[logo organisatie]

[naam organisatie]

Comment [DK1]: Alle velden in dit document gemarkeerd met spekhaken [ ] moeten worden ingevuld.

BELEID VOOR BRING YOUR OWN DEVICE (BYOD)

Code:	
Versie:	
Versiedatum:	
Gemaakt door:	
Goedgekeurd door:	
Classificatie:	

Comment [DK2]: De documentcodering moet in overeenstemming zijn met het bestaande organisatiecoderingssysteem; indien een dergelijk systeem niet is geïmplementeerd, dan kan deze regel worden verwijderd.

Versieblad

Datum	Versie	Gemaakt door	Omschrijving van de aanpassing
DD/MM/JJJJ	0.1	Dejan Kosutic	Concept basisdocument

Inhoudsopgave

1. Doel, toepassingsgebied en gebruikers

Het doel van dit document is om te bepalen hoe de organisatie de controle kan behouden over haar informatie, terwijl dergelijke informatie wordt benaderd door apparaten die geen eigendom zijn van de organisatie.

Dit document wordt toegepast op alle apparaten in persoonlijk bezit, die de mogelijkheid hebben om gevoelige informatie op te slaan, overgedragen of verwerken binnen het Management Systeem voor Informatiebeveiliging (ISMS) toepassingsgebied. Dergelijke apparaten bevatten laptops, smartphones, tablets, USB-sticks, digitale camera`s, enz. Dergelijke apparaten worden in dit beleid aangeduid als BYOD.

Gebruikers van dit document zijn alle werknemers van [naam organisatie].

2. Gerefereerde documenten

- ISO/IEC 27001 norm, clausule A.6.2.1, A.6.2.2, A.13.2.1

3. Beveiligingsregels voor het gebruik van BYOD

De regels in dit beleid zijn van toepassing zijn op alle BYOD, of ze nu worden gebruikt voor werk of [illegible]

3.1. Bedrijfsbeleid

[Organisatie naam] ondersteunt het wijd verspreide gebruik van de BYOD voor zakelijk gebruik, - [illegible]

Comment [DK3]: Als alternatief, kunt u ook iets [illegible] andere wijze uit te voeren.

De bedrijfsgegevens die opgeslagen, overgedragen of verwerkt zijn op BYOD blijven eigendom van de [illegible] apparaten.

[Functie] zal een Lijst van BYOD maken met verboden toepassingen.

3.2. Wie is bevoegd voor het gebruik van BYOD, en voor wat

[Functie] zal een lijst van de functiebenamingen en/of welk persoon maken die BYOD mogen [illegible] eigen apparaten.

[Functie] creëert een lijst van BYOD met verboden toepassingen.

3.3. Welke apparaten zijn toegestaan

[illegible] mogen worden als BYOD, tezamen met verplichte instellingen voor elk apparaat.

Comment [DK4]: Bijv. firewall, back-up, schermbeveiliging, etc.

3.4. Aanvaardbaar gebruik

Voor elke BYOD, is het volgende verplicht:

- [beschrijf hoe de back-up voor bedrijfsinformatie moet worden gedaan]
- [beschrijf welke beveiligingssoftware dient te worden geïnstalleerd - b.v. antivirussoftware inbraakpreventie, software voor beheer van mobiel apparaten]
- [beschrijf de methode van authenticatie die wordt gebruikt.
- [beschrijf de beveiligingsmethode van connectie op het bedrijfsnetwerk]
- bij gebruik van BYOD buiten het bedrijfsterrein, mag het niet onbeheerd gelaten worden, en indien mogelijk, dient het fysiek te worden opgeborgen.
- bij het gebruik van BYOD op openbare plaatsen, moet de eigenaar ervoor zorgen dat niet kan worden gelezen door onbevoegde personen
- patches en updates moeten regelmatig worden geïnstalleerd
- geclassificeerde informatie moet extra worden beschermd volgens de [Beleid voor Geclassificeerde Informatie]
- breng [Functie] op de hoogte voordat de BYOD wordt weggegooid, of verkocht, of overgedragen aan een derde party voor onderhoud

Het volgende is niet toegestaan met BYOD:

