BK IT Solutions

OPENBAAR DOCUMENT
VERSIE 1.0

BK IT SOLUTIONS

Leveranciersdossier

Informatiebeveiliging, privacy en continuïteit

DOEL VAN DIT DOSSIER

Een praktisch en openbaar naslagwerk voor inkopers, security officers, privacy officers en klanten die BK IT Solutions als leverancier beoordelen.

ISO 27001 gecertificeerd	**NEN 7510** gecertificeerd	**Microsoft** Solutions Partner for Security

Versie 1.0 | 21 september 2026 | Classificatie: Openbaar
Vaste publicatie-URL: https://www.bkitsolutions.nl/leveranciersdossier.pdf

Inhoudsopgave

HFD	ONDERWERP	PAGINA
1	Inleiding	3
2	Kerngegevens	4
3	Certificaten en scope	5
4	Beheersmaatregelen	7
5	Standaardantwoorden leveranciersvragenlijst	8
6	Incidenten en meldplicht	10
7	Privacy en verwerking	11
8	Beoordeling van onze leveranciers	12
9	Beschikbaar op aanvraag	13
10	Contact en versiebeheer	14
A	Bijlage — Certificaten en bewijsstukken	15

1 Inleiding

Wat dit document is, voor wie het bedoeld is en hoe je het gebruikt

Dit leveranciersdossier geeft klanten en inkopers in één document inzicht in de organisatorische en technische basis waarop BK IT Solutions haar dienstverlening uitvoert. Het is bedoeld om veelvoorkomende leveranciersvragen sneller, eenduidiger en controleerbaar te beantwoorden.

Het dossier is bruikbaar bij een inkoopprocedure, periodieke leveranciersbeoordeling, AVG-beoordeling of toetsing van de digitale toeleveringsketen. De antwoorden zijn bewust op hoofdlijnen beschreven. Er staan geen klantnamen, IP-ranges, interne systeemdetails of productversies in.

Zo gebruik je dit dossier

- Gebruik hoofdstuk 2 en 3 voor de administratieve leveranciersregistratie.
- Gebruik hoofdstuk 4 en 5 voor security- en continuïteitsvragen.
- Gebruik hoofdstuk 6 en 7 voor incidentmelding, privacy en verwerking.
- Vraag bewijsstukken uit hoofdstuk 9 op wanneer een diepgaandere toets nodig is.

2 Kerngegevens

ONDERDEEL	GEGEVENS
Statutaire naam	BK IT Solutions B.V.
KvK-nummer	77468503
Vestigingsadres	Rhijnspoor 243, 2901 LB Capelle aan den IJssel
Jaar van oprichting	2008
Algemeen contact	info@bkitsolutions.nl | +31 (0)88 606 3100
Securitycontact	Security Officer | security@bkitsolutions.nl | +31 (0)88 606 3100
Privacycontact	Security Officer / privacyfunctie | security@bkitsolutions.nl | +31 (0)88 606 3100
Website	www.bkitsolutions.nl

3 Certificaten en scope

ISO 27001

Norm	NEN-EN-ISO/IEC 27001:2023/A1:2024 nl
Certificaatnummer	**DGT271721604-01**
Uitgevende instelling	DigiTrust B.V.
Accreditatie	Raad voor Accreditatie, RvA C618
Geldig vanaf	21 augustus 2025
Geldig tot	3 september 2027
Register	Validatie via QR-code/register van DigiTrust/Zertic

Scope: Informatiebeveiliging gerelateerd aan het adviseren, verkopen, leveren, implementeren en beheren van ICT-oplossingen en hostingfaciliteiten, alsmede de ondersteuning en training van klanten op het gebied van datacenter, infrastructuur, werkplek, Cloud en security al dan niet met behulp van partners.

NEN 7510

Norm	NEN 7510-1:2024
Certificaatnummer	**DGTN71425130**
Uitgevende instelling	DigiTrust B.V.
Accreditatie	Raad voor Accreditatie, RvA C618
Geldig vanaf	29 juli 2026
Geldig tot	3 september 2027
Register	Validatie via QR-code/register van DigiTrust/Zertic

Scope: Informatiebeveiliging gerelateerd aan het adviseren, verkopen, leveren, implementeren en beheren van ICT-oplossingen en hostingfaciliteiten, alsmede de ondersteuning en training van klanten op het gebied van datacenter, infrastructuur, werkplek, Cloud en security al dan niet met behulp van partners.

