					Daħħal hawn l-isem tal-entità ġuridika rreġistrata						
Numru tad-dokument: P34					Titlu tad-dokument: **Politika dwar 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 r-regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	5.2, 6.1, 7.5, 8	Japplika kontrolli tas-sigurtà u rekwiżiti ta' konformità
ISO/IEC 27002:2022	5.10, 8.1, 8.5, 8	Jipprovdi kontrolli dettaljati għall-ġestjoni ta' apparati mobbli
NIST SP 800-53 Rev.5	AC-19, AC-17, CM-7, MP-5, SC-12	Kontroll tal-aċċess, aċċess remot, konfigurazzjoni u rekwiżiti tas-sigurtà għal apparati mobbli
GDPR tal-UE	5(1)(f), 25, 32	Rekwiżiti obbligatorji għall-privatezza, l-iċċifrar tad-data u s-sigurtà tal-ipproċessar
Direttiva NIS2 tal-UE	21(2)(d)	Miżuri tekniċi u organizzattivi ta' protezzjoni għall-aċċess mobbli
DORA tal-UE	9, 10	Rekwiżiti ta' ġestjoni tar-riskju tal-ICT u sigurtà għal apparati mobbli
COBIT 2019	APO13.02, DSS01.04, BAI09	Pjanijiet tas-sigurtà tal-informazzjoni, konfigurazzjoni tal-assi u kontrolli għal ambjenti mobbli

1. Għan

1.1 Din il-politika tistabbilixxi r-rekwiżiti tas-sigurtà, tal-konformità u operattivi għall-użu ta' apparati mobbli u teknoloġija personali (BYOD – Ġib l-Apparat Tiegħek) meta dawn jintużaw biex jiġi aċċessat is-sistemi, l-applikazzjonijiet jew id-data tal-organizzazzjoni.

1.2 L-għan tagħha huwa li tiżgura l-Kunfidenzjalità, l-Integrità u d-Disponibbiltà (CIA) tal-informazzjoni tal-kumpanija li tiġi aċċessata jew ipproċessata permezz ta' endpoints mobbli, inklużi smartphones, tablets, laptops u apparati ibridi.

1.3 Din il-politika tistabbilixxi wkoll il-kontrolli tekniċi u proċedurali meħtieġa biex jitnaqqsu riskji bħat-tnixxija tad-data, aċċess mhux awtorizzat, telf jew serq ta' apparat, u kompromess ta' applikazzjonijiet mobbli.

1.4 Din il-politika tappoġġa l-konformità regolatorja u kuntrattwali filwaqt li tippermetti produttività mobbli sigura għall-impjegati, kuntratturi u partijiet terzi awtorizzati.

2. Kamp ta' applikazzjoni

2.1 Din il-politika tapplika għall-persunal kollu, inklużi impjegati, kuntratturi, interns u fornituri ta' servizzi ta' partijiet terzi, li jużaw apparati mobbli biex jaċċessaw id-data, is-sistemi, l-applikazzjonijiet jew il-pjattaformi ta' komunikazzjoni tal-kumpanija.

2.2 Hija tkopri l-apparati kollha tal-komputazzjoni mobbli, inklużi iżda mhux limitati għal:

2.2.1 Smartphones u tablets (iOS, Android, eċċ.)

2.2.2 Laptops u ultrabooks (Windows, macOS, Linux)

2.2.3 Apparati li jintlibsu u apparati intelliġenti ibridi li kapaċi jwettqu sinkronizzazzjoni tad-data

2.3 Tapplika kemm jekk l-apparat ikun proprjetà tal-kumpanija kif ukoll jekk ikun apparat personali kopert taħt arranġament ta' BYOD.

2.4 Il-politika tkopri l-mezzi kollha ta' aċċess, inklużi VPNs, desktops virtwali, applikazzjonijiet cloud, posta elettronika, pjattaformi ta' kollaborazzjoni (eż. SharePoint, Teams) u għodod ta' sinkronizzazzjoni tal-fajls (eż. OneDrive, Dropbox jekk awtorizzat).

