Datum
13-03-2025

Contactpersoon
Chief Information Security Officer

Classificatie
Publiek

BKR Verklaring van toepasselijkheid

ISO27001:2022

Inleiding

Achtergrond

Dit document omvat de Verklaring van Toepasselijkheid (VVT) conform ISO 27001:2022 standaard.

Doel

Deze verklaring van toepasselijkheid geeft inzicht in de reikwijdte van het ISMS binnen BKR, welke ISO 27001 bijlage A beheersmaatregelen van toepassing zijn, de reden voor selectie en de status van implementatie.

ISMS Reikwijdte (Scope)

De scope omvat de kernactiviteiten van stichting BKR: het verzamelen, ontsluiten en beheren van data die bruikbaar zijn voor:

- verantwoorde kredietverstrekking
- identiteitsverificatie
- het voorkomen van problematische schulden
- het voorkomen van fraude in het financiële verkeer

Dit behelst al het personeel van BKR, de fysieke locatie in TIEL en de systemen:
- Verantwoorde kredietverstrekking (CKI);
- Problematische schulden (VPS);
- Fraude in het financiële verkeer (EVA)
- Identiteitsverificatie (KYC/VIS).

Annex A Beheersmaatregelen

	Stichting BKR ISO 27001 Verklaring van Toepasselijkheid	Van toepassing?	Wet & Regelgeving	Bedrijfseis/ Best practice	Risico analyse	Geïmplementeerd?	**Niet van toepassing want:**
Organisatorische beheersmaatregelen							
A.5.1	Beleidsregels voor informatiebeveiliging	Ja		X		Ja	
A.5.2	Rollen en verantwoordelijkheden bij informatiebeveiliging	Ja		X	X	Ja	
A.5.3	Functiescheiding	Ja	X	X		Ja	
A.5.4	Managementverantwoordelijkheden	Ja	X	X		Ja	
A.5.5	Contact met overheidsinstanties	Ja	X	X		Ja	
A.5.6	Contact met speciale belangengroepen	Ja		X		Ja	
A.5.7	Informatie en analyses over dreigingen	Ja	X	X		Ja	
A.5.8	Informatiebeveiliging in projectmanagement	Ja		X	X	Ja	
A.5.9	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	Ja		X		Ja	
A.5.10	Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen	Ja		X		Ja	
A.5.11	Retourneren van bedrijfsmiddelen	Ja		X		Ja	
A.5.12	Classificeren van informatie	Ja		X	X	Ja	
A.5.13	Labelen van informatie	Ja		X	X	Ja	
A.5.14	Overdragen van informatie	Ja			X	Ja	
A.5.15	Toegangsbeveiliging	Ja		X	X	Ja	
A.5.16	Identiteitsbeheer	Ja		X	X	Ja	
A.5.17	Beheren van authenticatie-informatie	Ja		X		Ja	
A.5.18	Toegangsrechten	Ja		X	X	Ja	
A.5.19	Informatiebeveiliging in leveranciersrelaties	Ja	X	X	X	Ja	
A.5.20	Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Ja	X	X	X	Ja	
A.5.21	Beheren van informatiebeveiliging in de ICT-keten	Ja	X	X	X	Ja	
A.5.22	Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	Ja	X	X	X	Ja	
A.5.23	Informatiebeveiliging voor het gebruik van clouddiensten	Ja	X	X	X	Ja	
A.5.24	Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten	Ja	X	X	X	Ja	
A.5.25	Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen	Ja	X	X	X	Ja	

