					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P03					Titlu tad-dokument: **Politika dwar l-Użu Aċċettabbli**							
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 ma’ standards u regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżola 5	Tistabbilixxi normi ta’ mġiba u rekwiżiti għall-Politika dwar l-Użu Aċċettabbli
ISO/IEC 27002:2022	Kontrolli 6.1, 6.2, 8.1, 8.12	Tiggwida r-responsabbiltajiet tas-sigurtà tal-informazzjoni, l-għarfien, u l-governanza tal-apparat u tad-data
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Kontrolli tal-aċċess u tal-għarfien rilevanti għall-użu tal-assi tal-IT
GDPR tal-UE	Artikoli 5(1)(f), 32; Premessa 39	Teħtieġ il-kunfidenzjalità u l-integrità, timponi kontrolli tekniċi u organizzattivi, u bażijiet legali għall-użu xieraq
Direttiva NIS2 tal-UE	Artikolu 21(2)(a–d)	Teħtieġ politiki operazzjonali u taħriġ dwar użu sigur
DORA tal-UE	Artikolu 5	Tappoġġa l-ġestjoni tar-riskju tal-ICT billi tirregola l-imġiba tal-utenti
COBIT 2019	APO07, BAI05, DSS05, MEA01	Riżorsi umani, ġestjoni tal-bidla, servizzi ta’ sigurtà ġestiti, monitoraġġ tal-konformità u tal-prestazzjoni

1. Għan

1.1 Din il-politika tiddefinixxi l-użu aċċettabbli u dak mhux aċċettabbli tas-sistemi tal-informazzjoni tal-organizzazzjoni, tar-riżorsi informatiċi, tal-għodod ta’ komunikazzjoni u tal-prattiki ta’ ġestjoni tad-data.

1.2 Hija tiżgura li l-utenti kollha jifhmu r-responsabbiltajiet tagħhom meta jużaw assi tal-IT korporattivi u li l-azzjonijiet tagħhom jappoġġaw il-kunfidenzjalità, l-integrità, id-disponibbiltà u l-ipproċessar legali tal-informazzjoni.

1.3 Il-politika tissodisfa l-Klawżola 5.10 tal-ISO/IEC 27001:2022 billi tistabbilixxi regoli ta’ mġiba għall-użu tas-sistemi u tapplika salvagwardji tekniċi u proċedurali biex tnaqqas ir-riskju ta’ użu ħażin, negliġenza jew abbuż.

1.4 Hija tappoġġa wkoll attivitajiet ta’ investigazzjoni u implimentazzjoni, inkluż ir-rispons għall-inċidenti u miżuri dixxiplinarji għal ksur.

2. Kamp ta’ applikazzjoni

2.1 Din il-politika tapplika għall-individwi u l-entitajiet kollha li jingħataw aċċess għas-sistemi tal-informazzjoni u l-assi tal-organizzazzjoni, inklużi iżda mhux limitati għal:

2.1.1 Impjegati, kuntratturi, konsulenti, apprendisti u persunal ta’ aġenziji

2.1.2 Forniturі terzi b’aċċess għas-sistemi jew b’rwoli amministrattivi delegati

2.1.3 Mistednin jew imsieħba li jużaw infrastruttura tal-IT tal-organizzazzjoni jew awtorizzata minnha

2.2 Il-kamp ta’ applikazzjoni jinkludi l-assi teknoloġiċi u tad-data kollha tal-organizzazzjoni, inklużi:

2.2.1 Workstations, laptops, apparat mobbli u servers

2.2.2 Infrastruttura tan-network u servizzi ospitati fil-cloud

2.2.3 Email, messaġġi, ħażna ta' fajls, pjattaformi ta' kollaborazzjoni u VPNs

2.2.4 Data maħżuna, data fi tranżitu jew data waqt l-ipproċessar, irrispettivament mill-format jew mil-lokazzjoni

2.2.5 Kull apparat personali użat taħt arranġament BYOD (Bring Your Own Device) li jikkonnettja mas-sistemi tal-organizzazzjoni

2.3 Din il-politika tapplika fl-ambjenti tax-xogħol kollha, inklużi:

2.3.1 Uffiċini korporattivi u siti tal-produzzjoni

2.3.2 Postijiet ta' xogħol remot jew arranġamenti ibridi

2.3.3 Operazzjonijiet fuq il-post jew binjiet amministrati minn partijiet terzi

2.4 L-utenti kollha għandhom jirrikonoxxu u josservaw din il-politika bħala kundizzjoni għall-aċċess għas-sistemi tal-kumpanija jew għall-ġestjoni tad-data korporattiva.

