schuldenknooppunt

Beleidskader informatiebeveiliging

Schuldenknooppunt

Classificatie:	Vertrouwelijk
Auteur:	B. Tel (Axxemble)
Versie:	1.0.1
Datum:	20-07-2021

Managementsamenvatting

Het Schuldenknooppunt biedt een uniform communicatieplatform en standaardisering van het schuldhulpverleningsproces. Het Schuldenknooppunt vormt daarmee de technische schakel tussen schuldhulpverleners - die namens de schuldenaar bemiddelen - en de schuldeisers. Deze partijen sluiten aan op het Schuldenknooppunt voor de uitwisseling van berichten m.b.t. de schuldhulpverlening.

Gezien de aard van deze dienstverlening en de gevoeligheid van de uitgewisselde gegevens is het van belang om de informatiebeveiliging goed te organiseren. De eerste stap hierin is om een beleidskader vast te stellen voor de informatiebeveiliging.

Op basis van de ISO 27001 is een beleidskader opgesteld dat duidelijke doelstellingen en richting geeft aan de invulling van de informatiebeveiliging. Deze aanpak vertaalt zich in het bepalen van de context van de organisatie met de relevante interne en externe onderwerpen, het vaststellen van de eisen en verwachtingen van belanghebbenden, het formuleren van het beleid en doelstellingen alsook de benodigde rollen en verantwoordelijkheden om hier invulling aan te geven.

De organisatie kenmerkt zich door als een stichting zonder winstoogmerk een faciliterende dienst te leveren voor (en door) de deelnemers: schuldhulpverleners (gemeenten en uitvoerende organisaties) en schuldeisers (uiteenlopende organisaties). De organisatie is in opbouw en maakt de transitie van een projectorganisatie naar een staande organisatie.

De belanghebbenden zijn in de eerste plaats de deelnemers die naast wettelijke verplichtingen ook eisen hebben ten aanzien van de informatiebeveiliging om op veilige wijze te kunnen koppelen aan het communicatieplatform. Indirect zijn ook de belangen van de schuldenaren van belang ten aanzien van de bescherming van persoonsgegevens.

Om invulling te geven aan deze belangen is de volgende doelstelling geformuleerd:

> **Het beveiligen van informatie in relatie tot het realiseren, beheren en ontwikkelen van een centrale, digitale voorziening ter facilitering van de gegevensuitwisseling in het schuldendomein in Nederland (het Schuldenknooppunt) en de daaraan gerelateerde bedrijfsprocessen.**

Afgeleid daarvan zijn de volgende beleidsdoelstellingen opgesteld:

- Het verminderen van de risico's van menselijke fouten, diefstal, fraude of misbruik van voorzieningen;
- Het verzekeren van de beschikbaarheid van de informatie voor de bedrijfsprocessen;
- Het verzekeren van de integriteit van de informatie gedurende de uitvoering van het bedrijfsproces;
- Het verzekeren en beschermen van de vertrouwelijkheid van de informatie tegen ongeautoriseerde toegang;
- Het benoemen van het eigenaarschap van de bedrijfsprocessen met de bijbehorende informatiesystemen en het verankeren van de hieraan verbonden verantwoordelijkheden;
- Het waarborgen van beveiliging binnen informatiesystemen en het toepassen van beveiligingseisen in het proces van systeemontwikkeling en -onderhoud;
- Het rapporteren en onderzoeken van actuele en vermoede informatiebeveiligings- incidenten en mogelijke kwetsbaarheden;

- Het naleven van wettelijke en contractuele voorschriften, beveiligingscontrole op informatiesystemen, audits en interne controle.

Om de beleidsdoelstellingen te kunnen realiseren is gekeken naar de vereiste rollen en verantwoordelijkheden waarbij naast de reeds bestaande organisatie in ieder geval invulling gegeven moet worden aan:

- Security officer: belast met de dagelijkse zaken rondom informatiebeveiliging;
- Interne auditor: een controlerende rol op naleving van het eigen beleid en doelstellingen;
- Portefeuillehouder governance, privacy en security: uitbreiding van de bestaande rol binnen het bestuur voor security gerelateerde zaken.

Naast dit beleidskader is er een risicoanalyse en een stelsel van beheersmaatregelen opgesteld welke een verdere uitwerking geven van de beleidsdoelstellingen.

