

reBeleidsdocument

Strategisch beleid Informatiebeveiliging

Referentie: *IB21032025*

Auteurs: Steven Bronsveld, Wouter Damen

Datum: 6 april 2025

Versie: v1.1.0

Documentinformatie

Versiebeheer

Versie	Datum	Auteur	Review	Verwerking
v1.0.0	21-03-2025	Wouter Damen, Steven Bronsveld	Gezamenlijk opgesteld	Eerste goedgekeurde versie
v1.0.1	06-04-2025	Steven Bronsveld	Wouter Damen	Hernoemen "tactisch beleid" naar "themabeleid"
v1.1.1	05-05-2025	Steven Bronsveld	Wouter Damen	De reikwijdte van het ISMS (4.3) uitbreiden

Verwijzingen naar SURFaudit Toetsingskader en ISO27001

Kader	Verwijzing (tags)
SURFaudit Toetsingskader	
ISO27001	4.1; 4.2; 4.3; 5.1; 5.2; 5.3; 6.1; 6.2; 7.1; 7.2; 7.3; 7.4; 7.5; 8.1; 8.2; 8.3; 9.1; 9.2; 9.3; 10.1; 10.2

Creative Commons

Dit document is opgesteld op basis van een template van het SURF Security Expertise Centrum, welke beschikbaar is onder de licentie Creative Commons Naamsvermelding 4.0 Internationaal. <https://creativecommons.org/licenses/by/4.0/deed.nl>



1 Inhoudsopgave

1	Inhoudsopgave.....	3
2	Samenvatting.....	4
3	Inleiding.....	5
4	Context van de	6
5	Management.....	7
6	Risicomanagement.....	9
7	Mensen en middelen.....	10
8	Continu verbeteren.....	11
9	Vaststelling.....	12
10	Bijlage 1. Beleidspiramide.....	13

2 Samenvatting

Het primaire doel van dit beleid is het geven van richting aan onze informatiebeveiliging zodat de beschikbaarheid, vertrouwelijkheid en integriteit van informatie in de primaire processen van onze instelling zo goed mogelijk worden geborgd. Extern uitgangspunt voor dit document is de ISO 27001:2022-norm aangezien dit wereldwijd de 'best practice' vormt voor informatiebeveiliging op strategisch niveau. Achter hoofdstuk- en paragraaftitels zijn de verwijzingen naar relevante ISO-normen opgenomen.

3 Inleiding

Dit document beschrijft het strategisch informatiebeveiligingsbeleid Bronscore B.V. vanaf datum genoemd op het voorblad.

Dit strategisch informatiebeveiligingsbeleid, gebaseerd op ISO 27001:2022, stelt kaders en geeft richting. Op thematisch en operationeel niveau is dit beleid aangevuld met thema specifieke documenten (standaarden, richtlijnen, procedures en handleidingen).

3.1 Doel van het beleid

Bronscore B.V. versterkt met dit strategisch informatiebeveiligingsbeleid de cyberweerbaarheid, de groei in het volwassenheidsniveau en de bescherming van informatie en persoonsgegevens. Hiermee borgen we een veilige omgeving voor onze medewerkers, klanten en eindgebruikers.

3.2 Reikwijdte en toepassingsgebied

Bij Bronscore B.V. wordt informatieveiligheid breed geïnterpreteerd. Het heeft betrekking op alle vormen van formeel vastgelegde informatie (dus niet alleen digitale informatie), die Bronscore B.V. of haar relaties genereren en beheren.

Het beleid is tijd- en locatie-onafhankelijk en geldt dus 24x7 ook als men op een andere locatie dan op het terrein van Bronscore B.V. met informatie of informatievoorziening van Bronscore B.V. werkt, zoals thuis, in de trein, bij een andere organisatie of tijdens reizen naar het buitenland.

3.3 Definities en afkortingen

ISMS	Information Security Management System: een set van afspraken en procedures om informatiebeveiliging te organiseren
Informatiebeveiliging / Security	Geheel van maatregelen en processen die zijn ontworpen om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te waarborgen.
Privacy	Recht van individuen om controle te hebben over hun persoonlijke informatie en hoe deze informatie wordt verzameld, gebruikt, gedeeld en beschermd.
Beschikbaarheid	Zorgt ervoor dat informatie, systemen en processen toegankelijk zijn en gebruikt kunnen worden wanneer dat nodig is.
Integriteit	Waarborgt de nauwkeurigheid en volledigheid van informatie en de verwerkingsmethoden.
Vertrouwelijkheid	Zorgt ervoor dat informatie alleen toegankelijk is voor geautoriseerde personen en niet worden onthuld aan onbevoegde individuen, entiteiten of processen.

