					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P34					Documenttitel: **Beleid inzake mobiele apparaten en Bring Your Own Device (BYOD)**							
Versie: 1.0		Ingangsdatum: 01.01.2025			Documenteigenaar:							
X	Beleid		Standaard		Procedure		Formulier		Register		Overig	

Revisiegeschiedenis				
Revisienummer	**Revisiedatum**	**Wijzigingen**	**Beoordeeld door**	**Proceseigenaar**

Goedkeuringen			
Naam	**Functie**	**Datum**	**Handtekening**

Juridische kennisgeving (auteursrecht en gebruiksbeperkingen)

(C) 2025 Clarysec LLC. All rights reserved.

Dit document is intellectueel eigendom van Clarysec LLC. Geen enkel deel van dit document mag zonder voorafgaande uitdrukkelijke schriftelijke toestemming worden gekopieerd, hergebruikt, verspreid of gewijzigd voor commerciële of implementatiedoeleinden.
Ongeautoriseerd gebruik is strikt verboden en kan leiden tot juridische stappen.
Neem voor licentiëring contact op via: info@clarysec.com

Afstemming op normen en regelgeving

Norm/regelgeving	Clausule/artikel	Opmerking
ISO/IEC 27001:2022	5.2, 6.1, 7.5, 8	Past beveiligingsmaatregelen en nalevingsverplichtingen toe
ISO/IEC 27002:2022	5.10, 8.1, 8.5, 8	Biedt gedetailleerde beheersmaatregelen voor het beheer van mobiele apparaten
NIST SP 800-53 Rev.5	AC-19, AC-17, CM-7, MP-5, SC-12	Toegangscontrole, externe toegang, configuratie- en beveiligingsvereisten voor mobiel gebruik
AVG	5(1)(f), 25, 32	Verplichte privacybescherming, gegevensversleuteling en beveiliging van verwerking
NIS2-richtlijn	21(2)(d)	Technische en organisatorische beveiligingsmaatregelen voor mobiele toegang
DORA	9, 10	Vereisten voor ICT-risicobeheer en beveiliging voor mobiel gebruik
COBIT 2019	APO13.02, DSS01.04, BAI09	Planning van informatiebeveiliging, configuratie van bedrijfsmiddelen en beheersmaatregelen voor mobiele omgevingen

1. Doel

1.1 Dit beleid stelt de beveiligings-, nalevings- en operationele vereisten vast voor het gebruik van mobiele apparaten en persoonlijke technologie (BYOD – Bring Your Own Device) bij toegang tot informatiesystemen, applicaties of gegevens van de organisatie.

1.2 Het beleid heeft tot doel de vertrouwelijkheid, integriteit en beschikbaarheid van bedrijfsinformatie te waarborgen die via mobiele eindpunten wordt geraadpleegd of verwerkt, waaronder smartphones, tablets, laptops en hybride apparaten.

1.3 Dit beleid schrijft tevens de technische en procedurele beheersmaatregelen voor die nodig zijn om risico's zoals datalekken, ongeautoriseerde toegang, verlies of diefstal van apparaten en compromittering van mobiele applicaties te beperken.

1.4 Dit beleid ondersteunt de naleving van wet- en regelgeving en contractuele verplichtingen en maakt tegelijkertijd veilige mobiele productiviteit mogelijk voor werknemers, contractanten en geautoriseerde derden.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle medewerkers, waaronder werknemers, contractanten, stagiairs en externe dienstverleners, die mobiele apparaten gebruiken voor toegang tot bedrijfsgegevens, systemen, applicaties of communicatieplatforms.

2.2 Het beleid omvat alle mobiele computerapparaten, waaronder, maar niet beperkt tot:

2.2.1 Smartphones en tablets (iOS, Android enz.)

2.2.2 Laptops en ultrabooks (Windows, macOS, Linux)

2.2.3 Wearables en hybride slimme apparaten die gegevens kunnen synchroniseren

2.3 Het beleid is van toepassing ongeacht of het apparaat eigendom is van de organisatie of persoonlijk eigendom is op basis van een BYOD-overeenkomst.

2.4 Het beleid omvat alle toegangsvormen, waaronder VPN's, virtuele desktops, cloudapplicaties, e-mail, samenwerkingsplatforms (bijv. SharePoint, Teams) en tools voor bestandssynchronisatie (bijv. OneDrive, Dropbox indien geautoriseerd).

2.5 Het beleid geldt voor gebruik in het kader van thuiswerken, op locatie, tijdens reizen of binnen hybride werkregelingen.

3. Doelstellingen

3.1 Het verminderen van het risico op compromittering, blootstelling of verlies van gegevens als gevolg van onveilig gebruik van mobiele apparaten.

3.2 Het afdwingen van consistente en handhaafbare beveiligingsmaatregelen op alle mobiele eindpunten, ongeacht het eigendomsmodel (bedrijfsapparaat of BYOD).

3.3 Het waarborgen dat het gebruik van mobiele apparaten voldoet aan ISO/IEC 27001 en andere toepasselijke wettelijke en regelgevende kaders op het gebied van privacy, gegevensbescherming en cyberbeveiliging.

