					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P34S					Titlu tad-dokument: **Politika dwar l-Apparati Mobbli u l-BYOD**							
Verżjoni: 1.0		Data tad-dħul fis-seħħ: 01.01.2025			Sid tad-dokument:							
X	Politika		Standard		Proċedura		Formola		Reġistru		Oħra	

Storja tar-reviżjonijiet				
Numru tar-reviżjoni	**Data tar-reviżjoni**	**Bidliet**	**Ivrevedut minn**	**Sid tal-proċess**

Approvazzjonijiet			
Isem	**Pożizzjoni**	**Data**	**Firma**

Allinjata mal-istandards u mar-regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżoli 5.1, 5.2, 6.1, 6.2, 8	Rekwiżiti ġenerali tal-ISMS u kontrolli għall-apparati mobbli/BYOD
ISO/IEC 27002:2022	Kontrolli 5.10–5.13	Kontrolli dettaljati għall-apparati mobbli/BYOD u l-aċċess remot
NIST SP 800-53 Rev.5	AC-19, AC-20, CM-6, MP-7	Kontrolli federali għall-apparati, il-mezzi u l-konfigurazzjoni
GDPR tal-UE	Artikolu 5(1)(f)	Protezzjoni tad-data personali u tal-endpoints mobbli
Direttiva NIS2 tal-UE	Artikolu 21(2)(d)	Protezzjoni ta' apparati kritiċi għan-negozju, inkluż il-BYOD
DORA tal-UE	Artikoli 9, 10	Ġestjoni tar-riskju tal-ICT u kontinwità għal endpoints mobbli
COBIT 2019	APO13, DSS01, DSS05	Governanza tal-IT, operazzjonijiet u kontrolli tas-servizzi tas-sigurtà

Għan

1.1. Din il-politika tiddefinixxi r-rekwiżiti obbligatorji tas-sigurtà għall-użu ta' apparati mobbli, inklużi smartphones, tablets u laptops, meta jiġi aċċessat tagħrif, sistemi jew servizzi tal-kumpanija.

1.2. Tirregola wkoll l-użu ta' Bring Your Own Device (BYOD) sabiex tiżgura li d-data tal-klijenti u tan-negozju tkun protetta, irrispettivament minn min ikun is-sid tal-apparat.

1.3. Il-politika tistabbilixxi salvagwardji konsistenti għall-aċċess mobbli, tgħin biex jintlaħqu l-objettivi taċ-ċertifikazzjoni ISO/IEC 27001, u tipprevjeni telf ta' data jew kompromess minħabba endpoints mobbli mitlufa, misruqa jew użati ħażin.

1.4. Tiżgura li jiġu applikati kemm kontrolli tekniċi kif ukoll proċedurali għall-użu mobbli f'SMEs mingħajr timijiet dedikati tal-IT, inklużi ambjenti ta' xogħol remot u servizzi fil-cloud.

2. Kamp ta' applikazzjoni

2.1. Din il-politika tapplika għall-impjegati, kuntratturi, interns u fornituri tas-servizzi kollha li:

2.1.1. Jużaw apparat mobbli biex jaċċessaw, jipproċessaw jew jaħżnu data jew sistemi tal-kumpanija

2.1.2. Jikkonnettjaw ma' servizzi tal-kumpanija, inkluż l-email, folders kondiviżi, apps fil-cloud jew sistemi interni permezz ta' VPN

2.2. Tkopri:

2.2.1. L-apparati mobbli kollha: smartphones, tablets u laptops, kemm jekk ipprovduti mill-kumpanija kif ukoll jekk personali taħt BYOD

2.2.2. Is-sistemi operattivi kollha (eż. iOS, Android, Windows, macOS)

2.2.3. Il-postijiet kollha (uffiċċju, dar, remot, spazji pubbliċi)

2.3. Il-politika tapplika fl-ambjenti kollha tax-xogħol u għandha tiġi infurzata irrispettivament mis-sjieda tal-apparat.

3. Objettivi

3.1. Prevenzjoni tat-Telf tad-Data (DLP): Jiġi żgurat li l-użu mobbli ma jesponix data sensittiva tal-kumpanija jew tal-klijenti għal aċċess mhux awtorizzat, serq jew użu ħażin.

3.2. Jiġu ddefiniti regoli ċari għall-BYOD: Jiġu stabbiliti kundizzjonijiet infurzabbli għall-użu ta' apparati personali għal skopijiet tan-negozju, b'salvagwardji legali u tekniċi adegwati.

3.3. Appoġġ għall-konformità regolatorja: Jintlaħqu r-rekwiżiti tal-ISO/IEC 27001, tal-GDPR, tan-NIS2 u obbligi legali oħra permezz ta' prattiki infurzabbli ta' sigurtà mobbli.

3.4. Tnaqqis tar-riskju operattiv: Tnaqqas il-probabbiltà ta' tfixkil operattiv ikkawżat minn użu ħażin, kompromess jew falliment ta' apparat mobbli.

