BKR Informatiebeveiligingsbeleid

Beleid voor informatiebeveiliging binnen Stichting BKR.

Versie 2.8

Documentbeheer

De CIO is eigenaar van dit document.

De documenteigenaar is verantwoordelijk voor:

- De inhoud van het document
- Het actueel houden van het document
- Het communiceren van het document binnen de organisatie

Voor wijzigingen in dit document is goedkeuring nodig van:

- Bestuur/MT

Wijzigingshistorie

Versie	Datum	Door	Omschrijving
2.3	11-05-2022	N. Ruinard	Nieuwe opzet
2.4	16-5-2022	T.A. Sinnema	Inhoudelijke verfijning doorgevoerd
2.5	23-5-2022	T.A. Sinnema	Verwerken reviewcommentaar
2.51	28-6-2022	T.A. Sinnema	Verwerken reviewcommentaar IB Stuurgroepleden
2.52	08-07-2022	T.A. Sinnema	Verwerken reviewcommentaar vanuit IB Stuurgroep
2.53	25-08-2022	T.A. Sinnema	Aanpassingen nav MT BKR & Reviewcommentaar Henk Bothof
2.54	06-09-2022	T.A. Sinnema	Aanpassingen nav SG IB 06-09-2022
2.6	04-10-2022	H.N. Bothof	Versie tbv Bestuur/MT
2.7	02-10-2023	S. Daskapan	Aanpassingen nav review
2.8	20-11-2024	S. Daskapan	Aanpassingen nav jaarlijkse directiebeoordeling

Distributie

Versie	Datum	Geadresseerden
2.3	11-05-2022	T. Sinnema
2.4	16-5-2022	N. Ruinard, M. Gouda, H. Bothof
2.5	23-5-2022	H. Bothof, M. Gouda
2.5	10-06-2022	IB Stuurgroepleden
2.51	29-06-2022	IB Stuurgroep
2.52	16-08-2022	MT BKR
2.53	31-8-2022	IB Stuurgroep
2.6	04-10-2022	Bestuur/MT
2.7	04-10-2023	Bestuur/MT
2.8	14-01-2025	Bestuur/MT

Inhoud

1 Inleiding

1.1 Achtergrond

Stichting BKR (hierna: BKR) hecht grote waarde aan een beheerste en integere bedrijfsvoering waarbij het belang van haar klanten en andere stakeholders en haar medewerkers centraal staat. BKR biedt een uitgebreide dienstverlening aan zakelijke klanten. Binnen BKR worden dagelijks op grote schaal data verwerkt. Ten dienste daarvan heeft BKR Informatiebeveiligingsbeleid (Hierna: dit Beleid) opgesteld, dat bijdraagt aan een adequate bescherming en verantwoorde omgang met data en informatie en het verantwoorden daarvan.

1.2 Reikwijdte

Dit Beleid is van toepassing op:

- Alle informatie die BKR verwerkt of laat verwerken, zowel fysiek als digitaal, zowel intern als extern
- Alle taken en processen waarin informatie wordt verwerkt waar BKR verantwoordelijk voor is
- Alle gebruikers (zowel intern als extern) die informatie van BKR verwerken
- Alle organisatorische, procedurele en technische maatregelen ter bescherming van informatie.