Inhoud

Inleiding

Het Schuldenknooppunt biedt een uniform communicatieplatform en standaardisering van het schuldhulpverleningsproces. Het Schuldenknooppunt vormt daarmee de technische schakel tussen schuldhulpverleners - die namens de schuldenaar bemiddelen - en de schuldeisers. Deze partijen sluiten aan op het Schuldenknooppunt voor de uitwisseling van berichten m.b.t. de schuldhulpverlening.

Gezien de aard van deze dienstverlening en de gevoeligheid van de uitgewisselde gegevens is het van belang om de informatiebeveiliging goed te organiseren. De eerste stap hierin is om een beleidskader vast te stellen voor de informatiebeveiliging.

Dit document geeft het beleidskader weer zoals dat voor het Schuldenknooppunt van toepassing is. De opzet van het document is afgeleid van de internationale norm voor informatiebeveiliging, de ISO 27001. Hierbij wordt invulling gegeven aan de context van de organisatie, de belanghebbenden, de beleidsdoelstellingen en de rollen en verantwoordelijkheden ten aanzien van de informatiebeveiliging binnen het Schuldenknooppunt.

Naast dit beleidskader is er een risicoanalyse en een stelsel van beheersmaatregelen opgesteld welke een verdere uitwerking geven van de beleidsdoelstellingen.

Context **van de organisatie**

Stichting Schuldenknooppunt, gevestigd te Utrecht, KvK-nummer 77260155, is beheerder en eigenaar van het Schuldenknooppunt. De stichting is in 2020 ontstaan uit de gezamenlijke behoefte van schuldhulpverleners - verenigd in de branchevereniging NVVK - en schuldeisers aan een uniform communicatieplatform en standaardisering van het schuldhulpverleningsproces. De stichting heeft geen winstoogmerk.

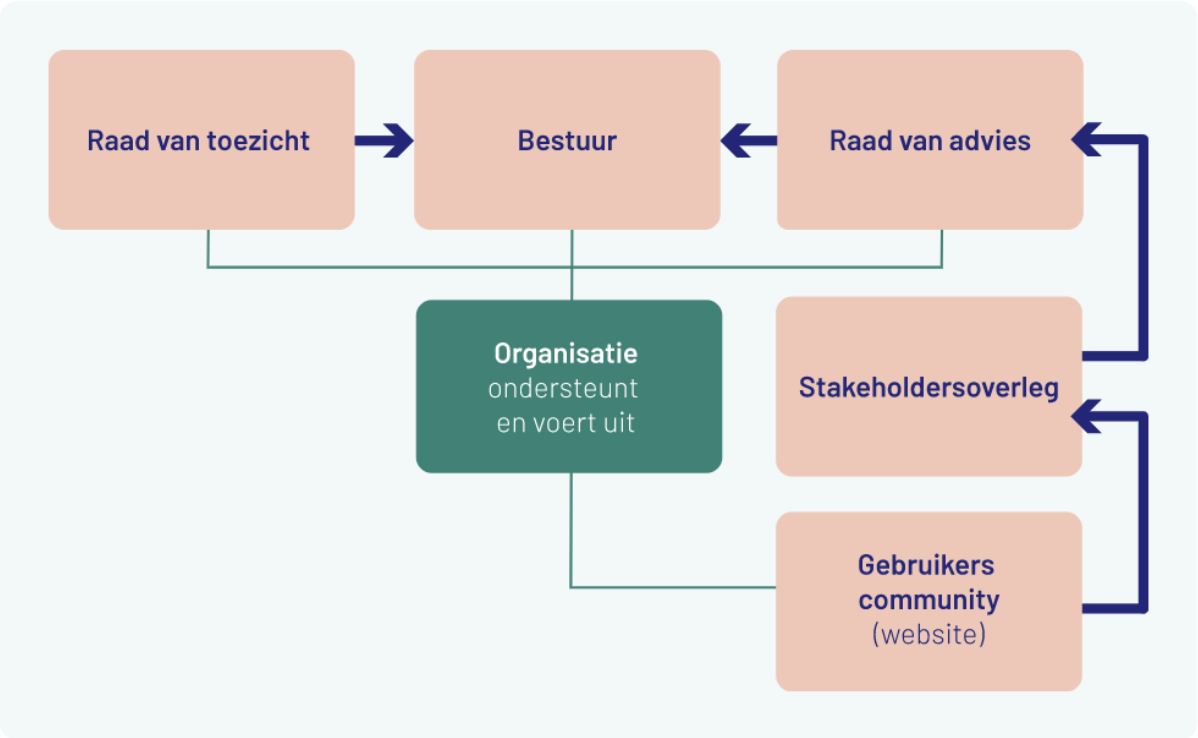
Stichting Schuldenknooppunt is eigenaar van het Schuldenknooppunt, een centrale, digitale voorziening ter facilitering van de gegevensuitwisseling in het schuldendomein in Nederland.