4 Context van de Organisatie

4.1 De organisatie en haar context (4.1)

Bronscore B.V. is een jong softwarebedrijf gespecialiseerd in web- en softwareontwikkeling en biedt maatwerk digitale oplossingen voor organisaties in verschillende sectoren zoals het onderwijs, financiële dienstverlening en de maakindustrie, gericht op het optimaliseren van complexe processen binnen deze organisaties. Als gevolg hiervan verwerkt Bronscore B.V. informatie die onderdeel is van kritieke bedrijfsprocessen.

Het soort gegevens dat verwerkt wordt kan variëren van persoonsgegevens en financiële data tot informatie onder NDA. De beschikbaarheid, integriteit en vertrouwelijkheid van deze informatie is dus van groot belang voor alle betrokken partijen.

Binnen Bronscore B.V. wordt voornamelijk gewerkt met cloudhosted-infrastructuur (bijv. Zoho, Azure, DigitalOcean, GitHub) en moderne softwareontwikkelingstechnieken zoals Git en CI/CD. Hierdoor vormen externe dreigingen zoals supply chain attacks en kwetsbaarheden in third-party software een risico voor onze dienstverlening.

Als onderdeel van haar missie biedt Bronscore B.V. ook part-time posities voor diverse ervaringsniveaus in softwareontwikkeling die hierdoor werkervaring op kunnen doen. De toegang van deze medewerkers tot de centrale systemen vereist precieze controles.

4.2 De behoefte en verwachtingen van belanghebbenden (4.2)

De verwachtingen zijn afhankelijk van de rol van de belanghebbenden.

- Klanten verwachten dat Bronscore B.V. zich houdt aan de afspraken over informatiebeveiliging vastgelegd in hun contracten en overeenkomsten.
- Eindgebruikers verwachten dat de door Bronscore B.V. ontwikkelde softwareapplicaties betrouwbaar en veilig zijn en dat hun privacy geborgd is.
- Medewerkers verwachten een omgeving waarin de data en systemen voor het werk betrouwbaar en veilig zijn en waarin hun privacy geborgd is. Verder verwachten medewerkers een omgeving waarin duidelijk is wat er van hun verwacht wordt wat betreft de kwaliteit, efficiëntie en veiligheid van het werk dat ze leveren.
- Bestuur verwacht efficiëntie, effectiviteit en uitvoerbaarheid van het beleid en dat deze in lijn is met de visie en richting van het bedrijf.

Deze verwachtingen vormen de basis voor een correcte classificatie van data (en/of informatie) om vervolgens bijpassende technische, fysieke, mensgerichte en/of organisatorische maatregelen te kunnen toepassen.

4.3 De reikwijdte van het ISMS (4.3)

Om te voorkomen dat de hiervoor genoemde verwachtingen van belanghebbenden geschaad worden, organiseren we onze informatieveiligheid met behulp van een proces

genaamd Information Security Management System (ISMS). De reikwijdte van het ISMS omvat de volledige organisatie: alle bedrijfsprocessen, medewerkers, locaties, projecten en ondersteunende systemen die onder de verantwoordelijkheid van Bronscore Holding B.V. vallen. Dit geldt voor zowel interne activiteiten als voor projecten en diensten die voor of namens klanten worden uitgevoerd. Er zijn geen onderdelen van de organisatie uitgesloten van het ISMS. Deze reikwijdte is vastgesteld op basis van de kleinschalige aard van onze organisatie en het strategische doel om informatiebeveiliging breed te borgen. Het ISMS vormt daarmee een structurele en toekomstbestendige basis voor het beheren van informatiebeveiligingsrisico's in alle facetten van onze bedrijfsvoering.

5 Management

5.1 Uitgangspunten van ons beleid (5.2)

Centraal uitgangspunt van ons beleid zijn de gebruikers van onze informatie en systemen. Om de beschikbaarheid, integriteit en vertrouwelijkheid te borgen hanteren we de volgende uitgangspunten. Binnen onze organisatie:

1. werken we risico gebaseerd

We baseren de te treffen maatregelen op de mogelijke veiligheidsrisico's van onze gegevens, processen, informatievoorzieningen en -systemen en op de risicobereidheid (risk appetite) van het bestuur.