1.3 Werking van dit document

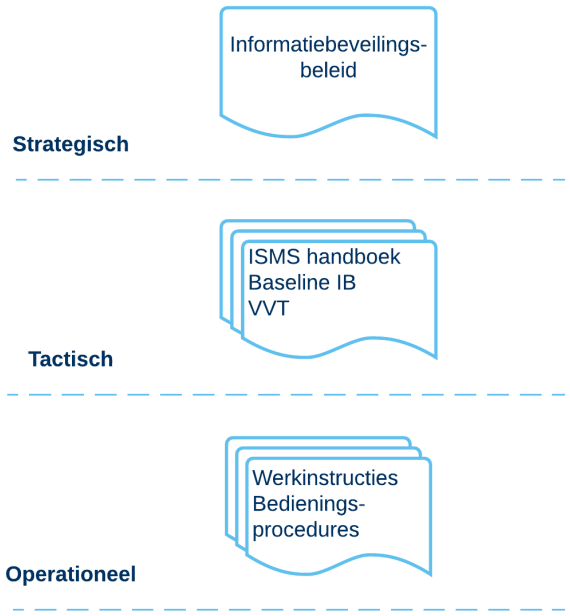
- De uitgangspunten uit dit beleid rondom de informatiebeveiliging zijn onderdeel van het Information Security Management Systeem (ISMS)
- BKR voldoet aan eventuele aanvullende eisen die worden opgelegd vanuit wetgeving, vanuit de reglementen van de door BKR beheerde stelsels, en datgene BKR contractueel heeft afgesproken met haar zakelijke klanten.
- BKR hanteert met betrekking tot deze uitgangspunten het principe “pas toe of leg uit”. Afwijkingen van de uitgangspunten rondom informatiebeveiliging dienen voorgelegd te worden aan de CISO.
- De eisen in dit Beleid zijn richtinggevend (parapluregels) en geen vervanging voor het inrichten en implementeren van meer gedetailleerde en specifieke beheersmaatregelen op basis van gerichte risico-overwegingen vanuit proces-, mens-, system- of applicatie-perspectief.
- Beheersmaatregelen worden genomen gebaseerd op het risiconiveau van de dreiging en rekening houdend met de risicobereidheid van BKR.
- De kosten van beheersmaatregelen moeten in verhouding staan tot de risico’s die BKR loopt. Hierbij geniet een technische oplossing altijd de voorkeur boven gedragsvoorschriften. Restrisico's worden onderkend.
- Management bevordert communicatie en bewustwording rondom informatiebeveiliging zodat management, werknemers en externen hun verantwoordelijkheden rondom informatiebeveiliging begrijpen en nakomen.

1.4 Gerelateerde documenten

Beleid interne beheersing
Dit Beleid hangt onder het overkoepelende Beleid Interne Beheersing..

Informatiebeveiliging specifiek

De onderstaande afbeelding laat zien hoe de verschillende informatiebeveiligingsdocumenten in verband met elkaar staan binnen het Information Security Management System (ISMS) van BKR.



Strategisch

Het informatiebeveiligingsbeleid vormt het kader voor strategieën, doelstellingen en verantwoordelijkheden ten aanzien van informatiebeveiliging.

Tactisch

- Het ISMS-handboek beschrijft de processen van het ISMS en hoe de ISO/IEC 27001-vereisten zijn vervuld.
- De Baseline Informatiebeveiliging bevat de maatregelen die worden genomen om de informatiebeveiliging te beheersen.
- De Verklaring Van Toepasselijkheid (VVT) laat zien welke normelementen in scope zijn bij het ISMS van BKR.

Operationeel

De operationele documenten zijn ondersteunende documenten die operationele procedures en werkinstructies met betrekking tot informatiebeveiliging beschrijven.

1.5 Taken en verantwoordelijkheden

De verantwoordelijkheden ten aanzien van dit beleid liggen vast in onderstaande RASCI-matrix:

- R, Responsible: degene die verantwoordelijk is voor de uitvoering van een process of activiteit. Hij/zij legt verantwoording af aan de person die accountable is.
- A, Accountable: degene die eindverantwoordelijk is en goedkeuring geeft aan het resultaat
- S, Support: de person die ondersteuning verleent aan het process op project en de (lijn)werkzaamheden uitvoert
- C, Consulted: de persoon die moet worden geraadpleegd, goedkeuring verleent of input levert voorafgaand aan een stap in het process. Deze person geeft (mede) richting aan het resultaat
- I, Informed: de person die geïnformeerd moet worden over de beslissingen, zodat er een volgende stap genomen kan worden

RASCI Activiteiten	R	A	S	C	I
Opstellen en actueel houden beleid	(C)ISO	CISO		Risicomanagers	
Goedkeuren beleid	Bestuur/MT	CISO		MT-leden	Risicomanagers
Communicatie beleid	(C)ISO	CISO	MT, Risicomanagers	Marketing en Communicatie	
Ondersteunen en adviseren van de business tav Beleid	ISO, Risicomanagers	CISO	Risicomanagers		
Naleven beleid	Alle medewerkers BKR	Bestuur/MT	Risicomanagers		
Monitoren naleving beleid	ISO, Risicomanagers	CISO		Risicomanagers	Medewerkers

