[logo organisatie]

[naam organisatie]

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

BELEID VOOR DRAAGBARE APPARATEN EN TELEWERKEN

Comment [D2]: Dit Beleid behoeft niet in een apart document te worden vervat indien dezelfde regels worden voorgeschreven in het Toegangsbeleid.

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

Comment [DK3]: 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 ongeautoriseerde toegang tot draagbare apparaten binnen en buiten de panden van de organisatie.

Dit document is van toepassing op het hele toepassingsgebied van het Managementsysteem voor Informatiebeveiliging (ISMS, d.w.z. voor alle personen, gegevens en apparatuur in het ISMS-toepassingsgebied.

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

2. Gerefereerde documenten

- ISO/IEC 27001 norm, clausules A.6.2 en A.11.2.6
- Informatiebeveiliginsbeleid
- Beleid voor Geclassificeerde Informatie
- [Beleid voor Aanvaardbaar Gebruik]

3. Werken met draagbare computers

3.1. Introductie

Draagbare mobiele apparatuur zijn allerlei draagbare computers, mobieltjes, geheugenkaarten en andere draagbare apparatuur gebruikt voor opslag en verwerking en overdragen van gegevens.

De hierboven genoemde apparatuur mag alleen van het terrein worden meegenomen na het verkrijgen van autorisatie in overeenstemming met het Beleid voor Aanvaardbaar Gebruik.

Comment [D4]: Verwijder dit hele item indien beheersmaatregel A.11.2.5 als niet van toepassing is aangegeven in de Verklaring van Toepasselijkheid.

3.2. Basisregels

Speciale zorg moet in acht worden genomen wanneer draagbare computerapparatuur in auto's worden gelegd of in andere vormen van transport, openbare ruimten, hotelkamers, ontmoetingsplaatsen, conferentiecentra, en andere onbeschermde gebieden buiten het organisatieterrein.

De persoon die de draagbare computerapparatuur van het (organisatie) terrein afneemt moet zich aan de volgende regels houden:

- draagbare computerapparatuur die belangrijke, gevoelige of kritische informatie bevat dient niet onbeheerd gelaten te worden en, indien mogelijk, zou het fysiek opgesloten moeten worden, of moeten special sloten worden gebruik om de apparatuur veilig te stellen
- wanneer draagbare computerapparatuur in openbare ruimten worden gebruikt, dan dient de gebruiker er zorg voor te dragen dat de gegevens niet door een onbevoegd persoon kunnen worden gelezen

Comment [DK5]: Verwijder dit hele item indien beheersmaatregel A.11.2.5 als niet van toepassing is aangegeven in de Verklaring van Toepasselijkheid.

- updates of patches en andere systeeminstellingen worden uitgevoerd [specificeer hoe dit
- wordt geïmplementeerd, of refereer aan een document dat dit proces beschrijft]
- de persoon die de draagbare computerapparatuur buiten het (organisatie) terrein gebruikt is
- verbinding met communicatienetwerken en gegevensuitwisseling dienen de gevoeligheid van gegevens te weerspiegelen en wordt uitgevoerd [specificeer hoe dit technisch wordt
- is voor de hele harde schijf of alleen de gevoelige bestanden, enz.]
- bescherming van gevoelige gegevens dient te worden geïmplementeerd in overeenstemming
- voor onbeheerde gebruikersapparatuur worden toegepast in overeenstemming met het Clear Desk and Clear Screen-beleid

die personen die draagbare computerapparatuur gebruiken buiten het terrein.

4. Telewerken

Telewerken betekent dat informatie en communicatieapparatuur wordt gebruikt om werknemers
telefoons buiten het terrein van de organisatie.

[specificeer de autorisatiemethode].

[Functie] is verantwoordelijk voor het voorbereiden van plannen en procedures om het volgende te waarborgen:

Comment [D6]: In kleinere bedrijven hoeven van vastgestelde regels moet volstaan.

- bescherming van draagbare computerapparatuur as aangeven in het voorgaande sectie
- op de locatie waar het telewerken wordt uitgevoerd
- relevante configuratie van het lokale netwerk gebruikt voor het verbinden met het internet
- bescherming van de intellectuele eigendomsrechten van de organisatie, of voor software of
- dienstverband
- minimale niveau van configuratie van de faculteit waar het telewerken zal worden uitgevoerd

5. Registratiebeheer op basis van dit document

Naam registratie	Opslaglocatie	Persoon verantwoordelijk voor opslag	Beveiligingsmaatregelen voor registraties	Bewaartermijn
[Authorisatie voor telewerken]	[specificeer, de vorm van autorisatie in aanmerking nemend]	[functie]	[specificeer, de vorm van autorisatie in aanmerking nemend]	Registraties worden opgeslagen voor 3 jaar
Plannen en procedures voor telewerken	[intranet van de organisatie]	[functie]	[alleen functie mag de intere regels wijzigen en publiceren	3 jaar

Comment [D7]: Pas aan indien nodig.

Alleen [functie] kan andere werknemers toegang tot een van de bovengenoemde documenten verlenen.

6. Geldigheid en documentbeheer

Dit document is geldig vanaf [datum].

De eigenaar van dit document is [functie]. Hij/zij dient het [illegible] het minstens eens per jaar bij te werken.

Comment [DK8]: Dit is slechts een aanbeveling, pas de frequentie zo nodig aan.

Wanneer de doeltreffendheid en toereikendheid van dit document wordt beoordeeld, dan dienen de [illegible] te worden genomen.

- aantal incidenten in verband met het meenemen van draagbare computerapparatuur buiten [illegible]
- [illegible] computerapparatuur buiten het terrein van de organisatie

[functie]
[naam]

_____
[handtekening]

Comment [DK9]: Alleen noodzakelijk indien de Procedure voor Beheersing voor Documenten en Registraties een ondertekening voorschrijft.