- iemand anders toegang verlenen, behalve de werknemer die eigenaar is van het apparaat
- installeren van toepassingen die worden vermeld in de Lijst van BYOD verboden applicaties
- plaatsen van illegaal materiaal op het apparaat
- installeren van software zonder licentie
- verbinding maken via Bluetooth met welk apparaat dan ook
- verbinding maken met onbekende Wi-Fi netwerken
- lokaal opslaan van wachtwoorden, behalve bij het gebruik van de volgende toepassingen: [lijst met toegestane toepassingen waar wachtwoorden kunnen worden opgeslagen]
- lokaal opslaan van de volgende informatie: [lijst gevoelige informatie]
- bedrijfsgegevens verzenden naar andere apparaten welke niet zijn toegestaan

3.5. Speciale rechten

[Organisatie naam] heeft het recht om alle bedrijfsgegevens te bekijken, aan te passen, en te verwijderen dat is opgeslagen, verzonden, verwerkt op de BYOD.

[Functie] is bevoegd tot het configureren van elke BYOD op basis van dit Beleid en bewaakt zijn gebruik via [specificeer de naam van de beheersoftware van het mobiele apparatuur].

[Organisatienaam] heeft het recht voor volledige verwijdering van alle data op BYOD uit te voeren indien zij dat noodzakelijk achten voor de bescherming van bedrijfsgegevens, zonder toestemming van de eigenaar van het apparaat.

3.6. Restitutie

Comment [DK5]: Bijv. wachtwoorden, toegangscodes, biometrische kaarten, etc.

Comment [DK6]: Bijv. VPN

Comment [DK7]: Indien technisch haalbaar, kunt u het slaggat "verwijdering van alle bedrijfsgegevens op BYOD"

[Organisatie naam] zal de werknemers (de eigenaren van BYOD) geen vergoeding betalen voor het [illegible]

Comment [DK8]: Als alternatief kunt u een [illegible] werknemers.

[Organisatie naam] zal betalen voor het volgende:

- alle nieuwe software die moet worden geïnstalleerd voor bedrijfsgebruik
- [illegible] maandelijkse rekeningen van de eigenaren.

3.7. Beveiligingsinbreuken

Alle veiligheidsinbreuken met betrekking tot BYOD moeten direct worden gemeld aan [functie].

Comment [DK9]: Dit is meestal de informatiebeveiliger, of de Helpdesk.

[illegible] binnen 1 werkdag worden gemeld.

3.8. Opleiding en bewustzijn

[Functie] is belast met de opleiding van nieuwe en bestaande medewerkers op het juiste gebruik van [illegible]

4. Registratiebeheer op basis van dit document

Naam registratie	*Opslaglocatie*	*Persoon verantwoordelijk voor opslag*	*Beveiligingsmaatregelen voor registraties*	*Bewaartermijn*
[Lijst van toegestane gebruikers van BYOD en waar zij toegang toe hebben]	[bedrijf intranet]	[functie]	Alleen [functie] kan een nieuwe versie van de Lijst bewerken of publiceren	Lijst die niet meer geldig is moet voor 3 jaar bewaard worden
[Lijst van acceptabele BYOD apparaten en hun Instellingen]	[bedrijf intranet]	[functie]	Alleen [functie] kan een nieuwe versie van de Lijst bewerken of publiceren	Lijst die niet meer geldig is moet voor 3 jaar gearchiveerd worden
[Lijst van verboden BYOD toepassingen]	[bedrijf intranet]	[functie]	Alleen [functie] kan een nieuwe versie van de Lijst bewerken of publiceren	Lijst die niet meer geldig is moet voor 3 jaar gearchiveerd worden

Comment [DK10]: Wijzig indien nodig.

Comment [DK11]: Wijzig indien nodig.

Comment [DK12]: Wijzig indien nodig.

5. Geldigheid en documentbeheer

Dit document is geldig vanaf [datum].

De eigenaar van dit document is [functie] dient het document te controleren en indien nodig het [illegible] aanvaardbare apparaten, en de lijst van verboden toepassingen elke 3 maanden beoordelen.

Comment [DK13]: Dit is slechts een aanbeveling, pas de frequentie zo nodig aan.

Wanneer de doeltreffendheid en toereikendheid van dit document wordt beoordeeld, dan dienen de volgende criteria in ogenschouw te worden genomen:

- [illegible]
- aantal werknemers welke gebruikt maakt van BYOD zonder toestemming

[functie]
[voor- en achternaam]

_____
[handtekening]

Comment [DK14]: Alleen noodzakelijk als de procedure voor het documenteren en registreren van documenten voorschrijft dat papieren documenten moeten worden ondertekend.