Door het Schuldenknooppunt wordt het schuldregelingsproces versneld, (maatschappelijke) kosten gereduceerd en de kwaliteit van dienstverlening verbeterd. Dit is in het belang van mensen met schulden en de maatschappij als geheel.

1. Het Schuldenknooppunt ontzorgt de informatie-uitwisseling tussen schuldhulpverleners en schuldeisers door standaardafspraken te maken over
    - berichten;
    - deelnemende partijen;
    - proces.
2. Het Schuldenknooppunt zorgt voor procesoptimalisatie:
    - gegevensuitwisseling vindt gestandaardiseerd plaats;
    - via een centraal beheerd digitaal platform;
    - waarop schuldhulpverleners en schuldeisers eenvoudig kunnen aansluiten;
    - dat voldoet aan de vereisten vanuit de AVG;
    - kwaliteit verbeterd door minder menselijke handelen;
    - snellere doorlooptijden, waardoor schuldhulpverleners meer tijd overhouden voor begeleiding en meer mensen met schulden kunnen helpen.
3. Het Schuldenknooppunt heeft geen commercieel oogmerk, het dient het maatschappelijk belang van betrokken partijen in de schuldenketen.

Structuur van de organisatie

Het gezamenlijk belang van schuldhulpverleners en schuldeisers bij het doel van het Schuldenknooppunt wordt weerspiegeld in de samenstelling van de organisatie van de stichting. Schuldhulpverleners en schuldeisers, publiek en privaat, zijn gelijkelijk vertegenwoordigd in de verschillende onderdelen van de stichting.



De uitvoerende organisatie (groen blok in bovenstaand overzicht) is momenteel als een projectorganisatie georganiseerd en zal op de middellange termijn overgaan in een 'staande' organisatie met vaste rollen en verantwoordelijkheden, ook t.a.v. informatiebeveiliging.

De organisatie zal daarbij naar verwachting verschillende taken uitbesteden zoals dat ook nu het geval is ten aanzien van administratie, ontwikkeling etc.

Externe en interne onderwerpen

Voor de organisatie worden de volgende externe en interne onderwerpen ten aanzien van informatiebeveiliging vastgesteld die haar vermogen beïnvloeden om de beoogde doelstellingen en resultaten te behalen.

Externe onderwerpen

Categorie	Externe onderwerpen (issues)
Wet- en regelgeving	De organisatie heeft naast standaard wetgeving meer in het bijzonder te maken met onderstaande wet- en regelgeving t.a.v. het Schuldenknooppunt: - Wet gemeentelijke schuldhulpverlening (met name artikel 8) ; - AVG en UAVG ; en - Gedragscode Schuldhulpverlening / Kwaliteitskader van de NVVK[1].
Politiek en markt	Deelnemers (schuldeisers) zijn actief in verschillende markten waarbinnen specifieke eisen t.a.v. informatiebeveiliging relevant kunnen zijn voor de organisatie.
Technisch	De organisatie biedt een online oplossing en dient daarom zoals elke organisatie met online activiteiten rekening te houden met algemene cyberdreigingen en richtlijnen zoals uitgegeven door de NCSC waar mogelijk toe te passen. In technische zin maakt de organisatie gebruik van eHerkenning EH3 en PKIoverheid certificaten.
(Natuur)rampen	De organisatie is in zeer beperkte mate kwetsbaar voor rampen zoals brand, explosies etc.
Economie	De organisatie is niet direct gevoelig voor economische omstandigheden. De oplossing die de organisatie biedt beoogt een efficiëntie verbetering te realiseren waarvoor de business case voor deelnemers positief is.