2. is iedereen verantwoordelijk

Iedereen voelt zich verantwoordelijk voor een juist en veilig gebruik van middelen en bevoegdheden.

3. wordt het informatiebeveiligingsbeleid altijd en overal gevolgd

Informatiebeveiliging zit in het DNA van onze organisatie en is integraal onderdeel van al onze werkzaamheden.

4. hanteren we Security en Privacy by Design

Informatiebeveiliging en bescherming van persoonsgegevens en privacy is vanaf de start een integraal onderdeel van ieder project of iedere verandering van onze gegevens, processen, informatievoorzieningen en -systemen.

5. hanteren we Security en Privacy by Default

Informatievoorzieningen en -systemen standaard zijn geconfigureerd met de meest veilige instellingen.

6. heeft iedereen toegang tot alleen dat wat nodig is

Gebruikers hebben alleen toegang tot gegevens, processen, informatievoorzieningen en -systemen passend bij hun functie en rollen.

7. gaan we uit van controle in plaats van blind vertrouwen

We hanteren een gelaagd beveiligingsmodel waarbij we verifiëren of aan

voorwaarden voor toegang tot en het gebruik van gegevens, processen, informatievoorzieningen en -systemen is voldaan.

5.2 Structuur van ons beleid

De structuur van ons beleid is opgebouwd in drie lagen (zie Bijlage 1 Beleidspiramide). De bovenste laag is het strategisch informatiebeveiligingsbeleid en is beschreven in dit document. Verdere specificering van het informatiebeveiligingsbeleid is vastgelegd in de onderliggende standaarden, richtlijnen, procedures en handleidingen.

5.3 Betrokkenheid, leiderschap en verantwoordelijkheden (5.1, 5.2, 5.3)

5.3.1 Betrokkenheid en leiderschap (5.1, 5.2)

Het Bestuur toont leiderschap en betrokkenheid door ervoor te zorgen dat het informatiebeveiligingsbeleid en de doelstellingen in lijn zijn met de strategische richting van onze instelling. De eisen van het managementsysteem (ISMS) integreren we in de processen van onderwijs, onderzoek en bedrijfsvoering. Het Bestuur communiceert het belang van effectieve informatiebeveiliging, zorgt dat de doelstellingen worden behaald, ondersteunt medewerkers in hun bijdragen aan het systeem, bevordert continue verbetering en spreekt andere managementrollen aan op hun verantwoordelijkheden.

5.3.2 Rollen en verantwoordelijkheden (5.3)

Het Bestuur draagt er zorg voor dat er binnen onze instelling duidelijkheid bestaat over verantwoordelijkheden en bevoegdheden van rollen met betrekking tot informatiebeveiliging. Het Bestuur kent de verantwoordelijkheden en bevoegdheden toe voor het waarborgen van de naleving van het informatiebeveiligingsbeleid en voor het rapporteren over de prestaties ervan.

6 Risicomanagement

6.1 ISMS-risico's en (bij)sturing door management (6.1, 8.1, 9.1)

Bronscore B.V. neemt bij het plannen van het managementsysteem voor informatiebeveiliging zowel de in- als externe context in overweging (hoofdstuk 2). Hierbij worden risico's en kansen geïdentificeerd om de beoogde resultaten te behalen en ongewenste effecten te voorkomen of te verminderen, met als doel voortdurende verbetering te realiseren. We nemen concrete acties om deze risico's en kansen aan te pakken en bepalen hoe we deze in onze processen integreren, implementeren en evalueren. Daarnaast definiëren en passen we een procedure toe voor de behandeling van informatiebeveiligingsrisico's. Dit omvat het selecteren van passende opties voor risicobehandeling, het vaststellen van beheersmaatregelen en het verkrijgen van goedkeuring van risico-eigenaren.

We stellen criteria vast voor deze processen en implementeren ze conform deze criteria. Gedocumenteerde informatie wordt beschikbaar gesteld in de benodigde omvang en diepgang om het vertrouwen te waarborgen dat de processen volgens planning zijn uitgevoerd. Geplande wijzigingen in onze (informatiemanagement-)processen beheren we en worden evenals onbedoelde wijzigingen geëvalueerd om indien nodig corrigerende maatregelen te nemen. Extern geleverde processen, producten of diensten worden tevens gecontroleerd en gemonitord door onze instelling.