1.6 informatiebeveiligingsdoelen

Voor 2025 zijn de volgende informatiebeveiligingsdoelen gesteld (zie ook ISMS handboek):

- Creëren bewustwording bij BKR medewerkers omtrent informatiebeveiliging
- Toegangsrechten tot de infrastructuur en de kritieke systemen van BKR zijn beheerst conform goedgekeurde autorisatiemodellen.
- Projecten en andere grote wijzigingen ondergaan allen een Informatiebeveiliging risico-analyse voordat de implementatie plaatsvindt.
- Risicos bij belangrijke leveranciers, ie waar onze kritieke systemen van afhangen, zijn gelijk of kleiner dan onze risicobereidheid.
- Materiele auditbevindingen, kwetsbaarheden en risico's worden tijdig gecorrigeerd.
- Security incidenten worden tijdig behandeld en beheerst

2 Beleidsuitgangspunten

2.1 Algemeen

- BKR dient te voldoen aan wet- en regelgeving
- Binnen BKR gelden gedragsregels voor het gebruik van informatievoorzieningen
- Vertrouwelijke informatie is beschermd tegen onbevoegden

2.2 Governance

- Voor informatiebeveiliging is een managementcyclus (ISMS) opgesteld
- Kwetsbaarheden, bedreigingen en incidenten worden gemeld en gerapporteerd
- Ontwikkelingen in wet- en regelgeving zijn inzichtelijk
- BKR beschikt over een continuïteitsplan (BCM: Business Continuity Management)

2.3 Organisatie

- De CISO is eindverantwoordelijk voor informatiebeveiliging; de eerste lijn is verantwoordelijk voor risicomanagement; binnen ICT is een risicomanager aangesteld. Als tweede lijns risicomanager is een Information Security Officer (ISO) aangesteld, die hiërarchisch rapporteert aan de CISO
- Taken en verantwoordelijkheden rondom informatiebeveiliging zijn belegd
- Toegang tot informatie wordt beperkt tot noodzakelijke functionarissen
- Informatie wordt geclassificeerd
- Mensen en middelen worden ook fysiek beveiligd

2.4 Processen

- Een proces is ingericht voor de juiste afhandeling van beveiligingsincidenten
- Een proces is ingericht om de risico's op het gebied van informatiebeveiliging in kaart te brengen bij het wijzigen of ontwikkelen van (nieuwe) producten
- Een proces is ingericht om bij het aangaan van samenwerkingsverbanden met externe partijen het geldende beleid te volgen
- Er zijn verschillende programma's geïmplementeerd waarin gecontroleerd wordt op de informatiebeveiliging

2.5 Communicatie & bewustzijn

- Binnen BKR geldt een clean desk & clear screen beleid
- Communicatie over informatiebeveiliging is begrijpelijk, transparant en relevant
- Medewerkers worden getraind om zodoende het beveiligingsbewustzijn te stimuleren

2.1 Algemeen

BKR dient te voldoen aan wet- en regelgeving

Omschrijving	**BKR dient te voldoen aan alle van toepassing zijnde wet- en regelgeving gerelateerd aan informatiebeveiliging**
Reden	BKR neemt een risico aversie in ten aanzien van risico's op het gebied van informatiebeveiliging. BKR's risicobereidheid is hiervoor laag.
Toelichting	Legal houdt wet- en regelgeving bij en ondersteunt hierbij de 1e lijn.