3. Objettivi

3.1 Li jiġu definiti u infurzati regoli għall-użu aċċettabbli tar-riżorsi tal-IT tal-organizzazzjoni.

3.2 Li jiġi evitat aċċess mhux awtorizzat, tnixxija ta' data jew ħsara li tirriżulta minn użu negliġenti jew malizzjuż.

3.3 Li jiġu protetti n-networks, l-assi u d-data tal-kumpanija minn theddid introdott permezz tal-imġiba tal-utenti.

3.4 Li jiġu appoġġati obbligi legali u kuntrattwali billi tintwera diliġenza dovuta fil-governanza tar-riżorsi tal-IT.

3.5 Li tiġi żgurata konsistenza u ċarezza fl-applikazzjoni ta' azzjonijiet dixxiplinarji u ta' proċessi għall-ġestjoni tal-eċċezzjonijiet.

3.6 Li tiġi promossa kultura ta' użu etiku, sigur u responsabbli tar-riżorsi informatiċi diġitali u fiżiċi.

4. Rwoli u responsabbiltajiet

4.1 Il-Maniġment Eżekuttiv

4.1.1 Japprova l-Politika dwar l-Użu Aċċettabbli (AUP) u jiżgura li tkun allinjata mal-objettivi tan-negozju, mar-rekwiżiti regolatorji u mal-valuri tal-organizzazzjoni.

4.1.2 Jalloka riżorsi għall-implimentazzjoni, it-taħriġ, il-monitoraġġ u r-rieżami tal-politika.

4.1.3 Jagħmel rieżami tal-istatus tal-konformità u tal-azzjonijiet dixxiplinarji marbuta ma' ksur tal-politika bħala parti mill-governanza tal-ISMS.

4.2 It-timijiet tal-IT u tas-Sigurtà tal-Informazzjoni

4.2.1 Jimplimentaw salvagwardji tekniċi biex jinfurzaw din il-politika, inklużi:

4.2.2 Filtrazzjoni tal-kontenut, protezzjoni kontra l-malware, sigurtà tal-endpoints u għodod ta' monitoraġġ tan-network

4.2.3 Konfigurazzjonijiet tas-sigurtà tal-email u soluzzjonijiet għall-prevenzjoni tat-telf ta' data (DLP)

4.2.4 Blocklists u allowlists għal software, hardware u websites

4.2.5 Iżommu inventarju ta' software, apparat u servizzi approvati u pprojbiti.

4.2.6 Jinvestigaw ksur suspettat tal-AUP, jiġbru evidenza forensika u jappoġġaw azzjoni dixxiplinarja jew legali fejn xieraq.

4.2.7 Jikkollaboraw mar-Riżorsi Umani u mal-funzjoni Legali dwar il-ġestjoni tal-inċidenti, l-eskalazzjoni u l-obbligi ta' rappurtar.

[... 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 Skattaturi u frekwenza tar-rieżami