Bronscore B.V. stelt vast wat wanneer en door wie moet worden gemonitord en gemeten, inclusief processen en beheersmaatregelen voor informatiebeveiliging, en bepaalt de methoden voor het monitoren, meten en analyseren. Gedocumenteerde informatie is beschikbaar als bewijs van de resultaten. Onze instelling evalueert de prestaties van de informatiebeveiliging en de doeltreffendheid van het managementsysteem voor informatiebeveiliging.

6.2 Operationeel risicomanagement (6.2, 8.2, 8.3)

Bronscore B.V. stelt informatiebeveiligingsdoelstellingen vast die in lijn zijn met het informatiebeveiligingsbeleid, meetbaar zijn, en rekening houden met geldende eisen en risicobeoordelingen. We monitoren, communiceren, actualiseren en documenteren deze doelstellingen. Bij het opstellen van plannen bepalen we wat er moet gebeuren, welke middelen nodig zijn, wie verantwoordelijk is, wanneer acties zijn voltooid en hoe resultaten worden geëvalueerd.

Bronscore B.V. voert regelmatig of bij belangrijke veranderingen zoals het aansluiten van nieuwe klanten risicobeoordelingen voor informatiebeveiliging uit, waarbij we rekening houden met vastgestelde criteria voor risicobeoordeling en acceptatie, en bewaart gedocumenteerde informatie over de resultaten van deze beoordelingen. Tevens implementeert Bronscore B.V. het risicobehandelingsplan voor informatiebeveiliging en bewaren we gedocumenteerde informatie over de resultaten van de risicobehandeling.

7 Mensen en middelen

7.1 Middelen voor informatiebeveiliging (7.1)

Bronscore B.V. bepaalt en maakt de middelen (systemen, processen en budgetten) beschikbaar die nodig zijn voor het opzetten, implementeren, onderhouden en voortdurend verbeteren van het managementsysteem voor informatiebeveiliging en voor het uitvoeren van dit informatiebeveiligingsbeleid.

7.2 Kennis en competenties (7.2, 7.3)

Bronscore B.V. identificeert de vereiste vaardigheden (competenties en bewustzijn) voor in- en externe medewerkers die taken uitvoeren die de beschikbaarheid, integriteit en/of vertrouwelijkheid beïnvloeden. We waarborgen dat deze medewerkers bekwaam zijn. Indien nodig ondernemen we stappen om de benodigde vaardigheden te ontwikkelen en evalueren we de doeltreffendheid van deze inspanningen.

Medewerkers die werkzaamheden verrichten namens, voor en/of binnen Bronscore B.V. dienen zich bewust te zijn van het informatiebeveiligingsbeleid, hun rol bij het bevorderen van de doeltreffendheid van het informatiebeveiligingsmanagementsysteem en de consequenties van het niet naleven van de eisen van dit managementsysteem.

7.3 Documentatie en Communicatie (7.4, 7.5)

Het managementsysteem voor informatiebeveiliging van Bronscore B.V. omvat onder andere documentatie behorende bij dit beleidsdocument en andere informatie die de organisatie nodig acht voor de effectiviteit van het managementsysteem.

Bij het creëren en bijwerken van deze documentatie zorgt Bronscore B.V. ervoor dat elk stuk een duidelijke identificatie en beschrijving heeft, inclusief een titel, datum, auteur of referentienummer en in het juiste format en medium is opgesteld. Verder worden ze beoordeeld en goedgekeurd op geschiktheid en volledigheid.

Gedocumenteerde informatie, zoals het managementsysteem voor informatiebeveiliging en relevante documenten, is actueel, beschikbaar en wordt adequaat beveiligd tegen verlies van vertrouwelijkheid, ongeoorloofd gebruik en manipulatie.

Het beheer van deze documentatie omvat verschillende activiteiten waaronder distributie, toegang, opslag, behoud, beheersing van wijzigingen en uiteindelijke bewaring of vernietiging. Externe documentatie die nodig is voor het managementsysteem voor informatiebeveiliging wordt ook geïdentificeerd en beheerd op een manier die passend is voor Bronscore B.V.

Bronscore B.V. identificeert welke interne en externe communicatie relevant is voor het managementsysteem voor informatiebeveiliging, inclusief het bepalen van de onderwerpen, het tijdstip, de doelgroep en de communicatiemethoden.

8 Continu verbeteren

8.1 Audits en compliance monitoring (9.2)

Met regelmaat voert Bronscore B.V. in- en externe audits uit om te bepalen of opzet, bestaan en werking van het informatiebeveiligingsbeleid aantoonbaar voldoen aan zowel de in- en externe normen.

