					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P34S					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	Clausules 5.1, 5.2, 6.1, 6.2, 8	Algemene vereisten voor het ISMS en beheersmaatregelen voor mobiele apparaten/BYOD
ISO/IEC 27002:2022	Beheersmaatregelen 5.10–5.13	Gedetailleerde beheersmaatregelen voor mobiele apparaten/BYOD en externe toegang
NIST SP 800-53 Rev.5	AC-19, AC-20, CM-6, MP-7	Federale beheersmaatregelen voor apparaten, media en configuratie
AVG	Artikelen 5(1)(f)	Bescherming van persoonsgegevens op mobiele eindpunten
EU NIS2	Artikel 21(2)(d)	Bescherming van bedrijfskritische apparaten (inclusief BYOD)
EU DORA	Artikelen 9, 10	Eisen voor ICT-risicobeheer en continuïteit voor mobiele eindpunten
COBIT 2019	APO13, DSS01, DSS05	IT-governance, operationele beheersing en beveiligingsmaatregelen voor diensten

1. Doel

1.1. Dit beleid definieert de verplichte beveiligingsvereisten voor het gebruik van mobiele apparaten, waaronder smartphones, tablets en laptops, bij toegang tot bedrijfsinformatie, systemen of diensten.

1.2. Dit beleid regelt tevens het gebruik van Bring Your Own Device (BYOD) om te waarborgen dat klant- en bedrijfsgegevens worden beschermd, ongeacht wie eigenaar is van het apparaat.

1.3. Dit beleid schrijft een consistente bescherming van mobiele toegang voor, ondersteunt de doelstellingen voor ISO/IEC 27001-certificering en voorkomt gegevensverlies of compromittering als gevolg van verloren, gestolen of onjuist gebruikte mobiele eindpunten.

1.4. Het waarborgt dat zowel technische als procedurele beveiligingsmaatregelen worden toegepast op mobiel gebruik binnen het mkb zonder eigen IT-teams, inclusief omgevingen voor werken op afstand en in de cloud gehoste diensten.

2. Reikwijdte

2.1. Dit beleid is van toepassing op alle werknemers, contractanten, stagiairs en dienstverleners die:

2.1.1. een mobiel apparaat gebruiken om bedrijfsgegevens of -systemen te raadplegen, te verwerken of op te slaan

2.1.2. verbinding maken met bedrijfsdiensten, waaronder e-mail, gedeelde mappen, cloudapplicaties of interne systemen via VPN

2.2. Dit beleid omvat:

2.2.1. alle mobiele apparaten: smartphones, tablets en laptops (door de organisatie verstrekt of persoonlijk eigendom in het kader van BYOD)

2.2.2. alle besturingssystemen (bijvoorbeeld iOS, Android, Windows en macOS)

2.2.3. alle locaties (kantoor, thuis, op afstand en openbare ruimten)

2.3. Dit beleid geldt voor alle werkomgevingen en moet worden gehandhaafd ongeacht het eigendom van het apparaat.

3. Doelstellingen

3.1. Voorkomen van gegevensverlies: waarborgen dat mobiel gebruik gevoelige bedrijfs- of klantgegevens niet blootstelt aan ongeautoriseerde toegang, diefstal of misbruik.

3.2. Duidelijke regels voor BYOD vaststellen: afdwingbare voorwaarden bieden voor het gebruik van persoonlijke apparaten voor zakelijke doeleinden, met passende juridische en technische beheersmaatregelen.

3.3. Ondersteunen van naleving van regelgeving: voldoen aan vereisten uit hoofde van ISO/IEC 27001, de AVG, NIS2 en andere wettelijke verplichtingen door middel van afdwingbare praktijken voor mobiele beveiliging.

3.4. Operationeel risico minimaliseren: de kans op operationele verstoring als gevolg van misbruik, compromittering of uitval van mobiele apparaten verkleinen.

3.5. Vertrouwen van klanten behouden: aan klanten en partners aantonen dat hun gegevens beschermd blijven, ook wanneer deze via mobiele of persoonlijke apparaten worden geraadpleegd.