Binnen BKR gelden gedragsregels voor het gebruik van informatievoorzieningen

Omschrijving	**Binnen BKR gelden gedragsregels voor het gebruik van informatievoorzieningen**
Reden	Zorgvuldig handelen is één van de kernwaarden binnen BKR; hieronder valt ook het zorgvuldig omgaan met informatievoorzieningen
Toelichting	Het personeel dient bekend te zijn met de HR-regelingen en beleidsstukken binnen BKR

(vertrouwelijke) Informatie is beschermd tegen onbevoegden

Omschrijving	**Informatie is technisch en organisatorisch beschermd tegen verlies, diefstal en ongewenste wijzigingen**
Reden	Om de kerndoelen van BKR te kunnen realiseren, is bescherming van (vertrouwelijke) informatie noodzakelijk
Toelichting	De eisen rondom de beveiliging van specifieke aandachtsgebieden zijn nader uitgewerkt in specifieke (beleids-)stukken (bijv. Fysiek beveiligingsbeleid stichting BKR, Logisch toegangsbeveiligingsbeleid)

2.2 Governance

Voor informatiebeveiliging is een ISMS ingericht

Omschrijving	**Voor informatiebeveiliging is een management/beheer-cyclus ingericht**
Reden	Informatiebeveiliging is een voortdurend proces dat geborgd moet zijn in een ISMS
Toelichting	Dit uitgangspunt betekent dat de volgende zaken moeten zijn ingericht: • ISMS • Periodieke rapportage over de hoge risico's m.b.t. informatiebeveiliging aan de CISO, alsmede aan het Bestuur/MT

Kwetsbaarheden, bedreigingen en incidenten worden gemeld en gerapporteerd

Omschrijving	**Management en medewerkers melden bedreigingen, uitzonderingen, incidenten en overige bijzonderheden m.b.t. informatiebeveiliging. Management beoordeelt bij belangrijke incidenten achteraf de getroffen maatregelen en oorzaak**
Reden	Kwetsbaarheden, bedreigingen en incidenten moeten zo snel mogelijk worden opgelost en naar de toekomst worden voorkomen
Toelichting	Dit uitgangspunt betekent dat het volgende moet zijn ingericht: • Registratiesysteem voor kwetsbaarheden, incidenten en overige bijzonderheden • Periodieke rapportage aan het management over kwetsbaarheden, incidenten en bedreigingen • Gedetailleerde terugkoppeling aan leiding over ontstaan en opvolging van belangrijke incidenten

Ontwikkelingen in wet- en regelgeving zijn inzichtelijk

Omschrijving	**Ontwikkelingen in wet- en regelgeving op het gebied van informatiebeveiliging zijn inzichtelijk. De impact van deze ontwikkelingen is bepaald en de ontwikkelingen zijn meegenomen in de securityplannen.**
Reden	Voorkomen non-compliance Voorbereiden op potentiële risico's
Toelichting	Er dient een aparte Legal functie te zijn ingericht die het volgen en duiden van ontwikkelingen in wetgeving tot zijn verantwoordelijkheid rekent en daarmee de 1e lijn ondersteunt.

BKR beschikt over een continuïteitsplan als onderdeel van Business Continuity Management (BCM)

Omschrijving	**BKR beschikt over een continuïteitsplan waarin adequate maatregelen gericht op het waarborgen van de beschikbaarheid van de bedrijfsprocessen en de hierbij gebruikte informatie(systemen).**
Reden	Waarborgen van de beschikbaarheid van informatie Risicobeheersing
Toelichting	Dit uitgangspunt betekent dat het volgende ingericht moet zijn: • Crisisorganisatie • Continuiteitsplan • Periodiek oefenen van de getroffen maatregelen • Inzicht in resterende Single Point of Failures (SPOF's) en afweging op risico bij SPOF

2.3 Organisatie

Een Information Security Officer (ISO) is aangesteld

Omschrijving	**BKR heeft een ISO aangesteld die toeziet op- en adviseert over de naleving van informatiebeveiliging. Deze ISO ziet toe op het (operationeel) handhaven en het (laten) implementeren van het minimum beveiligingsniveau van BKR**
Reden	Conform Beleid Interne Beheersing
Toelichting	Het adviseren over het inrichten en vervolgens monitoren, adviseren & (laten) implementeren van Informatiebeveiliging vormt een onderdeel van de functieomschrijving van de ISO. Hij vervult daarmee een 2e lijns rol. Vanwege de wijze waarop de 2e lijn ISO bij BKR is georganiseerd is hij/zij ook ondersteunend in de volledige breedte van het bedrijf bij implementatievraagstukken die spelen vanuit de 1e lijn rondom informatiebeveiliging. Deze vloeien voort uit het Informatiebeveiliging beleid en de Informatiebeveiliging baseline die door de ISO zijn opgesteld ter ondersteuning van de CISO De ISO borgt onder de eindverantwoordelijkheid van de CISO hiermee dat we voldoen aan de ISO normering

