VERKLARING VAN TOEPASSELIJKHEID
NEN-EN-ISO/IEC 27001: 2023/A1:2024 NL

Code:	4448-06-01
Versie:	20
Versiedatum	16-09-2024
Gemaakt door:	Hijmen van Bloemendaal
Goedgekeurd door:	DvdM

Versieblad

Datum	Versie	Gemaakt door	Omschrijving van de aanpassing
02-02-2017	0.1	Dirk van den Muijsenberg	Concept basisdocument
15-02-2017	0.2	Hijmen van Bloemendaal	Kolom “Reden voor selectie/ non-selectie” gevuld en hier en daar kolom “Van toepassing (JA/NEE)” aangepast Termen aangepast aan nieuwste NEN document
20-02-2017	0.3	Hijmen van Bloemendaal	Kolom Beheersdoelstellingen gevuld Waar nodig kolom Implementatie methode leeggemaakt
22-02-2017	0.4	Hijmen van Bloemendaal	Diverse aanpassingen allo kolommen nu gevuld
15-03-2017	1.0	Hijmen van Bloemendaal	Alle punten doorlopen en status aangepast door Marc/Dirk en Hijmen
09-08-2017	1.1	Hijmen van Bloemendaal	Diverse punten nav bespreking
27-10-2017	1.2	Hijmen van Bloemendaal	
30-11-2017	1.2	Marc Siebers	Goedgekeurd
14-06-2018	1.4	Dirk van den Muijsenberg	Goedgekeurd
14-06-2018	1..5	Dirk van den Muijsenberg	Goedgekeurd
15-06-2018	1.6	Hijmen van Bloemendaal	Kleine aanpassingen en goedgekeurd
10-09-2018	1.7	Dirk	Diverse aanpassingen n.a.v. directieoverleg en tevens goedgekeurd.
18-09-2018	1.8	Hijmen	Schema restrisico’s verwijderd
22-07-2019	1.9	Hijmen	Aangepast nav aanpassingen in risicotabel
28-07-2020	1.10	Hijmen	Aangepast nav aanpassingen in risicotabel
04-08-2021	1.11	Hijmen	Kleine tekstuele aanpassingen en toevoegen laadlocatie (A.11.1.6) tevens goedgekeurd.
31-08-2021	1.12	Hijmen	Kleine tekstuele aanpassingen tevens goedgekeurd.

15-08-2022	13	Hijmen	Nieuwe opzet van de verklaring, nav nieuwe risicoanalyse
22-08-2022	13	Hijmen	Goedgekeurd
21-12-2022	14	Hijmen	Foute verwijzing naar documentatie aangepast en goedgekeurd.
11-01-2023	15	Hijmen	Lay-out aangepast
10-08-2023	16	Hijmen	Enkele aanpassingen naar aanleiding van Risicobeoordeling en goedkeuring.
15-03-2024	17	Dirk	Beheersdoelstelling 16.1.5. aangepast
18-06-2024	18	Hijmen	Transitie naar ISO 27001:2023 en tevens enkele aanpassingen naar aanleiding van eerdere audits (Issue 29835 en 29964) en beheersmaatregel toegevoegd m.b.t. klimaatverandering
02-09-2024	19	DvdM	Naamgeving was gebaseerd op de Engelse (2022) variant. Moet de Nederlandse (2023) zijn.
16-09-2024	20	Hijmen	Correcte naamgeving ook doorgevoerd in de titel
23-07-2025	21	Hijmen	Aanpassingen naar aanleiding van wijzigingen in de risicotabel, en toevoeging van de maatregel “Veilig gebruik van AI”

Inhoudsopgave

1. DOEL, TOEPASSINGSGEBIED EN GEBRUIKERS 5

2. GEREFEREERDE DOCUMENTEN 5

3. TOEPASSELIJKHEID VAN MAATREGELEN 6

4. GELDIGHEID EN DOCUMENTBEHEER 23

1. Doel, toepassingsgebied en gebruikers

Het doel van dit document is om maatregelen te definiëren die passend zijn om te implementeren binnen Xaurum, om de doelstellingen van deze maatregelen te bepalen en hoe ze zowel worden geïmplementeerd, als ook om restrisico's goed te keuren en het formeel goedkeuren van de implementatie van de genoemde maatregelen .

Dit document bevat alle maatregelen vermeld in Bijlage A van de NEN-EN-ISO/IEC 27001: 2023 NL norm. Maatregelen zijn van toepassing op het gehele Toepassingsgebied van het Managementsysteem voor Informatiebeveiliging (ISMS).