1 De organisatie en deelnemers actief als schuldhulpverlener, hanteren deze regels. Lidmaatschap van de NVVK is echter geen vereiste.

Interne onderwerpen

Categorie	Interne onderwerpen (issues)
Beleid en doelstellingen	De organisatie ervaart in toenemende mate druk om informatiebeveiliging op een goede wijze te organiseren en toe te passen.
Kwetsbaarheden	Verschillende maatregelen zijn genomen en worden toegepast om mogelijke kwetsbaarheden op te sporen en het risico hiervan te mitigeren.
Organisatie	De organisatie t.a.v. informatiebeveiliging leunt op dit moment op de professionaliteit van medewerkers en leveranciers. De rollen en verantwoordelijkheden t.a.v. de informatiebeveiliging zijn niet vastgesteld.
Middelen	Voor exploitatie van de diensten is een model gemaakt dat uitgaat van deling door kosten van deelnemers. Dit wordt jaarlijks geëvalueerd en indien nodig bijgesteld na goedkeuring bestuur.
Processen en procedures	De huidige projectorganisatie zal op de middellange termijn overgaan in een 'staande' organisatie met vaste rollen en verantwoordelijkheden, ook t.a.v. informatiebeveiliging. De organisatie zal daarbij naar verwachting verschillende taken uitbesteden.
Cultuur	Het Schuldenknooppunt is een professionele organisatie waarbinnen veel aandacht en bewustzijn is t.a.v. de risico's m.b.t. de informatiebeveiliging.

Belanghebbenden

De organisatie heeft onderstaande belanghebbenden die m.b.t. informatiebeveiliging een belangrijke relatie hebben.

Deelnemers

Deelnemers willen de zekerheid dat de informatie die verwerkt wordt door de organisatie vertrouwelijk behandeld wordt, in correcte staat en beschikbaar is en blijft zoals bepaald t.a.v. de beoogde dienstverlening.

De deelnemers aan het Schuldenknooppunt zijn onder te verdelen in twee categorieën:
schuldhulpverleners
schuldeisers

Voor alle deelnemers gelden de aansluitvoorwaarden. Hierin zijn verschillende punten t.a.v. de informatiebeveiliging opgenomen:

Behoefte / verwachtingen	Vastgelegd in / referentie	Opmerkingen
Deelnemers hebben belang bij beschikbaarheid van de dienst maar de beschikbaarheidseis is beperkt.	Aansluitvoorwaarden, Artikel 5: Vergoeding	Deelnemer heeft recht op een restitutie naar rato van de door hem betaalde vergoeding indien het Schuldenknooppunt voor een aaneengesloten periode van ten minste vijf werkdagen niet operationeel is.
Deelnemers en beheerder dienen eisen t.a.v. de beveiliging toe te passen, zorg te dragen voor het dataverkeer, scheiding van netwerken te garanderen, incidenten te melden en wijzigingen gecontroleerd door te voeren.	Aansluitvoorwaarden, Artikel 7: Beveiliging	Beveiligingsmaatregelen zijn niet in detail uitgewerkt.
Deelnemers en beheerder dienen geheimhouding toe te passen op alle informatie waarvan redelijkerwijs is aan te nemen dat bekendmaking daarvan de belangen van de andere partij zou schaden.	Aansluitvoorwaarden, Artikel 9: Geheimhouding	
Deelnemers en beheerder respecteren de intellectuele eigendomsrechten.	Artikel 11: Intellectuele eigendomsrechten	

Verder geldt de verwerkersovereenkomst waarin afspraken t.a.v. de AVG vastgelegd worden tussen de deelnemers (als verwerkingsverantwoordelijken) en het Schuldenknooppunt (als verwerker).

Behoefte / verwachtingen	Vastgelegd in / referentie	Opmerkingen
Deelnemers en beheerder werken in overeenstemming met de AVG: doel van de verwerking, rechtsgrondslag, rechten van betrokkenen, melden van datalekken, bewaartermijnen etc.	AVG	
Personenen werkzaam voor verwerker (en subverwerkers) dienen een geheimhoudingsverklaring te tekenen wanneer zij toegang hebben tot persoonsgegevens.	Verwerkersovereenkomst, Artikel 4.4: Geheimhouding	

Toegang tot de dienst is voorbehouden aan organisaties o.b.v. gevalideerde deelname waarbij de organisatie dient te beschikken over eHerkenning en een PKIoverheid certificaat.

