THALASSA CLOUD SERVICES B.V.

ISO/IEC 27001:2022 · Annex A

Verklaring van Toepasselijkheid

Thalassa Cloud Services B.V. hanteert een ISMS conform ISO/IEC 27001:2022 om risico’s rond vertrouwelijkheid, integriteit en beschikbaarheid van informatie in onze clouddienstverlening systematisch te beheersen. Beleid en beheersmaatregelen worden periodiek beoordeeld en waar nodig aangescherpt.

Deze verklaring van toepasselijkheid (VvT) geeft per Annex A-control aan of de maatregel binnen ons ISMS van toepassing is. In deze openbare versie voor (potentiële) klanten zijn alleen control, titel en toepasbaarheid opgenomen; aanvullende informatie delen wij waar relevant onder geheimhouding.

Versie v1.4.0 · Datum 29-10-2026

---

93 controls · **91** toepasbaar · **2** niet toepasbaar

A.5 Organisatorische beheersmaatregelen

Control	Titel	Toepasbaar
A.5.1	Beleidsregels voor informatiebeveiliging	Ja
A.5.2	Rollen en verantwoordelijkheden bij informatiebeveiliging	Ja
A.5.3	Functiescheiding	Ja
A.5.4	Managementverantwoordelijkheden	Ja
A.5.5	Contact met overheidsinstanties	Ja
A.5.6	Contact met speciale belangengroepen	Ja
A.5.7	Informatie en analyses over dreigingen	Ja
A.5.8	Informatiebeveiliging in projectmanagement	Ja
A.5.9	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	Ja
A.5.10	Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen	Ja
A.5.11	Retourneren van bedrijfsmiddelen	Ja
A.5.12	Classificeren van informatie	Ja
A.5.13	Labelen van informatie	Ja
A.5.14	Overdragen van informatie	Ja
A.5.15	Toegangsbeveiliging	Ja
A.5.16	Identiteitsbeheer	Ja
A.5.17	Authenticatie-informatie	Ja
A.5.18	Toegangsrechten	Ja
A.5.19	Informatiebeveiliging in leveranciersrelaties	Ja
A.5.20	Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Ja
A.5.21	Beheren van informatiebeveiliging in de ICT-toeleveringsketen	Ja
A.5.22	Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	Ja
A.5.23	Informatiebeveiliging voor het gebruik van clouddiensten	Ja
A.5.24	Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten	Ja
A.5.25	Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen	Ja
A.5.26	Reageren op informatiebeveiligingsincidenten	Ja
A.5.27	Leren van informatiebeveiligingsincidenten	Ja
A.5.28	Verzamelen van bewijsmateriaal	Ja
A.5.29	Informatiebeveiliging tijdens een verstoring	Ja
A.5.30	ICT-gereedheid voor bedrijfscontinuïteit	Ja
A.5.31	Wettelijke, statutaire, regelgevende en contractuele eisen	Ja
A.5.32	Intellectuele-eigendomsrechten	Ja
A.5.33	Beschermen van registraties	Ja
A.5.34	Privacy en bescherming van persoonsgegevens	Ja
A.5.35	Onafhankelijke beoordeling van informatiebeveiliging	Ja
A.5.36	Naleving van beleid, regels en normen voor informatiebeveiliging	Ja
A.5.37	Gedocumenteerde bedieningsprocedures	Ja

A.6 Mensgerichte beheersmaatregelen

Control	Titel	Toepasbaar
A.6.1	Screening	Ja
A.6.2	Arbeidsovereenkomst	Ja
A.6.3	Bewustwording van, opleiding en training in informatiebeveiliging	Ja
A.6.4	Disciplinaire procedure	Ja
A.6.5	Verantwoordelijkheden na beëindiging of wijziging van het dienstverband	Ja
A.6.6	Vertrouwelijkheids- of geheimhoudingsovereenkomsten	Ja
A.6.7	Werken op afstand	Ja
A.6.8	Melden van informatiebeveiligingsgebeurtenissen	Ja

A.7 Fysieke beheersmaatregelen

Control	Titel	Toepasbaar
A.7.1	Fysieke beveiligingszones	Ja
A.7.2	Fysieke toegangsbeveiliging	Ja
A.7.3	Beveiligen van kantoren, ruimten en faciliteiten	Ja
A.7.4	Monitoren van de fysieke beveiliging	Ja
A.7.5	Beschermen tegen fysieke en omgevingsdreigingen	Ja
A.7.6	Werken in beveiligde zones	Ja
A.7.7	Clear desk’ en ‘clear screen’	Ja
A.7.8	Plaatsen en beschermen van apparatuur	Ja
A.7.9	Beveiligen van bedrijfsmiddelen buiten het terrein	Ja
A.7.10	Opslagmedia	Ja
A.7.11	Nutsvoorzieningen	**Nee**
A.7.12	Beveiligen van bekabeling	Ja
A.7.13	Onderhoud van apparatuur	Ja
A.7.14	Veilig verwijderen of hergebruiken van apparatuur	Ja

A.8 Technologische beheersmaatregelen

Control	Titel	Toepasbaar
A.8.1	User endpoint devices’	Ja
A.8.2	Speciale toegangsrechten	Ja
A.8.3	Beperking toegang tot informatie	Ja
A.8.4	Toegangsbeveiliging op broncode	Ja
A.8.5	Beveiligde authenticatie	Ja
A.8.6	Capaciteitsbeheer	Ja
A.8.7	Bescherming tegen malware	Ja
A.8.8	Beheer van technische kwetsbaarheden	Ja
A.8.9	Configuratiebeheer	Ja
A.8.10	Wissen van informatie	Ja
A.8.11	Maskeren van gegevens	Ja
A.8.12	Voorkomen van gegevenslekken (data leakage prevention)	Ja
A.8.13	Back-up van informatie	Ja
A.8.14	Redundantie van informatieverwerkende faciliteiten	Ja
A.8.15	Logging	Ja
A.8.16	Monitoren van activiteiten	Ja
A.8.17	Kloksynchronisatie	Ja
A.8.18	Gebruik van speciale systeemhulpmiddelen	Ja
A.8.19	Installeren van software op operationele systemen	Ja
A.8.20	Beveiliging netwerkcomponenten	Ja
A.8.21	Beveiliging van netwerkdiensten	Ja
A.8.22	Netwerksegmentatie	Ja
A.8.23	Toepassen van webfilters	Ja
A.8.24	Gebruik van cryptografie	Ja
A.8.25	Beveiligen tijdens de ontwikkelcyclus	Ja
A.8.26	Toepassingsbeveiligingseisen	Ja
A.8.27	Veilige systeemarchitectuur en technische uitgangspunten	Ja
A.8.28	Veilig coderen	Ja
A.8.29	Testen van de beveiliging tijdens ontwikkeling en acceptatie	Ja
A.8.30	Uitbestede systeemontwikkeling	**Nee**
A.8.31	Scheiding van ontwikkel-, test- en productieomgevingen	Ja
A.8.32	Wijzigingsbeheer	Ja
A.8.33	Testgegevens	Ja
A.8.34	Bescherming van informatiesystemen tijdens audits	Ja