3 Certificaten en scope

NIS2 Supply Chain SC-30

Keurmerk	NIS2 Quality Mark, Supply Chain niveau 30 (hoogste van drie niveaus)
Registratienummer	**BTUHEGVB0H4xM5aC**
Toetsende partij	Procertify
Accreditatie	Raad voor Accreditatie, RvA C707
Geldig vanaf	4 maart 2026
Geldig tot	4 maart 2029
Register	Openbaar register via registry.nis2qualitymark.eu

Microsoft Solution Partner AI Business

Partner-ID	**2486900**
Designations	Solutions Partner for Security; Solutions Partner for AI Business Solutions
Verificatie	Microsoft partnerverklaring, gedateerd 14 augustus 2026

Microsoft Solutions Partner Security

Partner-ID	**2486900**
Designations	Solutions Partner for Security
Verificatie	Microsoft partnerverklaring, gedateerd 14 augustus 2026

4 Beheersmaatregelen

Vier herkenbare vragen

Blijft het draaien?

BK IT Solutions borgt continuïteit door risico's vooraf te beoordelen, kritieke processen te documenteren, back-ups te controleren en herstel te testen. Het continuïteitsplan wordt periodiek beoordeeld en bevat scenario's voor cyberaanvallen, uitval van kritieke componenten, uitval van sleutelmedewerkers en onbereikbaarheid van kantoor.

- Back-ups worden periodiek gecontroleerd.
- Restoretests worden uitgevoerd.
- Continuïteitsmaatregelen worden waar mogelijk getest.
- Herstelprocedures en verantwoordelijkheden zijn gedocumenteerd.

Wie mag erbij?

Toegang wordt beperkt tot geautoriseerde medewerkers en toegekend via formele procedures. Multi-factor authenticatie is verplicht op systemen. Rechten zijn gekoppeld aan rollen en worden vastgelegd en periodiek beoordeeld.

- Least privilege en functiescheiding.
- MFA en voorwaardelijke toegang.
- Formele onboarding, wijziging en intrekking van toegang.
- Geheimhouding en screening van medewerkers.

Zien we het aankomen?

Belangrijke systemen worden gemonitord en logbestanden worden beschermd tegen wijziging. Kwetsbaarheden, malware, afwijkingen en incidenten worden gevolgd en geëscaleerd volgens vastgelegde processen.

- Monitoring op belangrijke systemen.
- Bescherming en beoordeling van logbestanden.
- Patch- en kwetsbaarhedenbeheer.
- 24/7 bereikbaarheid voor kritieke incidenten.

Wie controleert ons?

Het ISMS wordt intern beoordeeld en extern geaudit. De directie voert minimaal jaarlijks een managementreview uit. DigiTrust heeft in juli 2026 positief geadviseerd over voortzetting van de ISO 27001- en NEN 7510-certificering.

- Interne audits en directiebeoordeling.
- Externe controle-audits door een geaccrediteerde certificerende instelling.
- Externe Security Pentests via onafhankelijke leveranciers.
- Opvolging van afwijkingen en verbeterpunten.
- Periodieke herziening van beleid en risico's.

5 Standaardantwoorden leveranciersvragenlijst

Kort, bevestigend en geschikt om over te nemen

THEMA	ANTWOORD	TOELICHTING
Toegangsbeheer en MFA	**Ja**	Toegang is beperkt tot geautoriseerd personeel. MFA is verplicht op systemen. Autorisaties worden volgens formele procedures toegekend en ingetrokken.
Versleuteling	**Ja**	Persoonsgegevens worden tijdens transport en in rust versleuteld met passende industriestandaarden. Waar de dienstverlening identificatie vereist, wordt pseudonimisering niet standaard toegepast.
Back-up en herstel	**Ja**	Voor relevante diensten zijn back-up- en herstelmaatregelen ingericht. Succesvolle back-ups worden gecontroleerd en herstel wordt periodiek getest. Hersteltijden zijn afhankelijk van dienst en contract.
Kwetsbaarheden en patchen	**Ja**	Systemen worden gemonitord en regelmatig gepatcht. Technische kwetsbaarheden worden beoordeeld en opgevolgd op basis van risico en impact.
Logging en bewaartermijnen	**Ja, met context**	Belangrijke systemen produceren beveiligde logging die niet ongeautoriseerd mag worden gewijzigd. Specifieke bewaartermijnen zijn afhankelijk van systeem, doel, contract en wettelijke eisen. Een generieke openbare logretentie is daarom niet opgenomen.