Bronscore B.V. stelt een auditplan (inclusief frequentie, methoden, verantwoordelijkheden) vast, voert dit uit en rapporteert de resultaten. Bij het opzetten van het auditplan wordt rekening gehouden met het belang van de betrokken processen en eerdere auditresultaten.

8.2 Directiebeoordeling en strategische evaluatie (9.3)

Het Bestuur beoordeelt periodiek het managementsysteem voor informatiebeveiliging van Bronscore B.V. op voortdurende geschiktheid, toereikendheid en doeltreffendheid.

Hierbij wordt aandacht besteed aan de status van verbeterpunten uit eerdere managementreviews, relevante veranderingen in de context en naar de behoeften en verwachtingen van belanghebbenden. Tevens worden trends in afwijkingen en corrigerende maatregelen, resultaten van monitoring en auditresultaten meegenomen. Daarnaast wordt feedback van belanghebbenden, resultaten van risicobeoordelingen en de status van het risicobehandelingsplan beoordeeld, evenals kansen voor continue verbetering.

De managementreviews resulteren in beslissingen voor continue verbetering en wijzigingen in het managementsysteem voor informatiebeveiliging, ondersteund door gedocumenteerde informatie.

8.3 Afwijkingen en corrigerende maatregelen (10.1, 10.2)

Bronscore B.V. waarborgt het voortdurend verbeteren van het managementsysteem voor informatiebeveiliging door middel van een Plan, Do, Check, Act-cyclus.

Bij het constateren van afwijkingen reageren we adequaat en treffen passende maatregelen. Daartoe identificeren en beoordelen we deze afwijkingen en oorzaken. Vervolgens evalueren we de effectiviteit van deze corrigerende maatregelen en passen indien nodig wijzigingen toe in ons management voor informatiebeveiliging. Als bewijs leggen we de aard van de afwijkingen, de genomen maatregelen en de resultaten van de corrigerende acties vast.

9 Vaststelling

Dit beleid is aldus vastgesteld.

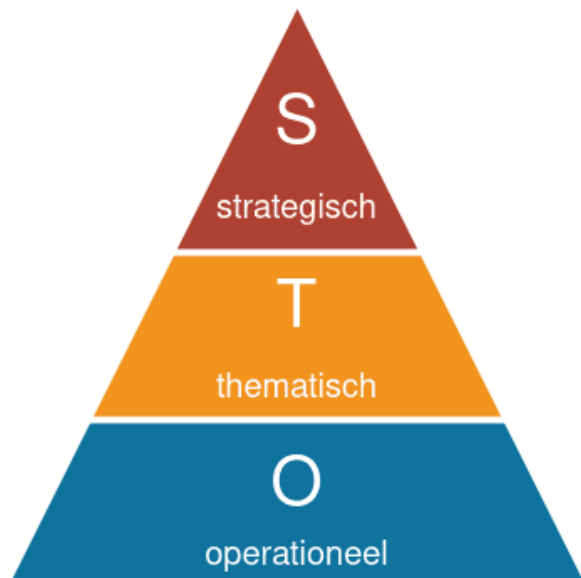
Nijmegen, 5 mei 2025.

Steven Bronsveld
algemeen directeur

Wouter Damen
operationeel directeur

10 Bijlage 1. Beleidspiramide

De beleidspiramide van onze instelling bestaat uit drie lagen: strategisch beleid, thematisch beleid, operationele procedures.



Figuur 1: Beleidspiramide Bronscore B.V.

1.1 Strategisch beleid

Op het 1^e niveau is het strategisch beleid beschreven (dit document). Dit niveau bepaalt de langetermijnstrategie en naleving van wet- en regelgeving (zoals ISO 27001 en AVG).

1.2 Thematisch beleid (topic specific policies)

Op het 2^e niveau is het thematisch beleid beschreven: het wat. Het thematische niveau vertaalt het strategische informatiebeveiligingsbeleid naar concrete richtlijnen en processen die het bedrijf kan implementeren. Dit niveau richt zich (per thema) op hoe de strategische doelstellingen worden toegepast in de organisatie, met focus op risico's, toegang, softwareontwikkeling en incidentbeheer.

1.3 Operationele procedures

Op het 3^e niveau zijn de operationele procedures beschreven: het hoe. Het operationele niveau is de dagelijkse praktijk waarin het tactische beleid wordt uitgevoerd. Dit niveau omvat de concrete werkprocessen, technische implementatie en controles om te zorgen dat de richtlijnen effectief worden nageleefd.