4. Rollen en verantwoordelijkheden

4.1. Algemeen directeur (GM):

4.1.1. draagt de eindverantwoordelijkheid voor dit beleid.

4.1.2. keurt ieder gebruik van mobiele toegang en BYOD-toegang tot bedrijfssystemen goed.

4.1.3. ziet erop toe dat BYOD-overeenkomsten worden ondertekend, opgeslagen en nageleefd.

4.1.4. verifieert dat externe IT-dienstverleners de vereiste beveiligingsmaatregelen voor mobiele apparaten afdwingen.

4.2. Aangewezen medewerker of IT-ondersteuning:

4.2.1. ondersteunt bij de inrichting, registratie en configuratie van mobiele apparaten die voor werk worden gebruikt.

4.2.2. handhaaft toegangsbeheersmaatregelen, applicatiebeperkingen en beleidsregels voor monitoring met betrekking tot mobiele apparaten.

4.2.3. ondersteunt de respons op incidenten met mobiele apparaten (verloren, gestolen of gecompromitteerde apparaten).

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

9. Eisen voor herziening en actualisatie

9.1. Jaarlijkse herziening

9.1.1. De Algemeen directeur (GM) moet dit beleid ten minste eenmaal per 12 maanden herzien.

9.1.2. De herziening moet bevestigen dat het beleid blijvend is afgestemd op de vereisten van ISO/IEC 27001, op ontwikkelingen in mobiele technologieën en op wijzigingen in de bedrijfsvoering.

9.1.3. Actualisaties moeten ook rekening houden met recente incidenten, auditresultaten of ontwikkelingen in wet- en regelgeving (bijvoorbeeld de AVG, NIS2 en DORA).

9.2. Triggergebeurtenissen voor tussentijdse herziening

9.2.1. Dit beleid moet onmiddellijk worden bijgewerkt indien een van de volgende situaties zich voordoet:

9.2.1.1. een ernstig mobiel beveiligingsincident (bijvoorbeeld een inbreuk via een verloren of gehackt apparaat)

9.2.1.2. een wijziging in ondersteunde platforms of tools voor mobiel apparaatbeheer

9.2.1.3. een wettelijke of regelgevende wijziging die van invloed is op het gebruik van persoonlijke apparaten of gegevensbescherming

9.2.1.4. de introductie van nieuwe apps, diensten of tools van derde partijen die op mobiele apparaten worden gebruikt

9.3. Documentatie van wijzigingen

9.3.1. Alle herzieningen en actualisaties moeten worden gedocumenteerd, inclusief de beoordelingsdatum, de aangebrachte wijzigingen en de goedkeuring door de GM

9.3.2. Een versiehistorie moet worden bewaard voor auditdoeleinden

9.4. Communicatie en toegang

9.4.1. De GM moet ervoor zorgen dat alle gebruikers (werknemers, contractanten en derde partijen) over wijzigingen worden geïnformeerd

9.4.2. Geactualiseerde versies moeten eenvoudig toegankelijk worden gemaakt, bijvoorbeeld via gedeelde mappen of interne platforms

10. Gerelateerd beleid en samenhang

10.1. Dit beleid maakt deel uit van het totale pakket mkb-beleid voor informatiebeveiliging en moet in samenhang met het volgende worden geïmplementeerd:

10.1.1. P4S – Beleid inzake toegangsbeheersing: definieert vereisten voor het beheren van veilige toegang tot systemen, inclusief systemen die via mobiele apparaten worden benaderd. Dwingt wachtwoordhygiëne en sessiebeheer af.

10.1.2. P8S – Beleid inzake bewustwording en opleiding op het gebied van informatiebeveiliging: waarborgt dat gebruikers zijn opgeleid in veilig gebruik van mobiele apparaten, incidentmelding en BYOD-voorwaarden.

10.1.3. P17S – Beleid inzake gegevensbescherming en privacy: brengt de verwerking van persoonsgegevens en bedrijfsgegevens op mobiele platforms in overeenstemming met de AVG, in het bijzonder wanneer persoonlijke apparaten voor werk worden gebruikt.

