	● Gedragscode / geheimhoudingsverklaring ● Overeenkomsten ● Uitbestedingsbeleid ● Continuïteitsbeheer

In de Privacy en Security Code worden de basisvereisten opgesomd die Werken in Gelderland stelt aan medewerkers van Werken in Gelderland en medewerkers van subverwerkers.