Gebruikers van dit document zijn alle werknemers van Xaurum die een rol hebben in het ISMS.

2. Gerefereerde documenten

- NEN-EN-ISO/IEC 27001: 2023 NL norm, clausule 6.1.3d)
- Informatiebeveiligingsbeleid
- Methodologie van Risicobeoordeling en Risicobehandeling
- Rapport van de Risicobeoordeling en Risicobehandeling

3. Toepasselijkheid van maatregelen

De volgende maatregelen van NEN-EN-ISO/IEC 27001: 2023 NL Bijlage A gelden:

Beheersmaatregelen Maatregelen volgens NEN-EN-ISO/IEC 27001: 2023 NL						
ID	**Titel**	**Beheersmaatregel**	**Rechtvaardiging**	**Van toepassing**	**Geïmplementeerd**	**Rechtvaardiging bij uitsluiting**
A.5	**Informatiebeveiligingsbeleid**					
A.5.1	Beleidsregels voor informatiebeveiliging	Informatiebeveiligingsbeleid en onderwerpspecifieke beleidsregels behoren te worden gedefinieerd, goedgekeurd door het management, gepubliceerd, gecommuniceerd aan en erkend door relevant personeel en relevante belanghebbenden en met geplande tussenpozen en als zich significante wijzigingen voordoen, te worden beoordeeld.	Risicobeoordeling nr. 4, 108, 1905	Ja	Ja	
A.5.2	Rollen en verantwoordelijkheden bij informatiebeveiliging	Rollen en verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie.	Risicobeoordeling nr. 2, 109	Ja	Ja	
A.5.3	Functiescheiding	Conflicterende taken en conflicterende verantwoordelijkheden behoren te worden gescheiden.	Risicobeoordeling nr. 114, 131, 147, 165, 3404, 3413, 3418, 3505, 3507	Ja	Ja	

A.5.4	Managementverantwoordelijkheden	Het management behoort van al het personeel te eisen dat ze informatiebeveiliging toepassen overeenkomstig het vastgestelde informatiebeveiligingsbeleid, de onderwerpspecifieke beleidsregels en procedures van de organisatie.	Risicobeoordeling nr. 1, 1301	Ja	Ja	
A.5.5	Contact met overheidsinstanties	De organisatie behoort contact met de relevante instanties te leggen en te onderhouden.	Risicobeoordeling nr. 22, 25, 2003, 2007	Ja	Ja	
A.5.6	Contact met speciale belangengroepen	De organisatie behoort contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en beroepsverenigingen te leggen en te onderhouden.	Risicobeoordeling nr. 23, 26, 2001, 2005	Ja	Ja	
A.5.7	Informatie en analyse over bedreigingen	Informatie met betrekking tot informatiebeveiligingsdreigingen behoort te worden verzameld en geanalyseerd om informatie over dreigingen te produceren.	Risicobeoordeling nr. 254, 332, 510, 1116, 1216, 1913, 6101, 6102			
A.5.8	Informatiebeveiliging in projectmanagement	Informatiebeveiliging behoort te worden geïntegreerd in projectmanagement.	Risicobeoordeling nr. 6, 102, 1503, 1916, 2503	Ja	Ja	
A.5.9	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	Er behoort een inventarislijst van informatie en andere gerelateerde bedrijfsmiddelen, met inbegrip van de eigenaren, te worden opgesteld en onderhouden.	Risicobeoordeling nr. 204, 243, 2402, 2405, 6101, 6102	Ja	Ja	
A.5.10	Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen	Regels voor het aanvaardbaar gebruik van en procedures voor het omgaan met informatie en andere gerelateerde bedrijfsmiddelen behoren te worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	Risicobeoordeling nr. 141, 214, 232, 237, 251, 309, 324, 1412, 1505, 1524, 1903, 2101, 2104, 2505	Ja	Ja	