3.4 Het mogelijk maken van een veilige integratie van mobiele apparaten in de operationele werkstromen en communicatie- en samenwerkingsprocessen van de organisatie.

3.5 Het vastleggen van duidelijke verantwoordelijkheden en processen voor Mobile Device Management (MDM), waaronder registratie, wissen op afstand, encryptie, authenticatie en monitoring.

3.6 Het beschermen van de privacyrechten van personen die hun eigen apparaten gebruiken, terwijl tegelijkertijd de gevoelige informatie van de organisatie wordt beschermd.

4. Rollen en verantwoordelijkheden

4.1 Chief Information Security Officer (CISO) / IT-beveiligingsverantwoordelijke

4.1.1 Stelt beleid en technische standaarden vast voor mobiel gebruik en BYOD.

4.1.2 Houdt toezicht op naleving, incidentrespons en uitzonderingsbeheer met betrekking tot beheersmaatregelen voor mobiele apparaten.

4.1.3 Stemt af met Juridische Zaken, Compliance en HR om te waarborgen dat de handhaving juridisch houdbaar is en aansluit bij de organisatie.

4.2 IT-beheerder / MDM-beheerder

4.2.1 Beheert toegangsverlening, registratie en configuratie van mobiele apparaten via MDM-oplossingen.

4.2.2 Dwingt beheersmaatregelen op apparaatniveau af (bijv. encryptie, pincodevereisten en applicatiebeheersmaatregelen).

4.2.3 Voert wissen op afstand, apparaatvergrendeling en intrekking van toegangsrechten uit indien vereist.

[... Secties 4.3–8 zijn niet opgenomen in dit voorbeeld. Koop het volledige document voor toegang tot de volledige inhoud. ...]

9. Eisen voor beoordeling en actualisatie

9.1 Dit beleid moet ten minste jaarlijks worden beoordeeld door de CISO of een aangewezen informatiebeveiligingsmanager om afstemming te waarborgen met:

9.1.1 Wijzigingen in mobiele besturingssystemen, MDM-technologieën of authenticatiestandaarden

9.1.2 Wijzigingen in wet- en regelgeving of contractuele verplichtingen die van invloed zijn op de bescherming van mobiele gegevens (bijv. AVG, DORA, NIS2)

9.1.3 Wijzigingen in de beheersmaatregelensets van ISO/IEC 27001:2022, ISO/IEC 27002:2022 of NIST SP 800-53 Rev.5

9.1.4 Feedback uit audits, evaluaties na incidenten of meldingen van medewerkers

9.2 Tussentijdse beoordelingen kunnen worden geactiveerd door:

9.2.1 Beveiligingsincidenten met betrekking tot mobiele apparaten of BYOD-platforms

9.2.2 Meldingen van leveranciers over kwetsbaarheden met een hoog risico in ondersteunde platforms

9.2.3 Introductie van nieuwe mobiele apps of samenwerkingsplatforms die worden gebruikt voor bedrijfsactiviteiten

9.3 Beleidsactualisaties moeten:

9.3.1 Worden gedocumenteerd in de versiehistorie van het beleid

9.3.2 Worden gecommuniceerd aan alle medewerkers en betrokken contractanten

9.3.3 Opnieuw worden bevestigd met een bijgewerkte kennisneming door alle BYOD-gebruikers

9.4 Alle beoordelingen en herzieningen moeten formeel worden goedgekeurd door het topmanagement en worden vastgelegd in het register voor beleidswijzigingen.

10. Gerelateerde beleidslijnen en samenhang

10.1 Dit beleid hangt samen met meerdere kernbeleidslijnen binnen het ISMS-raamwerk van de organisatie. Belangrijke verbanden zijn onder meer:

10.1.1 P1 – Informatiebeveiligingsbeleid: stelt de overkoepelende governanceregels vast voor alle beheersmaatregelen voor informatiebeveiliging, waaronder die voor het gebruik van mobiele apparaten.

10.1.2 P3 – Beleid inzake aanvaardbaar gebruik: definieert toegestane gedragingen en beperkingen met betrekking tot technologiegebruik, die rechtstreeks van toepassing zijn op mobiele toegang en BYOD.

10.1.3 P9 – Beleid inzake werken op afstand: beschrijft aanvullende beveiligingsverplichtingen voor mobiele werkomgevingen en vult de in dit beleid vastgestelde mobiele beheersmaatregelen aan.

10.1.4 P13 – Beleid inzake gegevensclassificatie en etikettering: bepaalt hoe gegevens op mobiele apparaten moeten worden behandeld op basis van classificatieniveau, met gevolgen voor opslag, overdracht en afgedwongen encryptie.

10.1.5 P22 – Logging- en monitoringbeleid: ondersteunt het verzamelen en beoordelen van toegangslogboeken voor mobiele toegang om afwijkingen of overtredingen te detecteren.

10.1.6 P30 – Incidentresponsbeleid: regelt hoe mobiele incidenten (bijv. verlies van een apparaat, ongeautoriseerde toegang) worden afgehandeld en geëscaleerd.