Behoefte / verwachtingen	Vastgelegd in / referentie	Opmerkingen
Deelnemers kunnen uitsluitend toegang krijgen tot de dienst bij authenticatie via eHerkenning niveau EH3.	eHerkenning	Deelnemers vragen zelf de eHerkenning aan (indien zij die nog niet ter beschikking hebben).
Deelnemers kunnen uitsluitend communiceren met de dienst op basis van PKIoverheid certificaten.	PKIoverheid certificaten	Deelnemers vragen zelf het PKIoverheid certificaat aan, specifiek voor het Schuldenknooppunt.

Schuldhulpverleners

Schuldhulpverleners zijn per definitie de gemeenten in Nederland volgens de Wet gemeentelijke schuldhulpverlening. Gemeenten kunnen deze taak zelf uitvoeren of uitbesteden aan uitvoeringsorganisaties zoals kredietbanken of stadsbanken. De uitvoeringsorganisaties zijn gemandateerd door de gemeenten; elke gemeente heeft een mandaatregister.

Aangezien schuldhulpverleners een vertrouwelijke rol hebben is de authenticiteit en controle daarop van groot belang. De authenticiteit van de schuldhulpverleners wordt gecontroleerd (in de praktijk door de NVVK). In technische zin is er een extra waarborg door de noodzaak voor toepassing van eHerkenning en PKIoverheid certificaten waarbij de validiteit van de organisaties gecontroleerd is.

Schuldeisers

Vrijwel alle (publieke en private) organisaties in Nederland zijn mogelijk schuldeiser en kunnen een aanvraag doen voor deelname. In de praktijk zullen organisaties met een substantieel aantal schuldenaren gebruik willen maken van de dienst om het proces op efficiënte wijze te faciliteren.

Mogelijk deelnemende schuldeisers:

- Zorgverzekeraars
- Energieleveranciers
- Telecomproviders
- Incasso-organisaties

- Gerechtsdeurwaarders
- Lokale belasting organisaties (gemeenten etc.)
- enz.

De verschillende organisaties kunnen t.a.v. de gegevensuitwisseling eisen hebben t.a.v. de informatiebeveiliging.

Behoefte / verwachtingen	Vastgelegd in / referentie	Opmerkingen
De organisatie (beheerder) dient passende certificering te hebben en/of voldoende beheersmaatregelen te implementeren om de informatiebeveiliging te waarborgen.	Certificering (ISO 27001 / NEN 7510)	
De organisatie (beheerder) dient passende beheersmaatregelen te implementeren en aan te tonen zodat de financiële integriteit / transacties gewaarborgd is.	SOC I of II rapportage	Aangezien de dienst geen financiële transacties verwerkt - uitsluitend communicatie / afstemming - wordt dit niet in scope geacht.

Schuldenaren

De schuldenaren - betrokkenen in relatie tot de verwerking van persoonsgegevens - hebben op basis van de AVG rechten welke middels de verwerkersovereenkomst geborgd worden.

Behoefte / verwachtingen	Vastgelegd in / referentie	Opmerkingen
Betrokkenen hebben recht op bescherming van hun privacy en gerelateerde rechten.	Verwerkersovereenkomst, Artikel 4.6: Rechten van betrokkenen	Als een betrokkene een beroep doet op zijn rechten ondersteunen de verwerker(s) en subverwerker(s) om daarop binnen de wettelijke termijnen een beslissing te nemen.

Overheid

De overheid vereist dat de organisatie zich houdt aan wet- en regelgeving. Wet- en regelgeving heeft ook betrekking op informatiebeveiliging en privacybescherming van natuurlijke personen (waaronder medewerkers, contactpersonen etc.) Waar nodig dient de organisatie hier verantwoording over af te leggen.