Taken en verantwoordelijkheden rondom informatiebeveiliging zijn belegd

Omschrijving	**Taken en verantwoordelijkheden rondom informatiebeveiliging zijn belegd**
Reden	Aanbrengen van organisatorische functie- en rolscheiding Aanwezig hebben van noodzakelijke specialismen rondom risicomanagement en informatiebeveiliging

Toelichting	Informatiebeveiliging is de verantwoordelijkheid van de 1e lijn. De Chief Information Security Officer (CISO) is eindverantwoordelijk voor de informatiebeveiliging, het beleid en de werking van het ISMS; beleid wordt vastgesteld door het Bestuur/MT De Information Security Officer (ISO) adviseert en ondersteunt de verantwoordelijken voor informatie en processen bij de implementatie en het ten uitvoer brengen van het Informatiebeveiligingsbeleid en het creëren van risicobewustzijn bij medewerkers; Als vanuit de ISO wordt gesignaleerd dat de normen worden overschreden, wordt dit gesignaleerd en gerapporteerd aan de verantwoordelijken. Als het niet wordt opgelost, wordt dit gerapporteerd in de lijn naar het MT; Verbetering en behoud van informatiebeveiliging is een gezamenlijke inspanning van de gehele organisatie in de zin van iedereen die met informatie werkt. De teammanager Facilitair is verantwoordelijk gesteld voor de fysieke informatiebeveiligingsaspecten Directeur HR is verantwoordelijk gesteld voor informatiebeveiligingsaspecten gerelateerd aan personeel (oa. werving en training). De Teammanager IT-Operations is verantwoordelijk voor security operations, waaronder security incident management, Kwetsbaarheden (vulnerability management), opvolging van meldingen uit het Security Operation Center (SOC), patchen van systemen, toegangscontrole, netwerk security, disaster recovery en systeem security hardening. ICT risico officer is verantwoordelijk voor de 1e lijns ondersteuning aan de ICT medewerkers bij de risico identificatie, risicoanalyse en mitigatie in de diverse processen (inkoop, leveranciers mngt, project, systeem ontwikkeling, uitvoer controles, etc.). Hij/Zij escaleert en krijgt ondersteuning van de 2e ISO op het inhoudelijke vlak van informatiebeveiliging en van de 2e lijns risico en compliance officer.

Toegang tot informatie wordt beperkt tot noodzakelijke functionarissen

Omschrijving	**Toegang tot informatie wordt beperkt tot noodzakelijke functionarissen**
Reden	Voorkomen van ongewenste functievermenging Voorkomen van ongeoorloofde toegang tot systemen en informatie
Toelichting	De eisen rondom logische toegang en autorisatie zijn uitgewerkt in het logisch toegangsbeveiliging beleid.

Informatie wordt geclassificeerd

Omschrijving	**Informatie wordt geclassificeerd op basis van vertrouwelijkheid/gevoeligheid**
Reden	Om de gewenste mate van beveiliging toe te kunnen passen, dient informatie geclassificeerd te zijn
Toelichting	Beleid op classificatie van informatiesystemen op de kwaliteitsaspecten Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV-codering) en ook documenten moet zijn uitgewerkt in aanvullend beleid

Mensen en middelen worden fysiek beveiligd

Omschrijving	**Mensen en middelen worden fysiek beveiligd**
Reden	Uitgangspunt is dat alleen geautoriseerde (geoorloofde) toegang tot mensen en middelen plaats kan vinden
Toelichting	De eisen rondom fysieke beveiliging zijn uitgewerkt in het fysiek beveiligingsbeleid.