2.5 Tinkludi l-użu fix-xogħol remot, fuq il-post, waqt l-ivvjaġġar jew f'arranġamenti ta' xogħol ibridu.

3. Objettivi

3.1 Li jitnaqqas ir-riskju ta' kompromess, tnixxija jew telf ta' data minħabba użu mhux sigur ta' apparati mobbli.

3.2 Li jiġu applikati kontrolli tas-sigurtà konsistenti u infurzabbli fuq l-endpoints mobbli kollha, irrispettivament mill-mudell ta' sjieda tagħhom (korporattiv jew BYOD).

3.3 Li jiġi żgurat li l-użu ta' apparati mobbli jkun konformi ma' ISO/IEC 27001 u ma' oqfsa regolatorji oħra applikabbli għall-privatezza, il-protezzjoni tad-data u ċ-ċibersigurtà.

3.4 Li tiġi ffaċilitata l-integrazzjoni sigura ta' apparati mobbli fil-flussi tax-xogħol operattivi, ta' komunikazzjoni u ta' kollaborazzjoni tal-organizzazzjoni.

3.5 Li jiġu stabbiliti responsabbiltajiet u proċessi definiti b'mod ċar għall-Ġestjoni ta' Apparati Mobbli (MDM), inklużi r-reġistrazzjoni, it-tħassir remot, l-iċċifrar, l-awtentikazzjoni u l-monitoraġġ.

3.6 Li jiġu protetti d-drittijiet tal-privatezza tal-individwi li jużaw l-apparati tagħhom stess filwaqt li tiġi ssalvagwardjata l-informazzjoni sensittiva tal-organizzazzjoni.

4. Rwoli u responsabbiltajiet

4.1 Uffiċjal Ewlieni tas-Sigurtà tal-Informazzjoni / Maniġer tas-Sigurtà tal-IT

4.1.1 Jiddefinixxi l-politika u l-istandards tekniċi għall-użu ta' apparati mobbli u tal-BYOD.

4.1.2 Jeżerċita sorveljanza fuq il-konformità, ir-rispons għall-inċidenti u l-ġestjoni tal-eċċezzjonijiet għall-kontrolli ta' apparati mobbli.

4.1.3 Jikkoordina mat-timijiet Legali u tar-Riżorsi Umani biex jiżgura li l-applikazzjoni tal-politika tkun ibbażata legalment u allinjata mar-rekwiżiti organizzattivi.

4.2 Amministratur tal-IT / Amministratur tal-MDM

4.2.1 Jimmaniġġja l-għoti tal-aċċess, ir-reġistrazzjoni u l-konfigurazzjoni ta' apparati mobbli permezz ta' soluzzjonijiet ta' Ġestjoni ta' Apparati Mobbli (MDM).

4.2.2 Japplika kontrolli fil-livell tal-apparat (eż. iċċifrar, kodiċijiet PIN, kontrolli tal-applikazzjonijiet).

4.2.3 Jagħmel tħassir remot, lockout tal-apparat u tneħħija tal-aċċess meta jkun meħtieġ.

[... 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 Din il-politika għandha tiġi riveduta mill-inqas kull sena mill-Uffiċjal Ewlieni tas-Sigurtà tal-Informazzjoni jew minn Maniġer tas-Sigurtà tal-Informazzjoni maħtur biex jiġi żgurat l-allinjament ma':

9.1.1 Bidliet fil-pjattaformi tal-OS mobbli, fit-teknoloġiji tal-MDM jew fl-istandards tal-awtentikazzjoni

9.1.2 Bidliet regolatorji jew kuntrattwali li jaffettwaw il-protezzjoni tad-data mobbli (eż. GDPR, DORA, NIS2)

9.1.3 Reviżjonijiet tas-settijiet ta' kontrolli ta' ISO/IEC 27001:2022, ISO/IEC 27002:2022 jew NIST SP 800-53 Rev.5

9.1.4 Feedback minn awditi, analiżijiet wara inċident jew rapporti tal-impjegati

9.2 Jistgħu jinbdew rieżamijiet interim minħabba:

9.2.1 Inċidenti tas-sigurtà li jinvolvu apparati mobbli jew pjattaformi BYOD

9.2.2 Notifika minn fornitur dwar vulnerabbiltajiet ta' riskju għoli fil-pjattaformi appoġġjati

9.2.3 Introduzzjoni ta' applikazzjonijiet mobbli ġodda jew pjattaformi ta' kollaborazzjoni użati għall-operazzjonijiet tan-negozju

