A.8 — Technologische Beheersmaatregelen

Gegenereerd op 21 september 2026 — © LemonB BV — trust.tenderb.nl

A.8 — Technologische Beheersmaatregelen

✅

34 beheersmaatregelen — alle geïmplementeerd en actief gemonitord als onderdeel van onze ISO/IEC 27001:2022 certificering.

🔐 Toegang & Authenticatie

- **A.8.2** — Geprivilegieerde toegangsrechten: De toewijzing en het gebruik van geprivilegieerde toegangsrechten worden beperkt en beheerd.
- **A.8.3** — Beperking van toegang tot informatie: Toegang tot informatie en andere gerelateerde bedrijfsmiddelen wordt beperkt overeenkomstig het vastgestelde onderwerpspecifieke beleid voor toegangscontrole.
- **A.8.4** — Toegang tot broncode: Lees- en schrijftoegang tot broncode, ontwikkeltools en softwarebibliotheken worden op passende wijze beheerd.
- **A.8.5** — Veilige authenticatie: Veilige authenticatietechnologieën en -procedures worden geïmplementeerd op basis van informatiebeveiligingsbeperkingen voor toegang.
- **A.8.18** — Gebruik van geprivilegieerde systeemprogramma's: Het gebruik van hulpprogramma's die systeemcontroles kunnen omzeilen wordt beperkt en streng gecontroleerd.

🛡️ Endpoint- & Netwerkbeveiliging

- **A.8.1** — Gebruikerseindpuntapparaten: Informatie opgeslagen op, verwerkt door of bereikbaar via gebruikerseindpuntapparaten wordt beschermd.
- **A.8.20** — Netwerkbeveiliging: Netwerken en netwerkapparaten worden beveiligd, beheerd en gecontroleerd om informatie in systemen en applicaties te beschermen.
- **A.8.21** — Beveiliging van netwerkdiensten: Beveiligingsmechanismen, serviceniveaus en servicevereisten van netwerkdiensten worden geïdentificeerd, geïmplementeerd en gemonitord.
- **A.8.22** — Segregatie van netwerken: Groepen van informatiediensten, gebruikers en informatiesystemen worden gesegregeerd in de netwerken van de organisatie.

🔒 Cryptografie & Data-bescherming

- **A.8.24** — Gebruik van cryptografie: Regels voor effectief gebruik van cryptografie, inclusief cryptografisch sleutelbeheer, worden gedefinieerd en geïmplementeerd.

- **A.8.11** — Maskering van gegevens: Gegevensmaskering wordt gebruikt overeenkomstig het onderwerpspecifieke beleid van de organisatie voor toegangscontrole en andere gerelateerde onderwerpspecifieke beleidsregels en zakelijke vereisten, rekening houdend met toepasselijke wetgeving.
- **A.8.12** — Preventie van gegevenslekken: Maatregelen voor preventie van gegevenslekken worden toegepast op systemen, netwerken en andere apparaten die gevoelige informatie verwerken, opslaan of verzenden.

💾 Backup & Beschikbaarheid

- **A.8.13** — Back-up van informatie: Back-upkopieën van informatie, software en systemen worden onderhouden en regelmatig getest overeenkomstig het overeengekomen onderwerpspecifieke beleid voor back-ups.
- **A.8.14** — Redundantie van informatievoorzieningsfaciliteiten: Informatievoorzieningsfaciliteiten worden geïmplementeerd met voldoende redundantie om aan de beschikbaarheidsvereisten te voldoen.

📦 Software & Applicatiebeheer

- **A.8.6** — Beheer van capaciteit: Het gebruik van middelen wordt gemonitord en aangepast overeenkomstig de huidige en verwachte capaciteitsvereisten.
- **A.8.7** — Bescherming tegen malware: Bescherming tegen malware wordt geïmplementeerd en ondersteund door passende gebruikersbewustwording.
- **A.8.8** — Beheer van technische kwetsbaarheden: Informatie over technische kwetsbaarheden van gebruikte informatiesystemen wordt verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden wordt geëvalueerd en passende maatregelen worden genomen.
- **A.8.9** — Configuratiebeheer: Configuraties, inclusief beveiligingsconfiguraties, van hardware, software, diensten en netwerken worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld.
- **A.8.10** — Verwijdering van informatie: Informatie opgeslagen in informatiesystemen, apparaten of in andere opslagmedia wordt verwijderd wanneer niet langer vereist.
- **A.8.19** — Installatie van software op operationele systemen: Procedures en maatregelen worden geïmplementeerd om de installatie van software op operationele systemen op veilige wijze te beheren.
- **A.8.25** — Veilige levenscyclus voor softwareontwikkeling: Regels voor de veilige ontwikkeling van software en systemen worden vastgesteld en toegepast.
- **A.8.26** — Applicatiebeveiligingsvereisten: Informatiebeveiligingsvereisten worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van applicaties.

- **A.8.27** — Veilige systeemarchitectuur en engineeringprincipes: Principes voor het ontwerpen van veilige systemen worden vastgesteld, gedocumenteerd, onderhouden en toegepast op alle activiteiten voor de ontwikkeling van informatiesystemen.
- **A.8.28** — Veilig coderen: Veilige coderingsprincipes worden toegepast bij softwareontwikkeling.
- **A.8.29** — Beveiligingstesten in ontwikkeling en acceptatie: Beveiligingstestprocessen worden gedefinieerd en geïmplementeerd in de ontwikkelingslevenscyclus.
- **A.8.30** — Uitbestede ontwikkeling: De organisatie stuurt, monitort en beoordeelt de activiteiten met betrekking tot uitbestede systeemontwikkeling.
- **A.8.31** — Scheiding van ontwikkel-, test- en productieomgevingen: Ontwikkel-, test- en productieomgevingen worden gescheiden en beveiligd.

🔍 Monitoring & Logging

- **A.8.15** — Logging: Logboeken die activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen registreren worden geproduceerd, opgeslagen, beschermd en geanalyseerd.
- **A.8.16** — Monitoringactiviteiten: Netwerken, systemen en applicaties worden gemonitord op afwijkend gedrag en passende maatregelen worden genomen om potentiële informatiebeveiligingsincidenten te evalueren.
- **A.8.17** — Kloksynchronisatie: De klokken van informatieverwerkingssystemen die door de organisatie worden gebruikt worden gesynchroniseerd met goedgekeurde tijdbronnen.

🌐 Web & Clouddiensten

- **A.8.23** — Webfiltering: Toegang tot externe websites wordt beheerd om blootstelling aan kwaadaardige inhoud te verminderen.
- **A.8.32** — Wijzigingsbeheer: Wijzigingen in informatieverwerking, informatiesystemen en netwerken worden onderworpen aan wijzigingsbeheerprocedures.
- **A.8.33** — Testinformatie: Testinformatie wordt op passende wijze geselecteerd, beschermd en beheerd.
- **A.8.34** — Bescherming van informatiesystemen tijdens audittesten: Audittesten en andere assuranceactiviteiten met beoordeling van operationele systemen worden gepland en overeengekomen tussen de tester en het bevoegd management.