A.5.11	Retourneren van bedrijfsmiddelen	Personeel en andere belanghebbenden, al naargelang de situatie, behoren alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst te retourneren	Risicobeoordeling nr. 245			
A.5.12	Classificeren van informatie	Informatie behoort te worden geclassificeerd volgens de informatiebeveiligingsbehoeften van de organisatie, op basis van de eisen voor vertrouwelijkheid, integriteit, beschikbaarheid en relevante eisen van belanghebbenden.	Risicobeoordeling nr. 138, 209, 1409, 1504, 1522, 1901, 2109, 2112, 2504	Ja	Ja	
A.5.13	Labelen van informatie	Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Risicobeoordeling nr. 1523, 1902, 2102	Ja	Ja	
A.5.14	Overdracht van informatie	Er behoren regels, procedures of overeenkomsten voor informatieoverdracht te zijn ingesteld voor alle soorten van communicatiefaciliteiten binnen de organisatie en tussen de organisatie en andere partijen.	Risicobeoordeling nr. 1408, 1423, 1513, 1909, 1911, 1917, 2513	Ja	Ja	
A.5.15	Toegangsbeveiliging	Er behoren regels op basis van bedrijfs- en informatiebeveiligingseisen te worden vastgesteld en geïmplementeerd om de fysieke en logische toegang tot informatie en andere gerelateerde bedrijfsmiddelen te beheersen.	Risicobeoordeling nr. 105, 107, 406, 806, 906, 1006, 1411, 1507, 2115, 2507, 3602, 3901	Ja	Ja	
A.5.16	Identiteitsbeheer	De volledige levenscyclus van identiteiten behoort te worden beheerd.	Risicobeoordeling nr. 242			

A.5.17	Beheren van authenticatie-informatie	De toewijzing en het beheer van authenticatie-informatie behoort te worden beheerst door middel van een beheerproces waarvan het adviseren van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt	Risicobeoordeling nr. 104, 110, 112, 116, 129, 139, 210, 807, 810, 907, 910, 1007, 1010, 1410	Ja	Ja	
A.5.18	Toegangsrechten	Toegangsrechten voor informatie en andere gerelateerde bedrijfsmiddelen behoren te worden verstrekt, beoordeeld, aangepast en verwijderd overeenkomstig het onderwerpspecifieke beleid en de regels inzake toegangsbeveiliging van de organisatie.	Risicobeoordeling nr. 113, 130, 140, 211, 244, 2201	Ja	Ja	
A.5.19	Informatiebeveiliging in leveranciersrelaties	Er behoren processen en procedures te worden vastgesteld en geïmplementeerd om de informatiebeveiligingsrisico's in verband met het gebruik van producten of diensten van de leverancier te beheersen.	Risicobeoordeling nr. 174, 1307, 1416, 1801, 1805, 3401, 3501, 3616, 3624, 3628, 3707	Ja	Ja	
A.5.20	Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Relevante informatiebeveiligingseisen behoren te worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie te worden overeengekomen.	Risicobeoordeling nr. 1417, 1802, 1806, 3403, 3503, 3509, 3617, 3625, 3629, 3708	Ja	Ja	
A.5.21	Beheer van informatiebeveiliging in de ICT-keten	Er behoren processen en procedures te worden bepaald en geïmplementeerd om de informatiebeveiligingsrisico's in verband met de toeleveringsketen van ICT-producten en -diensten te beheersen.	Risicobeoordeling nr. 1418, 1803, 1807, 3618, 3626, 3630, 3709	Ja	Ja	

A.5.22	Monitoring, beoordeling en beheren van wijzigingen van leveranciersdiensten	De organisatie behoort de informatiebeveiligingspraktijken en de dienstverlening van leveranciers regelmatig te monitoren, beoordelen, evalueren en veranderingen daaraan te beheren	Risicobeoordeling nr. 1804, 3504, 3601, 3612, 3619, 3627, 3631, 3710, 4101, 4201	Ja	Ja	
A.5.23	Informatiebeveiliging voor het gebruik van cloud diensten	Processen voor het aanschaffen, gebruiken, beheren en beëindigen van clouddiensten behoren overeenkomstig de informatiebeveiligingseisen van de organisatie te worden opgesteld.	Risicobeoordeling nr. 603, 826, 833, 926, 931, 1021, 3611, 3620	Ja	Ja	
A.5.24	Planning en voorbereiding van het beheer informatiebeveiligingsincidenten	De organisatie behoort plannen op te stellen voor, en zich voor te bereiden op, het beheren van informatiebeveiligingsincidenten door processen, rollen en verantwoordelijkheden voor het beheer van informatiebeveiligingsincidenten te definiëren, vast te stellen en te communiceren.	Risicobeoordeling nr. 3609, 3705	Ja	Ja	
A.5.25	Beoordelen van- en besluit over informatiebeveiligingsgebeurtenissen	De organisatie behoort informatiebeveiligingsgebeurtenissen te beoordelen en te beslissen of ze moeten worden gecategoriseerd als informatiebeveiligingsincidenten.	Risicobeoordeling nr. 8	Ja	Ja	
A.5.26	Reageren op informatiebeveiligingsincidenten	Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures en contractuele afspraken.	Risicobeoordeling nr. 9	ja	Ja	