9.3 L-aġġornamenti tal-politika għandhom ikunu:

9.3.1 Dokumentati fl-istorja tal-verżjonijiet tal-politika

9.3.2 Ikkomunikati lill-persunal kollu u lill-kuntratturi affettwati

9.3.3 Ikkonfermati mill-ġdid b'rikonoxximent aġġornat mill-utenti kollha tal-BYOD

9.4 Ir-rieżamijiet u r-reviżjonijiet kollha għandhom jiġu approvati formalment mill-Maniġment Eżekuttiv u rreġistrati fir-reġistru tal-bidliet fil-politika.

10. Politiki relatati u rabtiet

10.1 Din il-politika hija interdipendenti ma' diversi politiki ewlenin fil-qafas tal-ISMS tal-organizzazzjoni. Ir-rabtiet ewlenin jinkludu:

10.1.1 P1 – Politika tas-Sigurtà tal-Informazzjoni: Tistabbilixxi l-prinċipji ġenerali ta' governanza għall-kontrolli kollha tas-sigurtà tal-informazzjoni, inklużi dawk li jirregolaw l-użu ta' apparati mobbli.

10.1.2 P3 – Politika dwar Użu Aċċettabbli: Tiddefinixxi mġiba permessa u restrizzjonijiet relatati mal-użu tat-teknoloġija, li japplikaw direttament għall-aċċess mobbli u tal-BYOD.

10.1.3 P9 – Politika dwar ix-Xogħol Remot: Tindirizza obbligi addizzjonali tas-sigurtà għal ambjenti ta' xogħol mobbli, u tikkumplimenta l-kontrolli speċifiċi għall-mowbajl definiti f'din il-politika.

10.1.4 P13 – Politika ta' Klassifikazzjoni u Tikkettar tad-Data: Tirregola kif data fuq apparati mobbli għandha tiġi mmaniġġjata skont il-livell ta' klassifikazzjoni, u taffettwa l-ħażna, it-trasferiment u l-applikazzjoni tal-iċċifrar.

10.1.5 P22 – Politika tal-Illoggjar u l-Monitoraġġ: Tappoġġa l-ġbir u r-rieżami tal-logs tal-aċċess mobbli biex jinstabu anomaliji jew ksur.

10.1.6 P30 – Politika dwar ir-Rispons għall-Inċidenti: Tirregola kif jiġu mmaniġġjati u eskalati inċidenti relatati ma' apparati mobbli (eż. telf ta' apparat, aċċess mhux awtorizzat).

10.1.7 P33 – Politika dwar il-Monitoraġġ tal-Awditu u l-Konformità: Tipprovdi l-bażi għal verifiki perjodiċi tal-konformità tas-sigurtà mobbli, inkluża l-konformità mal-politika tal-BYOD.

11. Standards u oqfsa ta' referenza

11.1 Din il-politika hija allinjata ma' oqfsa taċ-ċibersigurtà rikonoxxuti internazzjonalment u ma' obbligi legali biex jiġi żgurat l-użu sigur ta' apparati mobbli u teknoloġiji personali (BYOD) f'ambjenti intrapriżali.

11.2 ISO/IEC 27001:

11.2.1 Klawżola 5.10 – Użu Awtorizzat tal-Informazzjoni u tal-Assi: Teħtieġ kontrolli għall-użu responsabbli tal-assi korporattivi, inklużi apparati mobbli.

11.2.2 Klawżola 5.11 – Xogħol Remot: Tirregola prattiki siguri meta jiġu aċċessati sistemi minn barra l-binjiet tal-kumpanija.

11.2.3 Klawżola 5.12 – Użu ta' Apparati Mobbli: Tobbliga kontrolli bbażati fuq ir-riskju għal endpoints mobbli u konfigurazzjonijiet tal-BYOD.

11.2.4 Klawżola 5.13 – Trasferiment tal-Informazzjoni: Teħtieġ il-protezzjoni tal-informazzjoni trasferita permezz ta' kanali mobbli.