10.1.4. P9S – Beleid inzake werken op afstand: sluit aan op de verwachtingen rond mobiel gebruik bij werken buiten de bedrijfslocatie of vanuit huis, inclusief apparaatgebruik en beveiligingsmaatregelen voor netwerktoegang.

10.1.5. P30S – Incidentresponsbeleid (P30): biedt het responskader voor mobiele incidenten, inclusief gecompromitteerde of verloren apparaten.

10.2. Deze gerelateerde beleidsdocumenten vormen gezamenlijk een complete set beheersmaatregelen voor de beveiliging van mobiele apparaten binnen mkb-organisaties zonder eigen IT-personeel en waarborgen afdwingbaarheid, transparantie en gereedheid voor certificering.

11. Referentienormen en -raamwerken

11.1. Dit beleid ondersteunt volledige afstemming op de volgende beveiligings- en nalevingsnormen:

11.2. ISO/IEC 27001:

11.2.1. Clausule 5.1 – Leiderschap en betrokkenheid: waarborgt managementtoezicht en verantwoordingsplicht voor mobiele toegang en BYOD-toegang

11.2.2. Clausule 6.1 – Maatregelen om risico's aan te pakken: vereist dat risico's op het gebied van mobiele beveiliging worden beoordeeld en behandeld

11.2.3. Clausule 8.1 – Operationele planning en beheersing: vereist consistente procedures voor mobiele toegang om bedrijfsgegevens te beschermen

11.3. ISO/IEC 27002:

11.3.1. Beheersmaatregelen 5.10 (gebruik van mobiele apparaten), 5.11 (thuiswerken), 5.12 (externe toegang) en 5.13 (BYOD): bieden implementatierichtlijnen voor het beheersen van apparaatrisico's in de context van een kleine onderneming

11.4. NIST SP 800-53 Rev.5:

11.4.1. AC-19 – Toegangscontrole voor mobiele apparaten: vereist beveiligingsinstellingen voor geautoriseerd mobiel gebruik

11.4.2. AC-20 – Gebruik van externe systemen: regelt risico's van BYOD en externe toegang

11.4.3. CM-6 – Configuratie-instellingen: dwingt veilige standaard- en aangepaste instellingen op mobiele platforms af

11.4.4. MP-7 – Gebruik van media: behandelt passend gebruik en beperkingen voor mobiele opslag en toegang tot gegevens

11.5. AVG (2016/679):

11.5.1. Artikel 5(1)(f) – Integriteit en vertrouwelijkheid: vereist gegevensbescherming door passende beveiliging van persoonsgegevens, in het bijzonder op mobiele platforms

11.5.2. Artikel 32 – Beveiliging van de verwerking: verplicht het gebruik van passende technische en organisatorische maatregelen voor de beveiliging van gegevens die via mobiele apparaten worden geraadpleegd of opgeslagen

11.6. EU NIS2-richtlijn (2022/2555):

11.6.1. Artikel 21(2)(d) – Beveiligingsmaatregelen voor apparaten: vereist beveiligingsmaatregelen voor hardware en software die worden gebruikt voor toegang tot kritieke bedrijfssystemen, inclusief persoonlijke apparaten

11.7. EU DORA (2022/2554):

11.7.1. Artikel 9 – ICT-risicobeheerkader: vereist bescherming van mobiele eindpunten die worden gebruikt voor kritieke bedrijfscommunicatie en cloudservices

11.7.2. Artikel 10 – ICT-bedrijfscontinuïteit: vereist blijvend veilige toegang tot bedrijfssystemen, ook tijdens verstoringen of werken op afstand

11.8. COBIT 2019:

11.8.1. APO13 – Beheer van beveiliging: vereist dat de organisatie beleid voor mobiele apparaten en BYOD afdwingt dat is afgestemd op het ondernemingsrisico

11.8.2. DSS01 – Beheer van operationele activiteiten: waarborgt de technische implementatie van mechanismen voor veilige toegang

11.8.3. DSS05 – Beheer van beveiligingsdiensten: regelt de betrokkenheid van derde partijen bij het in stand houden van beveiligde mobiele omgevingen en de coördinatie van incidentrespons