A.5.27	Leren van informatiebeveiligingsincidenten	Kennis die is opgedaan met informatiebeveiligingsincidenten behoort te worden gebruikt om de beheersmaatregelen voor informatiebeveiliging te versterken en te verbeteren.	Risicobeoordeling nr. 10	Ja	Ja	
A.5.28	Verzameling van bewijsmateriaal	De organisatie behoort procedures vast te stellen en te implementeren voor het identificeren, verzamelen, verkrijgen en bewaren van bewijs met betrekking tot informatiebeveiligingsgebeurtenissen om schade door onvoldoende bewijs uit te sluiten.	Risicobeoordeling nr.253, 511, 1109, 1114, 1215, 1228	Ja	Ja	
A.5.29	Informatiebeveiliging tijdens een verstoring	De organisatie behoort plannen te maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.	Risicobeoordeling nr. 11, 14, 1906, 3606, 3621, 3701	Ja	Ja	
A.5.30	ICT-gereedheid voor bedrijfscontinuïteit	De ICT-gereedheid behoort te worden gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfscontinuïteitsdoelstellingen en ICT-continuïteitseisen.	Risicobeoordeling nr. 12, 15, 1907, 3607, 3622, 3702	Ja	Ja	
A.5.31	Wettelijke, statutaire, regelgevende en contractuele eisen	Wettelijke, statutaire, regelgevende en contractuele eisen die relevant zijn voor informatiebeveiliging en de aanpak van de organisatie om aan deze eisen te voldoen, behoren te worden geïdentificeerd, gedocumenteerd en actueel gehouden.	Risicobeoordeling nr. 172, 913, 1701, 2002	Ja	Ja	
A.5.32	Intellectueel eigendomsrecht	De organisatie behoort passende procedures te implementeren om intellectuele-eigendomsrechten te beschermen.	Risicobeoordeling nr. 1702, 5101	Ja	Ja	

A.5.33	Beschermen van registraties	Registraties behoren te worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave.	Risicobeoordeling nr. 1528, 1703	Ja	Ja	
A.5.34	Privacy en bescherming van persoonsgegevens	De organisatie behoort de eisen met betrekking tot het behoud van privacy en de bescherming van persoonsgegevens volgens de toepasselijke wet- en regelgeving en contractuele eisen te identificeren en eraan te voldoen.	Risicobeoordeling nr. 1704	Ja	Ja	
A.5.35	Onafhankelijke beoordeling van informatiebeveiliging	De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan, met inbegrip van mensen, processen en technologieën, behoren onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, te worden beoordeeld.	Risicobeoordeling nr. 28	Ja	Ja	
A.5.36	Naleving van beleidslijnen en normen voor informatiebeveiliging	De naleving van het informatiebeveiligingsbeleid, het onderwerpspecifieke beleid, regels en de normen van de organisatie behoort regelmatig te worden beoordeeld.	Risicobeoordeling nr. 13, 29	Ja	Ja	
A.5.37	Gedocumenteerde bedieningsprocedures	Bedieningsprocedures voor informatieverwerkende faciliteiten behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan het personeel dat ze nodig heeft.	Risicobeoordeling nr. 248, 329, 2304, 2407	Ja	Ja	
A.6	**Maatregelen tav mensen**					