3.5. Jinżamm il-fiduċja tal-klijenti: Tintwera lill-klijenti u lis-sħab li d-data tagħhom tibqa' protetta anke meta tiġi aċċessata fuq apparati mobbli jew apparati personali.

4. Rwoli u responsabbiltajiet

4.1. Maniġer Ġenerali (GM):

4.1.1. Iżomm ir-responsabbiltà ġenerali għal din il-politika.

4.1.2. Japprova kull użu ta' apparati mobbli u aċċess BYOD għas-sistemi tal-kumpanija.

4.1.3. Jiżgura li l-ftehimiet tal-BYOD jiġu ffirmati, miżmuma u mmonitorjati.

4.1.4. Jivverifika li fornituri esterni ta' servizzi tal-IT japplikaw il-protezzjonijiet meħtieġa għall-użu mobbli.

4.2. Persunal maħtur jew Appoġġ tal-IT:

4.2.1. Jassisti fl-istabbiliment, fir-reġistrazzjoni u fil-konfigurazzjoni ta' apparati mobbli użati għax-xogħol.

4.2.2. Japplika kontrolli tal-aċċess relatati mal-użu mobbli, restrizzjonijiet fuq l-apps u politiki ta' monitoraġġ.

4.2.3. Jappoġġa r-rispons għal inċidenti relatati ma' apparati mobbli, inklużi apparati mitlufa, misruqa jew kompromessi.

[... Is-sezzjonijiet 4.3–8 mhumiex inklużi f'dan il-preview. Ixtri d-dokument sħiħ biex taċċessa l-kontenut kollu. ...]

9. Rekwiżiti għar-rieżami u l-aġġornament

9.1. Rieżami annwali

9.1.1. Il-Maniġer Ġenerali (GM) għandu jirrieżamina din il-politika mill-inqas darba kull 12-il xahar.

9.1.2. Ir-rieżami għandu jivverifika allinjament kontinwu mar-rekwiżiti tal-ISO/IEC 27001, mat-teknoloġiji mobbli li qed jevolvu, u mal-bidliet fl-operazzjonijiet tan-negozju.

9.1.3. L-aġġornamenti għandhom iqisu wkoll inċidenti reċenti, riżultati tal-awditjar, jew żviluppi regolatorji (eż. GDPR, NIS2, DORA).

9.2. Avvenimenti li jattivaw rieżami interim

9.2.1. Din il-politika għandha tiġi aġġornata minnufih jekk iseħħ xi wieħed minn dawn li ġejjin:

9.2.1.1. Inċident ewlieni ta' sigurtà mobbli (eż. ksur permezz ta' apparat mitluf jew hacked)

9.2.1.2. Bidla fil-pjattaformi appoġġjati jew fl-għodod tal-ġestjoni mobbli

9.2.1.3. Bidla legali jew regolatorja li taffettwa l-użu ta' apparati personali jew il-protezzjoni tad-data

9.2.1.4. Introduzzjoni ta' apps, servizzi jew għodod ġodda ta' partijiet terzi użati fuq apparati mobbli

9.3. Dokumentazzjoni tal-bidliet

9.3.1. Ir-rieżamijiet u l-aġġornamenti kollha għandhom jiġu dokumentati, inklużi d-data tar-rieżami, il-bidliet li saru u l-approvazzjoni tal-GM

9.3.2. Għandha tinżamm storja tal-kontroll tal-verżjonijiet għal finijiet ta' awditjar

9.4. Komunikazzjoni u aċċess

9.4.1. Il-GM għandu jiżgura li l-utenti kollha (impjegati, kuntratturi, partijiet terzi) jiġu infurmati bil-bidliet

9.4.2. Verżjonijiet aġġornati għandhom ikunu faċilment aċċessibbli, pereżempju f'folders kondiviżi jew fuq pjattaformi interni

10. Politiki relatati u rabtiet

10.1. Din il-politika tifforma parti mis-sett ġenerali ta' politiki tas-sigurtà tal-informazzjoni għall-SMEs u għandha tiġi implimentata flimkien ma' dawn li ġejjin:

10.1.1. P4S – Politika dwar il-Kontroll tal-Aċċess: Tiddefinixxi r-rekwiżiti għall-ġestjoni ta' aċċess sigur għas-sistemi, inklużi dawk aċċessati permezz ta' apparati mobbli. Tapplika l-iġjene tal-passwords u kontrolli tas-sessjonijiet.

10.1.2. P8S – Politika dwar l-Għarfien dwar is-Sigurtà tal-Informazzjoni u t-Taħriġ: Tiżgura li l-utenti jirċievu taħriġ dwar l-użu sigur ta' apparati mobbli, ir-rappurtar ta' inċidenti u l-kundizzjonijiet tal-BYOD.

10.1.3. P17S – Politika dwar il-Protezzjoni tad-Data u l-Privatezza: Tistabbilixxi l-immaniġġjar konformi mal-GDPR ta' data personali u data tal-kumpanija fuq pjattaformi mobbli, b'mod partikolari meta apparati personali jintużaw għax-xogħol.