Behoefte / verwachtingen	Vastgelegd in / referentie	Opmerkingen
Ten aanzien van de AVG dient de organisatie invulling te geven aan de volgende punten: - De organisatie is verwerker, toeleveranciers zijn (mogelijk) subverwerker; deelnemers zijn verwerkingsverantwoordelijken ; - Er wordt gebruik gemaakt van een Functionaris Gegevensbescherming (FG) en een privacy officer (PO) ; - Uitvoeren van een Data Protection Impact Assessment (DPIA) t.a.v. de verwerking.	AVG / UAVG	
De organisatie geeft ondersteuning aan de uitvoering van de Wet gemeentelijke schuldhulpverlening en dient de dienst daarom in overeenstemming hiermee aan te bieden.	Wet gemeentelijke schuldhulpverlening	De wet stelt zelf geen eisen t.a.v. informatiebeveiliging maar impliceert dat wel vanwege de relevantie voor overheidsorganisatie waarvoor de BIO van toepassing is.
De organisatie is wettelijk verplicht een administratie bij te houden van haar werkzaamheden en financiële gegevens en hanteert daarbij de wettelijke termijnen voor bewaring en vernietiging.	Algemene Wet Rijksbelastingen, Artikel 52.4	De organisatie is verplicht de administratie gedurende zeven jaar te bewaren.
De organisatie dient een cookie-waarschuwing weer te geven op openbare website(s) van de organisatie.	Telecommunicatiewet, Artikel 11.7a	De website geeft een cookiemelding. De organisatie volgt individuele gebruikers niet.
De organisatie verspreidt geen originele werken zonder dat daarvoor toestemming is verkregen van de eigenaar van de auteursrechten. Dit impliceert ook dat de organisatie voor het gebruik van	Auteurswet / intellectueel eigendom	

software de juiste licenties bezit en/of licentievoorwaarden naleeft.		
De wet computercriminaliteit richt zich op de strafrechtelijke probleemgebieden in relatie tot het computergebruik. De wet schrijft voor dat "enige beveiliging" vereist is alvorens er sprake kan zijn van het eventueel strafrechtelijk vervolgen van delicten jegens de organisatie.	Wet computercriminaliteit	Naleving van dit informatiebeveiligingsbeleid en implementatie van de genoemde maatregelen moet leiden tot een niveau van beveiliging dat als voldoende mag worden gezien in het kader van de wet computercriminaliteit.

Partners / leveranciers

Partners en leveranciers hebben belang bij een betrouwbare organisatie waarmee of waarvoor zij hun eigen activiteiten op een duurzame wijze uit kunnen voeren. Daarnaast is het voor de organisatie zelf van belang om te kunnen steunen op betrouwbare leveranciers.

Een belangrijke leverancier voor de dienstverlening van het Schuldenknooppunt is Innovadis. Hiermee is een Service Level Agreement (SLA) opgesteld waarin een aantal belangrijke punten ingevuld worden.

Behoefte / verwachtingen	Vastgelegd in / referentie	Opmerkingen
Geheimhouding	ICT~Office Voorwaarden, module algemeen, Artikel 4	Er is geen garantie tot geheimhouding na beëindiging van de overeenkomst.
Verwerkersovereenkomst	ICT~Office Voorwaarden, module algemeen, Artikel 5	Er is geen specifieke verwerkersovereenkomst. Huidige afspraken zijn verouderd.
Aansprakelijkheid	ICT~Office Voorwaarden, module algemeen, Artikel 12	Aansprakelijkheid is beperkt tot de omvang van de opdracht en sluit indirecte- en gevolgschade uit.
ISO 27001 certificering	-	Innovadis is momenteel bezig een ISO 27001 certificering te realiseren.
Ondersteuning (2e lijns support)	SLA, paragraaf 2.2	Innovadis biedt 8x5 ondersteuning (geen 24x7).
Gegevens binnen de EER	SLA, paragraaf 3.3	
OTAP inrichting	SLA, paragraaf 3.4	Er is een testomgeving (“preproductie”) beschikbaar voor deelnemers.
Beschikbaarheid 99,8%	SLA, paragraaf 3.5	
Certificaten	SLA, paragraaf 3.7	Voor testomgeving beschikbaar, binnen productieomgeving onderhouden deelnemers zelf PKIoverheid certificaten.
Monitoring servers	SLA, paragraaf 3.8	
Onderhoud / updates	-	

Medewerkers / projectteam

Het projectteam zorgt voor de realisatie van het Schuldenknooppunt, de aansluiting van deelnemers en de ondersteuning van de stichting. Op middellange termijn zal het projectteam haar werkzaamheden geleidelijk overdragen naar de staande organisatie van stichting Schuldenknooppunt.