A.6.1	Screening	De achtergrond van alle kandidaten voor een dienstverband behoort te worden gecontroleerd voordat ze bij de organisatie in dienst treden en daarna op gezette tijden te worden herhaald. Hierbij behoort rekening te worden gehouden met de toepasselijke wet- en regelgeving en ethische overwegingen, en deze controle behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.	Risicobeoordeling nr. 121, 3408	Ja	Ja	
A.6.2	Arbeidsovereenkomst	In arbeidsovereenkomsten behoort te worden vermeld wat de verantwoordelijkheden van het personeel en van de organisatie zijn wat betreft informatiebeveiliging.	Risicobeoordeling nr. 16, 18, 20, 101, 103, 117, 120, 151, 1501, 1506, 2114, 2501, 2506, 3402, 3407, 3502, 3508	Ja	Ja	
A.6.3	Bewustwording van, opleiding en training in informatiebeveiliging	Personeel van de organisatie en relevante belanghebbenden behoren een passende bewustwording van, opleiding en training in informatiebeveiliging en regelmatige updates over het informatiebeveiligingsbeleid, onderwerpspecifieke beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie, te krijgen.	Risicobeoordeling nr. 3, 21, 24, 111, 125, 144, 148, 155, 166, 203, 220, 227, 231, 238, 252, 320, 330, 412, 507, 701, 820, 830, 834, 922, 932, 1102, 1104, 1112, 1120, 1204, 1212, 1224, 1525, 1601, 1910, 1912, 2006, 2103, 2105, 2401, 2403, 2406, 2516, 2604, 3411, 3415, 3632, 3711	Ja	Ja	
A.6.4	Disciplinaire procedure	Er behoort een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen personeel en andere belanghebbenden die zich schuldig hebben gemaakt aan een schending van het informatiebeveiligingsbeleid.	Risicobeoordeling nr. 118, 122, 152, 2004, 2008, 3405, 3409, 3506	Ja	Ja	

A.6.5	Verantwoordelijkheden na beëindiging of wijziging van het dienstverband	Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband, behoren te worden gedefinieerd, gehandhaafd en gecommuniceerd aan relevant personeel en andere belanghebbenden.	Risicobeoordeling nr. 246, 327, 2303, 2404	Ja	Ja	
A.6.6	Vertrouwelijkheids- of geheimhoudingsovereenkomsten	Vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie inzake de bescherming van informatie weerspiegelen, behoren te worden geïdentificeerd, gedocumenteerd, regelmatig te worden beoordeeld en ondertekend door personeel en andere relevante belanghebbenden.	Risicobeoordeling nr. 801, 901, 1001, 1502, 2113, 2502, 5102	Ja	Ja	
A.6.7	Werken op afstand	Wanneer personeel op afstand werkt, behoren er beveiligingsmaatregelen te worden geïmplementeerd om informatie te beschermen die buiten het gebouw en/of terrein van de organisatie wordt ingezien, verwerkt of opgeslagen.	Risicobeoordeling nr. 205, 213, 222, 239, 304, 308, 313, 2508	Ja	Ja	
A.6.8	Melden van informatiebeveiligingsgebeurtenissen	De organisatie behoort te voorzien in een mechanisme waarmee personeel waargenomen of vermoede informatiebeveiligingsgebeurtenissen tijdig via passende kanalen kan melden.	Risicobeoordeling nr. 146, 836, 934, 1527, 3610, 3706, 5101, 5102	ja	Ja	
A.7	**Fysieke maatregelen**					
A.7.1	Fysieke beveiligingszone	Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, behoren te worden beschermd door beveiligingszones te definiëren en te gebruiken.	Risicobeoordeling nr. 2202, 2601	Ja	Ja	

A.7.2	Fysieke toegangsbeveiliging	Beveiligde zones behoren te worden beschermd door passende toegangsbeveiligingsmaatregelen en toegangspunten.	Risicobeoordeling nr. 2203, 2602	Ja	Ja	
A.7.3	Beveiligen van kantoren, ruimten en faciliteiten	Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en geïmplementeerd.	Risicobeoordeling nr. 2204	Ja	Ja	
A.7.4	Monitoren van fysieke beveiliging	Het gebouw en terrein behoort voortdurend te worden gemonitord op onbevoegde fysieke toegang.	Risicobeoordeling nr. 2205	Ja	Ja	
A.7.5	Beschermen tegen fysieke en omgevingsbedreigingen	Er behoort bescherming tegen fysieke en omgevingsdreigingen, zoals natuurrampen en andere opzettelijke of onopzettelijke fysieke dreigingen voor de infrastructuur, te worden ontworpen en geïmplementeerd.	Risicobeoordeling nr. 2206, 2603	Ja	Ja	
A.7.6	Werken in beveiligde zones	Voor het werken in beveiligde zones behoren beveiligingsmaatregelen te worden ontwikkeld en geïmplementeerd.	Risicobeoordeling nr. 2207	Ja	Ja	
A.7.7	Clear desk en clear screen	Er behoren ‘clear desk’-regels voor papieren documenten en verwijderbare opslagmedia en ‘clear screen’-regels voor informatieverwerkende faciliteiten te worden gedefinieerd en op passende wijze te worden afgedwongen. Doel hiervan is om te voorkomen dat gegeven die vertrouwelijk zijn niet door onbevoegden gezien kan worden.	Risicobeoordeling nr. 208, 216, 224, 229, 235, 241, 1515, 2106, 2514	Ja	Ja	
A.7.8	Plaatsen en beschermen van apparatuur	Apparatuur behoort veilig te worden geplaatst en beschermd.	Risicobeoordeling nr. 3603, 3613	Ja	Ja	
A.7.9	Beveiliging van bedrijfsmiddelen buiten de bedrijfsruimten	Bedrijfsmiddelen buiten het gebouw en/of terrein behoren te worden beschermd.	Risicobeoordeling nr. 207, 215, 223, 233, 240, 247, 306, 311, 315, 321, 325, 328	Ja	Ja	