10.1.7 P33 – Beleid inzake audit- en nalevingsmonitoring: biedt de basis voor periodieke controles op naleving van mobiele beveiligingsvereisten, waaronder naleving van het BYOD-beleid.

11. Referentienormen en -raamwerken

11.1 Dit beleid is afgestemd op internationaal erkende cyberbeveiligingsraamwerken en wettelijke verplichtingen om veilig gebruik van mobiele apparaten en persoonlijke BYOD-technologieën in bedrijfsomgevingen te waarborgen.

11.2 ISO/IEC 27001:

11.2.1 Clausule 5.10 – Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen: vereist beheersmaatregelen voor verantwoord gebruik van bedrijfsmiddelen, waaronder mobiele apparaten.

11.2.2 Clausule 5.11 – Retourneren van bedrijfsmiddelen: regelt veilige praktijken bij het beheer van bedrijfsmiddelen buiten de bedrijfsruimten.

11.2.3 Clausule 5.12 – Classificatie van informatie: verplicht risicogebaseerde beheersmaatregelen voor de bescherming van informatie op mobiele eindpunten en in BYOD-configuraties.

11.2.4 Clausule 5.13 – Etikettering van informatie: ondersteunt passende behandeling en bescherming van informatie die via mobiele kanalen wordt verwerkt of overgedragen.

11.3 ISO/IEC 27002:2022 – Beheersmaatregelen 5.10 tot en met 5.13:

11.3.1 Beheersmaatregelen uit bijlage A 5.10 tot en met 5.13 specificeren hoe mobiele toegang, encryptie, monitoring en verliesbeperking binnen een ISMS moeten worden afgedwongen. Deze beheersmaatregelen bieden gedetailleerde implementatierichtlijnen voor het beveiligen van mobiele eindpunten, het afdwingen van containerisatie, het bewaken van apparaatintegriteit en het waarborgen van privacybewuste configuraties voor BYOD-gebruik.

11.4 NIST SP 800-53 Rev.5:

11.4.1 AC-19 – Toegangscontrole voor mobiele apparaten: definieert basisbeveiliging, waaronder encryptie, authenticatie en MDM-afdwinging.

11.4.2 AC-17 – Externe toegang: vereist veilige authenticatie en sessiebeveiliging voor externe mobiele gebruikers.

11.4.3 CM-7 – Beginsel van minimale functionaliteit: ondersteunt het verwijderen van onnodige apps en functies van mobiele eindpunten om risico's te beperken.

11.4.4 MP-5 – Bescherming van mediatransport: regelt de veilige overdracht van gegevens van mobiele systemen naar externe of cloudbestemmingen.

11.4.5 SC-12 – Totstandbrenging en beheer van cryptografische sleutels: verplicht het gebruik van veilige cryptografische protocollen voor mobiele communicatie en opslag.

11.5 AVG (Verordening (EU) 2016/679):

11.5.1 Artikel 5(1)(f) – Integriteit en vertrouwelijkheid: vereist dat organisaties persoonsgegevens op mobiele apparaten beschermen tegen ongeautoriseerde of onrechtmatige toegang.

11.5.2 Artikel 25 – Gegevensbescherming door ontwerp en door standaardinstellingen: vereist dat privacy wordt ingebouwd in BYOD- en MDM-processen.

11.5.3 Artikel 32 – Beveiliging van de verwerking: schrijft risicogebaseerde beheersmaatregelen voor (bijv. encryptie, authenticatie, toegangscontrole) voor persoonsgegevens op mobiele platforms.

11.6 NIS2-richtlijn (EU 2022/2555):

11.6.1 Artikel 21(2)(d): verplicht dat mobiele toegang tot kritieke systemen en informatie wordt beschermd met passende technische en organisatorische maatregelen, zoals endpointcontrole, encryptie en monitoring.

11.7 DORA (Verordening (EU) 2022/2554):

11.7.1 Artikel 9 – Kader voor ICT-risicobeheer: vereist dat entiteiten in de financiële sector risico's van mobiele en externe toegang beperken als onderdeel van operationele weerbaarheid.

11.7.2 Artikel 10 – Beveiligingsvereisten voor ICT-systemen: vereist een veilige mobiele architectuur, monitoring en responsmechanismen voor cyberdreigingen die vanaf mobiele apparaten ontstaan.

11.8 COBIT 2019:

11.8.1 APO13.02 – Een informatiebeveiligingsplan opstellen en onderhouden: vereist dat het gebruik van mobiele apparaten, waaronder BYOD, wordt geïntegreerd in de beveiligingsstrategieën van de organisatie.

11.8.2 DSS01.04 – Configuratie en integriteit van bedrijfsmiddelen beheren: is van toepassing op configuratiebeheer en veilige implementatie van mobiele apparaten.

11.8.3 BAI09.01 – Beheersmaatregelen opstellen en onderhouden: ondersteunt de implementatie van technische en procedurele waarborgen voor veilige mobiele en externe activiteiten.