

Verklaring van Toepasselijkheid (VvT)

Deze verklaring bevat een overzicht van alle ISO 27001:2022 Annex A Beheersmaatregelen, waarbij per beheersmaatregel wordt aangegeven of deze maatregel wel of niet van toepassing is en de manier waarop de maatregel in onze organisatie is geïmplementeerd.

Scope

Ons informatiebeveiligingsmanagementsysteem (ISMS) heeft betrekking op alle interne en externe medewerkers van Aenova en omvat het ontwikkelen, verkopen, hosten, ondersteunen en onderhouden van workforce management systemen van Aenova.

Beheersmaatregelen

Beheersmaatregel	Relevant	Reden	Status
A.5.1 Beleidsregels voor informatiebeveiliging	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.2 Rollen en verantwoordelijkheden bij informatiebeveiliging	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.3 Functiescheiding	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.4 Managementverantwoordelijkheden	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.5 Contact met overheidsinstanties	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.6 Contact met speciale belangengroepen	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.7 Informatie en analyses over dreigingen	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.8 Informatiebeveiliging in projectmanagement	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.9 Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.10 Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.11 Retourneren van bedrijfsmiddelen	JA	Risicobeoordeling en -beheersing	Geïmplementeerd

Beheersmaatregel	Relevant	Reden	Status
A.5.12 Classificeren van informatie	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.13 Labelen van informatie	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.14 Overdragen van informatie	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.15 Toegangsbeveiliging	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.16 Identiteitsbeheer	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.17 Authenticatie-informatie	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.18 Toegangsrechten	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.19 Informatiebeveiliging in leveranciersrelaties	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.20 Adresseren van informatiebeveiliging in leveranciersovereenkomsten	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.21 Beheren van informatiebeveiliging in de ICT-keten	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.22 Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.23 Informatiebeveiliging voor het gebruik van clouddiensten	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.24 Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.25 Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.26 Reageren op informatiebeveiligingsincidenten	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.27 Leren van informatiebeveiligingsincidenten	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.28 Verzamelen van bewijsmateriaal	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.29 Informatiebeveiliging tijdens een verstoring	JA	Risicobeoordeling en -beheersing	Geïmplementeerd

Beheersmaatregel	Relevant	Reden	Status
A.5.30 ICT-gereedheid voor bedrijfscontinuïteit	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.31 Wettelijke, statutaire, regelgevende en contractuele eisen	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.32 Intellectuele eigendomsrechten	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.33 Beschermen van registraties	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.34 Privacy en bescherming van persoonsgegevens	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.35 Onafhankelijke beoordeling van informatiebeveiliging	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.36 Naleving van beleid, regels en normen voor informatiebeveiliging	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.5.37 Gedocumenteerde bedieningsprocedures	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.6.1 Screening	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.6.2 Arbeidsovereenkomst	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.6.3 Bewustwording van, opleiding en training in informatiebeveiliging	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.6.4 Disciplinaire procedure	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.6.5 Verantwoordelijkheden na beëindiging of wijziging van het dienstverband	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.6.6 Vertrouwelijkheids- of geheimhoudingsovereenkomsten	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.6.7 Werken op afstand	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.6.8 Melden van informatiebeveiligingsgebeurtenissen	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.7.1 Fysieke beveiligingszones	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.7.2 Fysieke toegangsbeveiliging	JA	Risicobeoordeling en -beheersing	Geïmplementeerd

Beheersmaatregel	Relevant	Reden	Status
A.7.3 Beveiligen van kantoren, ruimten en faciliteiten	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.7.4 Monitoren van de fysieke beveiliging	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.7.5 Beschermen tegen fysieke en omgevingsdreigingen	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.7.6 Werken in beveiligde zones	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.7.7 'Clear desk' en 'clear screen'	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.7.8 Plaatsen en beschermen van apparatuur	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.7.9 Beveiligen van bedrijfsmiddelen buiten het terrein	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.7.10 Opslagmedia	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.7.11 Nutsvoorzieningen	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.7.12 Beveiligen van bekabeling	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.7.13 Onderhoud van apparatuur	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.7.14 Veilig verwijderen of hergebruiken van apparatuur	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.8.1 'User endpoint devices'	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.8.2 Speciale toegangsrechten	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.8.3 Beperking toegang tot informatie	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.8.4 Toegangsbeveiliging op broncode	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.8.5 Beveiligde authenticatie	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.8.6 Capaciteitsbeheer	JA	Risicobeoordeling en -beheersing	Geïmplementeerd

Beheersmaatregel	Relevant	Reden	Status
A.8.7 Bescherming tegen malware	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.8.8 Beheer van technische kwetsbaarheden	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.8.9 Configuratiebeheer	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.8.10 Wissen van informatie	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.8.11 Maskeren van gegevens	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.8.12 Voorkomen van gegevenslekken (Data leakage prevention)	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.8.13 Back-up van informatie	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.8.14 Redundantie van informatieverwerkende faciliteiten	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.8.15 Logging	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.8.16 Monitoren van activiteiten	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.8.17 Kloksynchronisatie	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.8.18 Gebruik van speciale systeemhulpmiddelen	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.8.19 Installeren van software op operationele systemen	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.8.20 Beveiliging van netwerkcomponenten	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.8.21 Beveiliging van netwerkdiensten	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.8.22 Netwerksegmentatie	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.8.23 Toepassen van webfilters	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.8.24 Gebruik van cryptografie	JA	Risicobeoordeling en -beheersing	Geïmplementeerd

Beheersmaatregel	Relevant	Reden	Status
A.8.25 Beveiligen tijdens de ontwikkelcyclus	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.8.26 Toepassingsbeveiligingseisen	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.8.27 Veilige systeemarchitectuur en technische uitgangspunten	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.8.28 Veilig coderen	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.8.29 Testen van de beveiliging tijdens ontwikkeling en acceptatie	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.8.30 Uitbestede systeemontwikkeling	NEE	We besteden softwareontwikkeling niet uit.	Niet geïmplementeerd
A.8.31 Scheiding van ontwikkel-, test- en productieomgevingen	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.8.32 Wijzigingsbeheer	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.8.33 Testgegevens	JA	Risicobeoordeling en -beheersing	Geïmplementeerd
A.8.34 Bescherming van informatiesystemen tijdens audits	JA	Risicobeoordeling en -beheersing	Geïmplementeerd