A.7.10	Opslagmedia	Opslagmedia behoren te worden beheerd gedurende hun volledige levenscyclus van aanschaf, gebruik, transport en verwijdering overeenkomstig het classificatieschema en de hanteringseisen van de organisatie.	Risicobeoordeling nr. 404, 405, 408, 410	Ja	Ja	
A.7.11	Nutsvoorzieningen	Informatieverwerkende faciliteiten behoren te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen.	Risicobeoordeling nr. 1225, 2302, 3604, 3703, 3801	Ja	Ja	
A.7.12	Beveiligen van bekabeling	Voedingskabels en kabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen onderschepping, interferentie of beschadiging.	Risicobeoordeling nr. 605, 608	Ja	Ja	
A.7.13	Onderhoud van de apparatuur	Apparatuur behoort op de juiste wijze te worden onderhouden om de beschikbaarheid, integriteit en betrouwbaarheid van informatie te garanderen.	Risicobeoordeling nr. 2301, 3605, 3615, 4001	Ja	Ja	
A.7.14	Veilig verwijderen of hergebruik van apparatuur	Onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden gecontroleerd om te waarborgen dat gevoelige gegevens en gelicentieerde software zijn verwijderd of veilig zijn overschreven voordat ze worden verwijderd of hergebruikt.	Risicobeoordeling nr. 206, 221, 228, 305, 314, 318, 326	Ja	Ja	
A.8	**Fysieke maatregelen**					
A.8.1	Eindgebruikers apparatuur	Informatie die is opgeslagen op, wordt verwerkt door of toegankelijk is via ‘user endpoint devices’ behoort te worden beschermd.	Risicobeoordeling nr. 202, 212, 219, 226, 234, 236, 250, 255, 303, 307, 312, 317, 322, 323, 1517, 2107, 2515	Ja	Ja	

A.8.2	Speciale toegangsrechten	Het toewijzen en het gebruik van speciale toegangsrechten behoort te worden beperkt en beheerd.	Risicobeoordeling nr. 17, 19, 119, 123, 132, 142	Ja	Ja	
A.8.3	Beperking toegang tot informatie	De toegang tot informatie en andere gerelateerde bedrijfsmiddelen behoort te worden beperkt overeenkomstig het vastgestelde onderwerpspecifieke beleid inzake toegangsbeveiliging.	Risicobeoordeling nr. 115, 133, 149, 168, 5102	Ja	Ja	
A.8.4	Toegangsbeveiliging op broncode	Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken behoort op passende wijze te worden beheerd.	Risicobeoordeling nr. 135, 169	Ja	Ja	
A.8.5	Beveiligde authenticatie	Er behoren beveiligde authenticatietechnologieën en -procedures te worden geïmplementeerd op basis van beperkingen van de toegang tot informatie en het onderwerpspecifieke beleid inzake toegangsbeveiliging.	Risicobeoordeling nr. 106	Ja	Ja	
A.8.6	Capaciteitsbeheer	Het gebruik van middelen behoort te worden gemonitord en aangepast overeenkomstig de huidige en verwachte capaciteitseisen.	Risicobeoordeling nr. 832, 930, 1122	Ja	Ja	
A.8.7	Bescherming tegen malware	Bescherming tegen malware behoort te worden geïmplementeerd en ondersteund door een passend gebruikersbewustzijn.	Risicobeoordeling nr. 249, 509, 1115, 1214	Ja	Ja	
A.8.8	Beheer van technische kwetsbaarheden	Er behoort informatie te worden verkregen over technische kwetsbaarheden van in gebruik zijnde informatiesystemen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden behoort te worden geëvalueerd en er behorende passende maatregelen te worden getroffen.	Risicobeoordeling nr. 7, 153, 170, 1106, 1207, 1420, 1904	Ja	Ja	