10.1.4. P9S – Politika dwar ix-Xogħol Remot: Taqbel mal-aspettattivi għall-użu mobbli meta x-xogħol isir barra mis-sit jew mid-dar, inkluż l-immaniġġjar tal-apparati u s-salvagwardji tal-aċċess għan-network.

10.1.5. P30S – Politika dwar ir-Rispons għall-Inċidenti: Tipprovdi l-qafas ta' rispons għal inċidenti relatati ma' apparati mobbli, inklużi apparati kompromessi jew mitlufa.

10.2. Dawn il-politiki relatati jaħdmu flimkien biex jiffurmaw sett sħiħ ta' kontrolli għas-sigurtà tal-apparati mobbli f'SMEs mingħajr persunal dedikat tal-IT, u jiżguraw applikazzjoni, trasparenza u l-kapaċità li tintwera l-konformità.

11. Standards u oqfsa ta' referenza

11.1. Din il-politika tappoġġa allinjament sħiħ mal-istandards li ġejjin dwar is-sigurtà u l-konformità:

11.2. ISO/IEC 27001:

11.2.1. Klawżola 5.1 – Tmexxija u Impenn: Tiżgura sorveljanza mill-maniġment u responsabbiltà għall-aċċess mobbli u l-BYOD

11.2.2. Klawżola 6.1 – Azzjonijiet biex jiġi indirizzat ir-riskju: Teħtieġ li r-riskji tas-sigurtà mobbli jiġu evalwati u ttrattati

11.2.3. Klawżola 8.1 – Ippjanar u Kontroll Operattiv: Teħtieġ proċeduri konsistenti għall-aċċess mobbli sabiex tiġi salvagwardjata d-data tan-negozju

11.3. ISO/IEC 27002:

11.3.1. Kontrolli 5.10 (Użu ta' Apparati Mobbli), 5.11 (Teleworking), 5.12 (Aċċess Remot), u 5.13 (BYOD): Jipprovdu gwida għall-implimentazzjoni biex jiġu ġestiti r-riskji tal-apparati f'kuntest ta' negozju żgħir

11.4. NIST SP 800-53 Rev.5:

11.4.1. AC-19 – Kontroll tal-Aċċess għall-Apparati Mobbli: Jeħtieġ impostazzjonijiet tas-sigurtà għal użu mobbli awtorizzat

11.4.2. AC-20 – Użu ta' Sistemi Esterni: Jirregola r-riskji tal-BYOD u tal-aċċess remot

11.4.3. CM-6 – Impostazzjonijiet tal-konfigurazzjoni: Japplika impostazzjonijiet siguri predefiniti u personalizzati fuq pjattaformi mobbli

11.4.4. MP-7 – Użu tal-Mezzi: Jindirizza l-użu xieraq u r-restrizzjonijiet għall-ħażna mobbli u l-aċċess għad-data

11.5. GDPR tal-UE (2016/679):

11.5.1. Artikolu 5(1)(f) – Integrità u Kunfidenzjalità: Jeħtieġ il-protezzjoni tad-data permezz ta' sigurtà xierqa tad-data personali, b'mod partikolari fuq pjattaformi mobbli

11.5.2. Artikolu 32 – Sigurtà tal-Ipproċessar: Jobbliga l-użu ta' miżuri tekniċi u organizzattivi (TOMs) xierqa għas-sigurtà tad-data aċċessata jew maħżuna fuq apparati mobbli

11.6. Direttiva NIS2 tal-UE (2022/2555):

11.6.1. Artikolu 21(2)(d) – Miżuri tas-Sigurtà tal-Apparati: Jeħtieġ kontrolli tas-sigurtà għall-ħardwer u s-softwer użati biex jiġu aċċessati sistemi kritiċi tan-negozju, inklużi apparati personali

11.7. DORA tal-UE (2022/2554):

11.7.1. Artikolu 9 – Qafas tal-Ġestjoni tar-Riskju tal-ICT: Jeħtieġ il-protezzjoni ta' endpoints mobbli użati għal komunikazzjonijiet kritiċi tan-negozju u servizzi fil-cloud

11.7.2. Artikolu 10 – Kontinwità tan-Negozju tal-ICT: Japplika aċċess sigur kontinwu għas-sistemi tan-negozju anke waqt tfixkil jew xogħol remot

11.8. COBIT 2019:

11.8.1. APO13 – Manage Security: Jeħtieġ li l-organizzazzjoni tapplika politiki dwar apparati mobbli u BYOD allinjati mar-riskju tal-intrapriża

11.8.2. DSS01 – Manage Operations: Jiżgura l-implimentazzjoni teknika ta' mekkaniżmi ta' aċċess sigur

11.8.3. DSS05 – Manage Security Services: Jirregola l-involviment ta' partijiet terzi fiż-żamma ta' ambjenti mobbli siguri u l-koordinazzjoni tar-rispons għall-inċidenti