5 Standaardantwoorden leveranciersvragenlijst

THEMA	ANTWOORD	TOELICHTING
Security awareness	**Ja**	Medewerkers volgen verplichte cybersecuritytraining, phishing-simulaties en periodieke awarenessactiviteiten. Actuele kennis is onderdeel van het ISMS.
Screening en VOG	**Ja**	Screening maakt onderdeel uit van het personeelsbeleid. Voor medewerkers is een Verklaring Omtrent Gedrag opgenomen als vereiste. Geheimhouding geldt tijdens en na het dienstverband.
Fysieke beveiliging	**Ja**	Het kantoor is gezoneerd en kent regels voor bezoekers, sleutels, afsluiting, clean desk en toegang tot bedrijfsruimten.
Wijzigingsbeheer	**Ja**	Wijzigingen aan informatieverwerkende faciliteiten en systemen vallen onder procedures voor wijzigingsbeheer, inclusief testen, acceptatie en documentatie.
Periodieke controle	**Ja**	Beleid, risico's en maatregelen worden intern beoordeeld, in de directiebeoordeling behandeld en extern geaudit binnen de certificatiecyclus.

6 Incidenten en meldplicht

Kritieke storingen en vermoedelijke cyberincidenten kunnen 24/7 telefonisch worden gemeld via **+31 (0)88 606 3100**. Reguliere meldingen kunnen via **support@bkitsolutions.nl** of het overeengekomen ticketkanaal worden gedaan.

Informatie aan klanten

Wanneer een beveiligingsincident persoonsgegevens raakt, informeert BK IT Solutions de aangewezen contactpersoon zonder onnodige vertraging en in ieder geval binnen 24 uur na ontdekking. De melding bevat voor zover bekend de aard en omvang, categorieën van betrokken gegevens, waarschijnlijke gevolgen, genomen of voorgestelde maatregelen en een contactpunt voor vervolgacties.

Aansluiting op de meldplicht van de klant

De termijn van 24 uur is bedoeld om de klant voldoende ruimte te geven voor zijn eigen beoordeling en eventuele wettelijke melding. De klant blijft als verwerkingsverantwoordelijke verantwoordelijk voor de AVG melding. Voor organisaties die onder de Cyberbeveiligingswet vallen, wordt beschikbare informatie zo snel mogelijk gedeeld zodat de klant zijn eigen termijnen kan halen.

MOMENT	ACTIE
Direct	Incident registreren, classificeren, beperken en escaleren.
Zonder onnodige vertraging	Contact opnemen met de aangewezen klantcontactpersoon.
Uiterlijk binnen 48 uur na ontdekking bij een datalek	Beschikbare gegevens delen volgens het datalekprotocol.
Vervolg	Updates geven zodra wezenlijke nieuwe informatie beschikbaar is en afsluiten met oorzaakanalyse en maatregelen waar passend.

7 Privacy en verwerking

BK IT Solutions gebruikt een verwerkersovereenkomst die bestaat uit een Data Pro Statement en de standaardclausules voor verwerkingen van NLdigital, versie maart 2025. Het Data Pro Statement van BK IT Solutions is versie 1.1 en geldt vanaf 1 juli 2025.

Belangrijkste uitgangspunten

- Persoonsgegevens worden in opdracht van de klant verwerkt.
- Verwerking vindt in beginsel plaats binnen de EU/EER.
- Toegang is beperkt tot geautoriseerd personeel en beschermd met MFA.
- Privacy by design, dataminimalisatie, encryptie, logging en monitoring zijn onderdeel van de maatregelen.
- Na beëindiging worden gegevens in principe binnen drie maanden verwijderd of, indien afgesproken, in machineleesbaar formaat teruggegeven. Wettelijke uitzonderingen kunnen gelden.

Subverwerkers op hoofdlijnen

CATEGORIE	VOORBEELDEN VAN VERWERKING	LOCATIE/WAARBORG
Service-, beheer- en documentatieplatforms	Ticketing, remote beheer, configuratie- en assetdocumentatie	Overwegend EU/EER
Back-up- en continuïteitsdiensten	Back-up, herstel en beschikbaarheidscontrole	EU/EER waar vastgelegd
Financiële administratie	Facturatie en debiteurenbeheer	EU/EER
Communicatie en marketing	Transactionele e-mail, nieuwsbrieven en klantcommunicatie	EU/EER of passende doorgiftewaarborg
Volledig register	Beschikbaar in de actuele ROPA en Data Pro-verklaring	Op aanvraag onder passende voorwaarden

PRIVACYCONTACT
Security Officer | security@bkitsolutions.nl | +31 (0)88 606 3100

8 Beoordeling van onze leveranciers

BK IT Solutions beoordeelt leveranciers vanuit het risico dat hun producten of diensten opleveren voor beschikbaarheid, integriteit, vertrouwelijkheid, privacy en continuïteit. Leveranciers met toegang tot klantinformatie of een kritieke rol in de dienstverlening krijgen extra aandacht.