A.8.9	Configuratiebeheer	Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken behoren te worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld.	Risicobeoordeling nr. 502, 602	Ja	Ja	
A.8.10	Wissen van Informatie	In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie behoort te worden gewist als deze niet langer vereist is.	Risicobeoordeling nr. 126, 218, 813, 821, 920, 1013, 1424, 1516, 1602, 2110	Ja	Ja	
A.8.11	Maskeren van gegevens	Gegevens behoren te worden gemaskeerd overeenkomstig het onderwerpspecifieke beleid inzake toegangsbeveiliging en andere gerelateerde onderwerpspecifieke beleidsregels, en bedrijfseisen van de organisatie, rekening houdend met de toepasselijke wetgeving.	Risicobeoordeling nr. 127, 814, 822, 921, 1014	Ja	Ja	
A.8.12	Voorkomen van gegevenslekken	Maatregelen om gegevenslekken te voorkomen behoren te worden toegepast in systemen, netwerken en andere apparaten waarop of waarmee gevoelige informatie wordt verwerkt, opgeslagen of getransporteerd.	Risicobeoordeling nr. 27, 128, 137, 217, 225, 230, 310, 316, 319, 407, 409, 411, 702, 823, 923, 1426, 1514, 1518, 2108, 2111, 3417, 3420, 5102	Ja	Ja	
A.8.13	Back-up van Informatie	Back-ups van informatie, software en systemen behoren te worden bewaard en regelmatig te worden getest overeenkomstig het overeengekomen onderwerpspecifieke beleid inzake back-ups.	Risicobeoordeling nr. 508, 824, 924, 1019, 1113, 1213, 1303, 1405, 1427, 1512, 1918, 2512	Ja	Ja	
A.8.14	Redundantie van informatieverwerkende faciliteiten	Informatieverwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Risicobeoordeling nr. 201, 3608, 3704, 3903	Ja	Ja	

A.8.15	Logging	Er behoren logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, te worden geproduceerd, opgeslagen, beschermd en geanalyseerd.	Risicobeoordeling nr. 136, 143, 1123, 1124, 1125, 1406, 1510, 1914, 2511	Ja	Ja	
A.8.16	Monitoren van activiteiten	Netwerken, systemen en toepassingen behoren te worden gemonitord op afwijkend gedrag en er behoren passende maatregelen te worden getroffen om potentiële informatiebeveiligingsincidenten te evalueren.	Risicobeoordeling nr. 124, 1126, 1407, 1511, 1915	Ja	Ja	
A.8.17	Kloksynchronisatie	De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt, behoren te worden gesynchroniseerd met goedgekeurde tijdsbronnen.	Risicobeoordeling nr. 1127	Ja	Ja	
A.8.18	Gebruik van speciale systeemhulpmiddelen	Het gebruik van systeemhulpmiddelen die in staat kunnen zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen, behoort te worden beperkt en nauwkeurig te worden gecontroleerd.	Risicobeoordeling nr. 134	Ja	Ja	
A.8.19	Installeren van software op operationele systemen	Er behoren procedures en maatregelen te worden geïmplementeerd om het installeren van software op operationele systemen op veilige wijze te beheren.	Risicobeoordeling nr. 1101, 1201, 1203, 1205	Ja	Ja	
A.8.20	Beveiliging Netwerkcomponenten	Netwerken en netwerkapparaten behoren te worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Risicobeoordeling nr. 604, 804, 904, 1218, 1221, 1223, 1226, 1302, 1401, 1403, 1413, 1508, 1519, 2509, 3614	Ja	Ja	

A.8.21	Beveiliging van netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen voor alle netwerkdiensten behoren te worden geïdentificeerd, geïmplementeerd en gemonitord.	Risicobeoordeling nr. 501, 503, 506, 601, 607, 805, 817, 905, 917, 1005, 1017, 1219, 1222, 1227, 1229, 1402, 1404, 1414, 1509, 1520, 2510, 3902, 4002	Ja	Ja	
A.8.22	Netwerksegmentatie	Groepen informatiediensten, gebruikers en informatiesystemen behoren in de netwerken van de organisatie te worden gesegmenteerd.	Risicobeoordeling nr. 504, 606, 608, 1415, 1521	Ja	Ja	
A.8.23	Toepassen van webfilters	De toegang tot externe websites behoort te worden beheerd om de blootstelling aan kwaadaardige inhoud te beperken.	Risicobeoordeling nr. 255, 331, 1217, 1220	Ja	Ja	
A.8.24	Gebruik van cryptografie	Regels voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, behoren te worden gedefinieerd en geïmplementeerd in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving en veiligheidsvoorschriften. Dit is van belang om een betrouwbare applicatie te kunnen leveren welke voldoet aan eisen van stakeholders.	Risicobeoordeling nr. 173, 809, 811, 909, 911, 914, 1009, 1011, 1425	Ja	Ja	
A.8.25	Beveiligen tijdens de ontwikkelcyclus	Voor het veilig ontwikkelen van software en systemen behoren regels te worden vastgesteld en toegepast.	Risicobeoordeling nr. 158, 1107, 1208	Ja	Ja	
A.8.26	Toepassingsbeveiligingseisen	Er behoren eisen aan de informatiebeveiliging te worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen.	Risicobeoordeling nr. 505	Ja	Ja	