A.5.26	Reageren op informatiebeveiligingsincidenten	Ja	X	X	X	Ja	
A.5.27	Leren van informatiebeveiligingsincidenten	Ja	X	X		Ja	
A.5.28	Verzamelen van bewijsmateriaal	Ja	X			Ja	
A.5.29	Informatiebeveiliging tijdens een verstoring	Ja	X	X		Ja	
A.5.30	ICT-gereedheid voor bedrijfscontinuïteit	Ja	X	X	X	Ja	
A.5.31	Wettelijke, statutaire, regelgevende en contractuele eisen	Ja	X	X	X	Ja	
A.5.32	Intellectuele-eigendomsrechten	Ja	X			Ja	
A.5.33	Beschermen van registraties	Ja		X		Ja	
A.5.34	Privacy en bescherming van persoonsgegevens	Ja	X	X	X	Ja	
A.5.35	Onafhankelijke review van informatiebeveiliging	Ja	X	X		Ja	
A.5.36	Naleving van beleid, regels en normen voor informatiebeveiliging	Ja	X	X	X	Ja	
A.5.37	Gedocumenteerde bedieningsprocedures	Ja		X		Ja	
Mensgerichte beheersmaatregelen							
A.6.1	Screening	Ja		X		Ja	
A.6.2	Arbeidsovereenkomst	Ja	X	X		Ja	
A.6.3	Bewustwording van, opleiding en training in informatiebeveiliging	Ja	X	X	X	Ja	
A.6.4	Disciplinaire procedure	Ja	X	X	X	Ja	
A.6.5	Verantwoordelijkheden na beëindiging of wijziging van het dienstverband	Ja		X		Ja	
A.6.6	Vertrouwelijkheids- of geheimhoudingsovereenkomsten	Ja		X		Ja	
A.6.7	Werken op afstand	Ja		X	X	Ja	
A.6.8	Melden van informatiebeveiligingsgebeurtenissen	Ja	X	X		Ja	
Fysieke beheersmaatregelen							
A.7.1	Fysieke beveiligingszones	Ja		X		Ja	
A.7.2	Fysieke toegangsbeveiliging	Ja		X		Ja	
A.7.3	Beveiligen van kantoren, ruimten en faciliteiten	Ja		X		Ja	
A.7.4	Monitoren van de fysieke beveiliging	Ja		X		Ja	
A.7.5	Beschermen tegen fysieke en omgevingsdreigingen	Ja		X	X	Ja	
A.7.6	Werken in beveiligde zones	Ja		X		Ja	
A.7.7	‘Clear desk’ en ‘clear screen’	Ja		X		Ja	
A.7.8	Plaatsen en beschermen van apparatuur	Ja		X		Ja	
A.7.9	Beveiligen van bedrijfsmiddelen buiten het terrein	Ja		X		Ja	
A.7.10	Opslagmedia	Ja		X		Ja	
A.7.11	Nutsvoorzieningen	Ja		X		Ja	
A.7.12	Beveiligen van bekabeling	Ja		X		Ja	

A.7.13	Onderhoud van apparatuur	Ja		X		Ja	
A.7.14	Veilig verwijderen of hergebruiken van apparatuur	Ja		X		Ja	
Technologische beheersmaatregelen							
A.8.1	Gebruikersapparatuur	Ja		X		Ja	
A.8.2	Speciale toegangsrechten	Ja		X	X	Ja	
A.8.3	Beperking toegang tot informatie	Ja		X	X	Ja	
A.8.4	Toegangsbeveiliging op broncode	Ja		X	X	Ja	
A.8.5	Beveiligde authenticatie	Ja		X	X	Ja	
A.8.6	Capaciteitsbeheer	Ja		X	X	Ja	
A.8.7	Bescherming tegen malware	Ja		X	X	Ja	
A.8.8	Beheer van technische kwetsbaarheden	Ja	X	X	X	Ja	
A.8.9	Configuratiebeheer	Ja		X	X	Ja	
A.8.10	Wissen van informatie	Ja	X	X		Ja	
A.8.11	Maskeren van gegevens	Ja	X	X		Ja	
A.8.12	Voorkomen van gegevenslekken (Data leakage prevention)	Ja	X	X	X	Ja	
A.8.13	Back-up van informatie	Ja		X	X	Ja	
A.8.14	Redundantie van informatieverwerkende faciliteiten	Ja		X	X	Ja	
A.8.15	Logging	Ja	X	X		Ja	
A.8.16	Monitoren van activiteiten	Ja	X	X		Ja	
A.8.17	Kloksynchronisatie	Ja		X		Ja	
A.8.18	Gebruik van speciale systeemhulpmiddelen	Ja		X	X	Ja	
A.8.19	Installeren van software op operationele systemen	Ja		X	X	Ja	
A.8.20	Beveiliging netwerkcomponenten	Ja		X		Ja	
A.8.21	Beveiliging van netwerkdiensten	Ja		X		Ja	
A.8.22	Netwerksegmentatie	Ja		X		Ja	
A.8.23	Toepassen van webfilters	Ja		X	X	Ja	
A.8.24	Gebruik van cryptografie	Ja	X	X	X	Ja	
A.8.25	Beveiligen tijdens de ontwikkelcyclus	Ja		X	X	Ja	
A.8.26	Toepassingsbeveiligingseisen	Ja		X	X	Ja	
A.8.27	Veilige systeemarchitectuur en technische uitgangspunten	Ja		X		Ja	
A.8.28	Veilig coderen	Ja		X	X	Ja	
A.8.29	Testen van de beveiliging tijdens ontwikkeling en acceptatie	Ja		X	X	Ja	
A.8.30	Uitbestede systeemontwikkeling	Nee					BKR besteedt dit niet uit
A.8.31	Scheiding van ontwikkel-, test- en productieomgevingen	Ja		X		Ja	

A.8.32	Wijzigingsbeheer	Ja		X	X	Ja	
A.8.33	Testgegevens	Ja		X		Ja	
A.8.34	Bescherming van informatiesystemen tijdens audits	Ja		X		Ja	