Medewerkers wensen een betrouwbare werkgever met bestaanszekerheid op de lange termijn. Zij willen hun persoonlijke gegevens beschermd zien en zijn bereid benodigde activiteiten uit te voeren om de veiligheid van informatie te garanderen mits deze realistisch uitvoerbaar zijn.

Stichting

De stichting kent een aantal organen op basis waarvan het bestuur van de stichting uitgevoerd en gecontroleerd wordt:

- Raad van toezicht
- Bestuur
- Raad van advies
- Stakeholdersoverleg

Met de verschillende partijen wordt managementinformatie uitgewisseld naar noodzaak en behoefte. Dit betreft onder andere informatie over aantallen aansluitingen, verplichtingen, eventuele risico's etc.

Beleid en doelstellingen

Op basis van de algemene doelstelling van de stichting kan het toepassingsgebied als volgt gedefinieerd worden:

> **Het beveiligen van informatie in relatie tot het realiseren, beheren en ontwikkelen van een centrale, digitale voorziening ter facilitering van de gegevensuitwisseling in het schuldendomein in Nederland (het Schuldenknooppunt) en de daaraan gerelateerde bedrijfsprocessen.**

Het doel van de informatiebeveiliging is daarbij om de continuïteit van de dienstverlening / activiteiten te waarborgen en het risico op schade te minimaliseren door incidenten te voorkomen en de impact te minimaliseren.

Het informatiebeveiligingsbeleid is daarom gericht op het beschermen van de informatiemiddelen tegen alle interne en externe dreigingen, opzettelijk of onopzettelijk.

Het informatiebeveiligingsbeleid heeft als beleidsdoelstellingen:

- Het verminderen van de risico's van menselijke fouten, diefstal, fraude of misbruik van voorzieningen;
- Het verzekeren van de beschikbaarheid van de informatie voor de bedrijfsprocessen;
- Het verzekeren van de integriteit van de informatie gedurende de uitvoering van het bedrijfsproces;
- Het verzekeren en beschermen van de vertrouwelijkheid van de informatie tegen ongeautoriseerde toegang;
- Het benoemen van het eigenaarschap van de bedrijfsprocessen met de bijbehorende informatiesystemen en het verankeren van de hieraan verbonden verantwoordelijkheden;
- Het waarborgen van beveiliging binnen informatiesystemen en het toepassen van beveiligingseisen in het proces van systeemontwikkeling en -onderhoud;
- Het rapporteren en onderzoeken van actuele en vermoedde informatiebeveiligings- incidenten en mogelijke kwetsbaarheden;
- Het naleven van wettelijke en contractuele voorschriften, beveiligingscontrole op informatiesystemen, audits en interne controle.

De security officer is verantwoordelijk voor het onderhoud van het informatiebeveiligings- beleid en het realiseren van de doelstellingen. De security officer geeft daartoe ondersteuning en advies gedurende de implementatie en uitvoering.

Het beleid wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, incidenten, risicoanalyses en controles.

De organisatie stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze gesteld in dit beleid.

Naleving van het informatiebeveiligingsbeleid is verplicht.

Het bestuur heeft zijn goedkeuring gegeven aan het informatiebeveiligingsbeleid.

Rollen en verantwoordelijkheden

De huidige projectorganisatie zal op de middellange termijn overgaan in een 'staande' organisatie met vaste rollen en verantwoordelijkheden. Hieronder wordt de beoogde toekomstige verdeling m.b.t. rollen en verantwoordelijkheden beschreven.

	Rol	Verantwoordelijkheden en bevoegdheden
	Directie	• Goedkeuring en vaststelling van het IB-beleid. • Het vaststellen van de processen en de bepaling van het beveiligingsniveau. • De totstandkoming van bewustzijn informatiebeveiliging en de risico´s. • Het ter beschikking stellen van de middelen om de gestelde doelstellingen te kunnen realiseren. • Het zorgdragen voor de evaluatie van de werking van het IB–beleid. • Het zorgdragen dat de vastgestelde maatregelen in de praktijk kunnen en worden uitgevoerd, • Ondersteuning van de medewerkers bij invoering van de maatregelen, • Toezien op de correcte naleving van de maatregelen, • Meewerken aan de uitvoering (en het oplossen) van audit (bevindingen).
	Medewerkers	• Geheimhouding en zorgvuldigheid bij de uitvoering van activiteiten. • De naleving van het IB-beleid en daarvan afgeleide processen, procedures, richtlijnen en het IB Management systeem; • Rapporteren van incidenten en afwijkingen aan de security officer.