2.4 Processen

Een proces is ingericht voor de juiste afhandeling van beveiligingsincidenten

Omschrijving	**Er is een proces ingericht voor de juiste en tijdige afhandeling van beveiligingsincidenten**
Reden	Processen geven richting aan een beheerste bedrijfsvoering en zijn noodzakelijk bij de beheersing van de risico's op het gebied van informatiebeveiliging.
Toelichting	Er moet een heldere procesbeschrijving zijn voor de bewaking en afhandeling van beveiligingsincidenten

Een proces is ingericht om de risico's op het gebied van informatiebeveiliging in kaart te brengen bij het wijzigen of ontwikkelen van (nieuwe) producten.

Omschrijving	**Een proces is ingericht om de risico's op het gebied van informatiebeveiliging in kaart te brengen bij het wijzigen of ontwikkelen van (nieuwe) producten**
Reden	Processen geven richting aan een beheerste bedrijfsvoering en zijn noodzakelijk bij de beheersing van de risico's op het gebied van informatiebeveiliging.
Toelichting	Binnen BKR is "Security en Privacy by design" uitgangspunt; in alle fases van ontwikkeling, aanschaf of wijziging van informatiesystemen dienen betrokken medewerkers nadrukkelijk aandacht te besteden aan informatiebeveiliging. Ook wordt een DPIA vereist op moment dat er sprake is van de verwerking van persoonsgegevens.

Een proces is ingericht om bij het aangaan van samenwerkingsverbanden met externe partijen het geldende beleid te volgen

Omschrijving	**Een proces is ingericht om bij het aangaan van samenwerkingsverbanden met externe partijen het geldende beleid te volgen**
Reden	Processen geven richting aan een beheerste bedrijfsvoering en zijn noodzakelijk bij de beheersing van de risico's op het gebied van informatiebeveiliging.
Toelichting	De eisen voor het aangaan van samenwerkingsverbanden zijn uitgewerkt in aanvullend beleid, dan wel reglementen

Er zijn verschillende (controle-)programma's geïmplementeerd waarin gecontroleerd wordt op de informatiebeveiliging

Omschrijving	**Er zijn (controle-)programma's geïmplementeerd waarin gecontroleerd wordt op o.a. de informatiebeveiliging en hierover wordt gerapporteerd.**

Reden	Hiermee wordt niet alleen de opzet, bestaan, maar ook de werking van informatiebeveiliging aangetoond
Toelichting	De aantoonbaarheid van informatiebeveiliging is o.a. belangrijk voor een ISO 27001 certificering. Er moet eenduidig zijn vastgelegd welke controles plaatsvinden en dit dient ook te worden gemonitord op uitvoering. Deze zijn aantoonbaar opgenomen in een sluitende administratie en in (IB-)rapportages

2.5 Communicatie en bewustzijn

Binnen BKR geldt een clean desk & clear screen beleid

Omschrijving	**Binnen BKR geldt een clean desk en clear screen beleid om zodoende het risico op incidenten te verkleinen**
Reden	Het voorkomen van ongeautoriseerde toegang tot informatie
Toelichting	In de gedragscode en via aanvullende awareness programma's dient de medewerker te worden gewezen op het belang van clean desk & clear screen.

Communicatie over informatiebeveiliging is begrijpelijk, transparant en relevant

Omschrijving	**Communicatie over informatiebeveiliging is in begrijpelijke taal, transparant, up-to-date, en inhoudelijk afgestemd op de doelgroep**
Reden	Om het nut en de noodzaak van informatiebeveiliging over te kunnen brengen aan betrokkenen, dient hierover begrijpelijk gecommuniceerd te worden
Toelichting	Dit uitgangspunt impliceert dat er verschillende inhoud wordt gebruikt bij verschillende communicatiekanalen, afgestemd op de doelgroep

Medewerkers worden getraind om zodoende het beveiligingsbewustzijn te stimuleren

Omschrijving	**Medewerkers worden doorlopend en op verschillende manieren getraind om zodoende het beveiligingsbewustzijn te stimuleren**
Reden	Verkleinen van het risico op incidenten
Toelichting	Bij het waarborgen van informatiebeveiliging, is de grootste afhankelijkheid het menselijk handelen. Een groot bewustzijn bij medewerkers over hoe om te gaan met informatie is daarom van essentieel belang.

3. Goedkeuring

Dit Beleid is goedgekeurd door Bestuur/MT op 14-01-2025