A.8.27	Veilige systeemarchitectuur en technische uitgangspunten	Uitgangspunten voor het ontwerpen van beveiligde systemen behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle activiteiten betreffende het ontwikkelen van informatiesystemen.	Risicobeoordeling nr. 145, 156, 161, 171, 835, 933, 1110, 1210, 1421, 1526	Ja	Ja	
A.8.28	Veilig coderen	Er behoren principes voor veilig coderen te worden toegepast op softwareontwikkeling.	Risicobeoordeling nr. 159, 1108, 1209	Ja	Ja	
A.8.29	Testen van beveiliging tijdens ontwikkeling en acceptatie	Processen voor het testen van de beveiliging behoren te worden gedefinieerd en geïmplementeerd in de ontwikkelcyclus.	Risicobeoordeling nr. 163, 803, 812, 816, 819, 828, 831, 903, 912, 916, 919, 928, 1003, 1012, 1016, 1111, 1118, 1121, 1132, 1211, 1422	Ja	Ja	
A.8.30	Uitbestede systeemontwikkeling	De organisatie behoort de activiteiten in verband met uitbestede systeemontwikkeling te sturen, bewaken en beoordelen.	Risicobeoordeling nr. 3406, 3410, 3412, 3414, 3416, 3419	Ja	Ja	
A.8.31	Scheiding van ontwikkel-, test- en productieomgevingen	Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden en beveiligd.	Risicobeoordeling nr. 157, 162, 802, 808, 815, 827, 902, 908, 915, 927, 1002, 1004, 1008, 1015, 1117			
A.8.32	Wijzigingsbeheer	Wijzigingen in informatieverwerkende faciliteiten en informatiesystemen behoren onderworpen te zijn aan procedures voor wijzigingsbeheer.	Risicobeoordeling nr. 150, 154, 160, 167, 1103, 1105, 1128, 1202, 1206, 1419	Ja	Ja	
A.8.33	Testgegevens	Testgegevens behoren op passende wijze te worden geselecteerd, beschermd en beheerd.	Risicobeoordeling nr. 164, 818, 825, 829, 918, 925, 929, 1018, 1020, 1119	Ja	Ja	
A.8.34	Bescherming van informatiesystemen tijdens audits	Audittests en andere auditactiviteiten waarbij operationele systemen worden beoordeeld, behoren te worden gepland en overeengekomen tussen de tester en het verantwoordelijke management.	Risicobeoordeling nr. 30, 1908	Ja	Ja	

A.9.1	Maatergelen in het kader van klimaatverandering	De organisatie behoort maatregelen te nemen in het kader van klimaatverandering	Risicobeoordeling nr. 2208, 3623, 3633, 4102	Ja	Ja	
A.9.2	Veilig gebruik van AI	Maatregelen om veilig gebruik van AI te borgen	Risicobeoordeling nr. 27-A, 128-A, 146-A, 837, 935	Ja	Ja	

4. Geldigheid en documentbeheer

De eigenaar van dit document is de ISMS Projectmanager, die het document dient te controleren en indien noodzakelijk minstens één keer per jaar, dien te bewerken en direct na een risicoherbeoordeling en updates aan de Tabel voor Risicobeoordeling en Tabel voor Risicobehandeling

Wanneer de doeltreffendheid en toereikendheid van dit document worden beoordeeld, dan dienen de volgende criteria in ogenschouw te worden genomen:

- aantal afwijkingen door een onduidelijke implementatiemethode van afzonderlijke maatregelen
- aantal afwijkingen door een onduidelijke definitie van maatregelen
- aantal maatregelen waarvan het resultaat van de maatregelen niet gemeten kunnen worden