	Security officer	• Gedelegeerd eigenaar van het IB Management systeem.
		• Strategische en tactische aansturing van het IB-managementproces.
		• Functionele aansturing van medewerkers binnen het IB-managementsysteem.
		• Opstellen en richting geven aan de IB aspecten in;
		  ○ Beleidsvorming,
		  ○ ICT-applicaties en organisatie,
		  ○ Integrale risicobeheersing en compliance,
		  ○ Bedrijfsprocessen,
		  ○ Gebruikersorganisatie.
		• Sturing geven aan en controle op;
		  ○ Interne en externe assessments en audits,
		  ○ Naleving in de gebruikersorganisatie,
		  ○ Effectiviteit van geïmplementeerde IB maatregelen,
		  ○ Correctieve en preventieve acties,
		  ○ Afhandeling van klachten en incidenten.
		• Ondersteunen van interne en externe assessments.
		• Opvolging geven aan verbeteractiviteiten.

		• Coördinatie bij IB-incidenten (inclusief klachten). • Incidentrapportages. • Bewaking en onderhoud van geïmplementeerde maatregelen. • Het assisteren bij de planning en uitvoering van interne en externe audits, • Het monitoren en begeleiden van het oplossen van bevindingen n.a.v. de interne en/of externe audit.
	Interne auditor	• Controle op naleving van het IB-beleid binnen het aandachtsgebied, • Ondersteunen van interne en externe assessments, • Planning en uitvoering van interne audits, • Het monitoren en begeleiden van het oplossen van bevindingen n.a.v. de interne audit.
	Functionaris Gegevensbescherming	• Toezicht op en advisering over naleving van de AVG en overige wet- en regelgeving m.b.t. de bescherming van persoonsgegevens.
	Privacy officer	• Coördinatie c.q. uitvoering van activiteiten in verband met naleving van de AVG en overige wet- en regelgeving m.b.t. de bescherming van persoonsgegevens.
	Bestuur	• Bewaken en sturen op de realisatie van de doelstelling van de stichting in het algemeen en die van informatiebeveiliging in het bijzonder.
	Portefeuillehouder governance, privacy en security	• Namens het bestuur eindverantwoordelijk voor de informatiebeveiliging en de bescherming van persoonsgegevens.

Competenties, opleiding en training

De benodigde competenties voor het adequaat invullen van de verantwoordelijkheden worden getoetst en indien nodig aangebracht door middel van opleiding en training.

Bijlage A - Lijst met afkortingen

Afkortingen en hun betekenis zoals gebruikt in dit document.

Afkorting	Betekenis
(U)AVG	(Uitvoeringswet) Algemene Verordening Gegevensverwerking
AWR	Algemene Wet Rijksbelastingen
BIO	Baseline Informatiebeveiliging Overheid
DPIA	Data Protection Impact Assessment
EH3	eHerkenning niveau 3
FG	Functionaris Gegevensbescherming
IB	InformatieBeveiliging
ISO	International Standards Organisation (Internationale Organisatie voor Standaardisatie)
NCSC	Nationaal Cyber Security Centrum
NEN	NEderlandse Norm [2]
NVVK	Nederlandse Vereniging voor Volkskrediet
PKI	Public Key Infrastructure
PO	Privacy Officer
OTAP	(Gescheiden) Ontwikkel-, Test-, Acceptatie- en Productie- omgeving(en)
SLA	Service Level Agreement
(I)SO	(Information) Security Officer
SOC	Service Organization Control
Wgs	Wet Gemeentelijke Schuldhulpverlening

[2] Tevens de naam van het samenwerkingsverband van de Stichting Koninklijk Nederlands Normalisatie Instituut en de Stichting Koninklijk Nederlands Elektrotechnisch Comité (NEC).