11.3 ISO/IEC 27002:2022 – Kontrolli 5.10 sa 5.13:

11.3.1 Kontrolli tal-Anness A 5.10 sa 5.13: Jispeċifikaw kif l-aċċess mobbli, l-iċċifrar, il-monitoraġġ u l-mitigazzjoni tat-telf għandhom jiġu applikati fi ħdan l-ISMS. Dawn il-kontrolli jipprovdu gwida dettaljata għall-implimentazzjoni biex jiġu żgurati endpoints mobbli, jiġi applikat il-containerization, tiġi mmonitorjata l-integrità tal-apparat u jiġu żgurati konfigurazzjonijiet li jqisu l-privatezza għall-użu tal-BYOD.

11.4 NIST SP 800-53 Rev.5:

11.4.1 AC-19 – Kontroll tal-Aċċess għal Apparati Mobbli: Jiddefinixxi salvagwardji bażi, inklużi l-iċċifrar, l-awtentikazzjoni u l-applikazzjoni tal-MDM.

11.4.2 AC-17 – Aċċess Remot: Jeħtieġ awtentikazzjoni sigura u protezzjoni tas-sessjonijiet għal utenti mobbli remoti.

11.4.3 CM-7 – L-inqas funzjonalità meħtieġa: Jappoġġa t-tneħħija ta' applikazzjonijiet u karatteristiċi mhux meħtieġa minn endpoints mobbli biex jitnaqqas ir-riskju.

11.4.4 MP-5 – Protezzjoni tat-Trasport tal-Mezzi: Tirregola t-trażmissjoni sigura ta' data minn sistemi mobbli lejn destinazzjonijiet esterni jew servizzi cloud.

11.4.5 SC-12 – Stabbiliment ta' Ċwievet Kriptografiċi: Jobbliga l-użu ta' protokolli kriptografiċi siguri għall-komunikazzjoni u l-ħażna mobbli.

11.5 GDPR tal-UE (2016/679):

11.5.1 Artikolu 5(1)(f) – Integrità u Kunfidenzjalità: Jeħtieġ li l-organizzazzjonijiet jipproteġu d-data personali fuq apparati mobbli kontra aċċess mhux awtorizzat jew illegali.

11.5.2 Artikolu 25 – Protezzjoni tad-Data mid-Disinn u b'Mod Predefinit: Jeħtieġ li l-privatezza tkun inkorporata fil-proċessi tal-BYOD u tal-MDM.

11.5.3 Artikolu 32 – Sigurtà tal-Ipproċessar: Jinforza kontrolli bbażati fuq ir-riskju (eż. iċċifrar, awtentikazzjoni, kontroll tal-aċċess) għal data personali fuq pjattaformi mobbli.

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

11.6.1 Artikolu 21(2)(d): Jobbliga li l-aċċess mobbli għal sistemi u informazzjoni kritiċi jiġi protett permezz ta' miżuri tekniċi u organizzattivi xierqa, bħal kontroll tal-endpoint, iċċifrar u monitoraġġ.

11.7 DORA tal-UE (2022/2554):

11.7.1 Artikolu 9 – Qafas tal-Ġestjoni tar-Riskju tal-ICT: Jeħtieġ li entitajiet fis-settur finanzjarju jnaqqsu r-riskji ta' aċċess mobbli u remot bħala parti mir-reżiljenza operattiva.

11.7.2 Artikolu 10 – Rekwiżiti tas-Sigurtà tas-Sistemi tal-ICT: Jeżiġi arkitettura mobbli sigura, monitoraġġ u mekkaniżmi ta' rispons għal theddid ċibernetiku li joriġina minn apparati mobbli.

11.8 COBIT 2019:

11.8.1 APO13.02 – Stabbilixxi u Żomm Pjan tas-Sigurtà tal-Informazzjoni: Jeħtieġ li l-użu ta' apparati mobbli, inkluż il-BYOD, jiġi integrat fl-istrateġiji tas-sigurtà tal-organizzazzjoni.

11.8.2 DSS01.04 – Immaniġġja l-Konfigurazzjoni u l-Integrità tal-Assi: Japplika għall-kontroll tal-konfigurazzjoni u l-implimentazzjoni sigura ta' apparati mobbli.

11.8.3 BAI09.01 – Stabbilixxi u Żomm Kontrolli: Jappoġġa l-implimentazzjoni ta' salvagwardji tekniċi u proċedurali għal operazzjonijiet mobbli u remoti siguri.