Selectie en periodieke beoordeling

STAP	WERKWIJZE
1. Classificeren	Bepalen welke gegevens, systemen en bedrijfsprocessen de leverancier raakt.
2. Risico beoordelen	Impact bepalen van uitval, ongeautoriseerde toegang, datalekken, leveranciersafhankelijkheid en wijzigingen.
3. Afspraken vastleggen	Security-, privacy-, continuïteits-, audit-, incident- en beëindigingsafspraken contractueel vastleggen waar relevant.
4. Bewijs beoordelen	Certificaten, assurance-informatie, privacyvoorwaarden, subverwerkers en continuïteitsmaatregelen beoordelen op basis van risico.
5. Monitoren	Prestaties, incidenten, wijzigingen, voortgang en afhankelijkheden volgen en periodiek herbeoordelen.
6. Exit en overdraagbaarheid	Bepalen hoe gegevens, configuraties en dienstverlening bij beëindiging veilig worden overgedragen of verwijderd.

NIS2-TOELEVERINGSKETEN

Deze werkwijze ondersteunt klanten bij het aantoonbaar beheersen van risico's in de digitale toeleveringsketen. De exacte bewijsvoering en diepgang worden afgestemd op het risico en de contractuele relatie.

9 Beschikbaar op aanvraag

Onder geheimhouding of na passende toetsing

DOCUMENT	BESCHIKBAARHEID
Verklaring van toepasselijkheid	Samenvatting of relevante passages uit de ISO 27001- en NEN 7510-verklaring van toepasselijkheid.
Auditrapportage	Samenvatting van interne of externe audits, inclusief opvolging van relevante bevindingen.
Penetratietest	Alleen beschikbaar wanneer een actuele en relevante test of samenvatting aanwezig is. In de geraadpleegde SharePoint-bronnen is geen eenduidige openbare pentestsamenvatting aangetroffen.
Continuïteitsplan	Samenvatting van scenario's, verantwoordelijkheden, testen en hersteluitgangspunten.
ROPA en subverwerkersregister	Actuele informatie over verwerkingsactiviteiten en subverwerkers.
Aanvullende bewijsstukken	Beleidsfragmenten, hersteltestbewijs of leveranciersbeoordelingen voor zover relevant en veilig deelbaar.

Verstrekking vindt plaats op basis van noodzaak, proportionaliteit en vertrouwelijkheid. Informatie die de beveiliging van BK IT Solutions of haar klanten kan verzwakken, wordt niet onbeperkt gedeeld.

10 Contact en versiebeheer

ONDERDEEL	GEGEVENS
Documenteigenaar	Directie BK IT Solutions B.V.
Inhoudelijk beheer	Security Officer
Contact	security@bkitsolutions.nl | +31 (0)88 606 3100
Reviewmoment	Na iedere relevante audit of materiële wijziging en minimaal jaarlijks
Classificatie	Openbaar
Publicatie-URL	https://www.bkitsolutions.nl/leveranciersdossier.pdf
Bronnenpeildatum	21 september 2026

Versiehistorie

DATUM	VERSIE	WIJZIGING
21 september 2026	**1.0**	

BK IT Solutions B.V.
Rhijnspoor 243, 2901 LB Capelle aan den IJssel
+31 (0)88 606 3100 · www.bkitsolutions.nl

A Certificaten en bewijsstukken

De originele documenten zijn als bijlage achter dit dossier opgenomen

DOCUMENT	UITGEVER	NUMMER	GELDIG TOT
ISO 27001-certificaat	DigiTrust B.V., RvA C618	DGT271721604-01	3 september 2027
NEN 7510-certificaat	DigiTrust B.V., RvA C618	DGTN71425130	3 september 2027
NIS2 Supply Chain SC-30	Procertify, RvA C707	BTUHEGVB0H4xM5aC	4 maart 2029
Microsoft partnerverklaring	Microsoft Corporation	Partner-ID 2486900	21 oktober 2026

Zelf controleren

- ISO 27001 en NEN 7510: te valideren via de QR-code op het certificaat of het register van DigiTrust/Zertic.
- NIS2 Supply Chain SC-30: te valideren in het openbare register op registry.nis2qualitymark.eu.
- Microsoft-designations: toelichting via aka.ms/MicrosoftSolutionsPartner.

LET OP

Certificaten hebben een beperkte geldigheidsduur. Controleer bij gebruik van dit dossier altijd de actuele status in het register van de uitgevende instelling. De Microsoft partnerverklaring wordt periodiek opnieuw afgegeven.

DigiTrust
CERTIFICATION OF MANAGEMENT SYSTEMS

Management Systeem Certificaat

Dit certificaat met nummer DGT271721604-01 is uitgegeven voor het managementsysteem van:

BK IT Solutions B.V.

Vestigingsadres: Rhijnspoor 243, 2901 LB te Capelle aan den IJssel

Voldoet aan de eisen gesteld in de Informatie Beveiliging Management Systeem norm:

NEN-EN-ISO/IEC 27001:2023/A1:2024 nl

Voor het toepassingsgebied: Informatiebeveiliging gerelateerd aan het adviseren, verkopen, leveren, implementeren en beheren van ICT- oplossingen en hostingfaciliteiten, alsmede de ondersteuning en training van klanten op het gebied van datacenter, infrastructuur, werkplek, Cloud en security al dan niet met behulp van partners.

In overeenstemming met de verklaring van toepasselijkheid versie 1.0 van 16 april 2024.

Dit certificaat is geldig vanaf:
21 augustus 2025

Dit certificaat is geldig tot:
3 september 2027

Datum eerste certificaat:
3 september 2021

Dit certificaat vervangt nr:
--

NAMENS

Marco Bijl
DigiTrust B.V.

MGMT. SYS.
RvA C 618

DigiTrust B.V.: Achtseweg Zuid 159R - 5651 GW Eindhoven - Nederland
Telefoon +31 88 224-5600 - sales@digitrust.nl - www.digitrust.nl - KvK 59396822

Deze afgifte is uitgevoerd in overeenstemming met en binnen de procedures van DigiTrust zoals ook bekend bij en gecontroleerd door de RvA. Dit certificaat is elektronisch uitgegeven, het is en blijft eigendom van DigiTrust. Het valt daarom onder en is gebonden aan de uitgifte condities van het contract.
Certificaten kunnen worden gevalideerd via de QR-code.

DigiTrust
CERTIFICATION OF MANAGEMENT SYSTEMS

NEN 7510
Informatiebeveiliging in de zorg

Management Systeem Certificaat

Dit certificaat met nummer DGTN71425130 is uitgegeven voor het managementsysteem van:

BK IT Solutions B.V.

Vestigingsadres: Rhijnspoor 243, 2901 LB te Capelle aan den IJssel

Voldoet aan de eisen gesteld in de Informatie Beveiliging Management Systeem norm:

NEN7510-1:2024

Voor het toepassingsgebied: Informatiebeveiliging gerelateerd aan het adviseren, verkopen, leveren, implementeren en beheren van ICT-oplossingen en hostingfaciliteiten, alsmede de ondersteuning en training van klanten op het gebied van datacenter, infrastructuur, werkplek, Cloud en security al dan niet met behulp van partners.

In overeenstemming met de verklaring van toepasselijkheid versie 1.0 van 27 april 2026 waarin is gespecificeerd welke activiteiten, producten of diensten zijn uitbesteed.

Dit certificaat is geldig vanaf:
29 juli 2026

Dit certificaat is geldig tot:
3 september 2027

Datum eerste certificaat:
3 september 2021

Dit certificaat vervangt nr:
DGTN71721226

NAMENS

Marco Bijl
DigiTrust B.V.

MGMT. SYS.
RvA C 618

DigiTrust B.V.: Achtseweg Zuid 159R - 5651 GW Eindhoven - Nederland
Telefoon +31 88 224-5600 - sales@digitrust.nl - www.digitrust.nl - KvK 59396822

Deze afgifte is uitgevoerd in overeenstemming met en binnen de procedures van DigiTrust zoals ook bekend bij en gecontroleerd door de RvA. Dit certificaat is elektronisch uitgegeven, het is en blijft eigendom van DigiTrust. Het valt daarom onder en is gebonden aan de uitgifte condities van het contract.
Certificaten kunnen worden gevalideerd via de QR-code.

CERTIFICATE

European Supply Chain Cyber Security Standard

NIS2 SUPPLY CHAIN

NIS2-SC30 HIGH

The audit was performed by:

ProCertify

Valid from 04-03-2026 until 04-03-2029

NIS2 Supply Chain certificate:

BK IT Solutions

for completing the NIS2 Supply Chain Audit successfully

Dr. D.P. Noordhoek RAE

Director-Secretary

Foundation for Quality & Innovation

BTUHEGVB0H4xM5aC