9.1.1 Din il-politika għandha tiġi riveduta:

9.1.1.1 Mill-inqas darba fis-sena

9.1.1.2 Wara kull bidla sinifikanti fit-teknoloġija jew fl-infrastruttura

9.1.1.3 Wara inċidenti jew sejbiet tal-awditjar li juru nuqqasijiet fl-implimentazzjoni

9.1.1.4 B'reazzjoni għal bidliet fil-liġijiet jew fil-kuntratti applikabbli

9.2 Sjieda u approvazzjoni

9.2.1 Is-CISO jew il-Maniġer tal-ISMS innominat huwa responsabbli mill-proċess ta' rieżami.

9.2.2 L-aġġornamenti għandhom jiġu approvati mill-Maniġment Eżekuttiv u kkomunikati fl-organizzazzjoni kollha.

9.2.3 Ir-rikonoxximent tat-termini aġġornati għandu jerġa' jinġabar meta l-politika terġa' tinħareġ.

9.3 Ġestjoni tad-dokument

9.3.1 Il-politika għandha tinkludi l-metadata u d-dettalji tal-verżjonar li ġejjin:

9.3.1.1 Titlu, ID u livell ta' klassifikazzjoni

9.3.1.2 Sid il-politika u kustodju tad-dokument

9.3.1.3 Storja tal-bidliet u r-raġuni għall-aġġornamenti

9.3.1.4 Dati tar-rieżami u tal-aġġornament skedat li jmiss

9.3.1.5 Referenzi għad-distribuzzjoni u għal-log tar-rikonoxximent

9.3.2 Il-kopja ewlenija għandha tinżamm fir-Repożitorju tad-Dokumenti tal-ISMS taħt kontroll tal-verżjoni.

10. Politiki relatati u rabtiet

10.1 Din il-politika għandha tiġi interpretata flimkien ma' dawn li ġejjin:

10.1.1 P1 – Politika tas-Sigurtà tal-Informazzjoni: Tistabbilixxi l-aspettattivi bażiċi tal-imġiba u l-impenn tal-maniġment superjuri lejn l-użu aċċettabbli.

10.1.2 P4 – Politika ta' Kontroll tal-Aċċess: Tiddefinixxi l-permessi u d-drittijiet marbuta mal-utenti, mas-sistemi u mal-aċċess għad-data, u b'hekk tinforza direttament il-limiti tal-użu aċċettabbli.

10.1.3 P6 – Politika ta' Ġestjoni tar-Riskju: Tindirizza r-riskji relatati mal-imġiba u tappoġġa l-attivitajiet ta' monitoraġġ u trattament marbuta ma' theddid ikkawżat mill-utenti.

10.1.4 P7 – Politika dwar l-Onboarding u t-Terminazzjoni: Tiżgura li t-termini tal-użu aċċettabbli jiġu rikonoxxuti mal-ingaġġ u revokati mat-tluq.

10.1.5 P9 – Politika dwar ix-Xogħol Remot: Testendi d-dispożizzjonijiet tal-użu aċċettabbli għall-ambjenti ta' xogħol remot u ibridu.

10.2 Dawn il-politiki relatati jiffurmaw mudell ta' difiża f'saffi għall-governanza tal-imġiba, teknika u kuntrattwali.

11. Standards u oqfsa ta' referenza

11.1 Din il-Politika dwar l-Użu Aċċettabbli (AUP) hija allinjata ma' standards internazzjonalment rikonoxxuti u ma' oqfsa legali biex tiżgura kontrolli tal-imġiba applikabbli, adattati għall-awditjar u bbażati fuq ir-riskju fl-użu kollu tas-sistemi ta' informazzjoni diġitali u fiżiċi.

11.2 ISO/IEC 27001:2022

11.2.1 Klawżola 5.10 – Użu Aċċettabbli tal-Informazzjoni u ta' Assi Oħra Assoċjati: Din il-politika tissodisfa direttament ir-rekwiżit li jiġu definiti, ikkomunikati u infurzati regoli li jirregolaw l-użu xieraq tar-riżorsi tal-IT.

11.2.2 Kontroll 6.1 tal-Anness A – Responsabbiltà għas-Sigurtà tal-Informazzjoni: Jassenja responsabbiltajiet ċari għall-imġiba tal-utenti u għas-sorveljanza tal-konformità.

11.2.3 Kontroll 6.2 tal-Anness A – Għarfien, Edukazzjoni u Taħriġ dwar is-Sigurtà tal-Informazzjoni: It-taħriġ integrat u l-proċessi ta' rikonoxximent tal-politika huma parti mill-implimentazzjoni tal-AUP.

11.2.4 Kontroll 8.1 tal-Anness A – Apparat tal-Utent fl-Endpoint u 8.12 – Prevenzjoni tat-Telf ta' Data: Jindirizza l-imġiba aċċettabbli fuq apparat tal-utenti u jirregola attivitajiet li jistgħu jwasslu għal esponiment jew tnixxija ta' data.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-19 (Kontroll tal-Aċċess għal Apparati Mobbli) u AC-20 (Użu ta' Sistemi ta' Informazzjoni Esterni): Din il-politika tiddefinixxi l-obbligi u r-restrizzjonijiet tal-utenti għal BYOD u għall-aċċess għal sistemi ta' partijiet terzi.

11.3.2 PL-4 (Regoli ta' Mġiba): Jipprovdi rekwiżiti dettaljati ta' użu aċċettabbli konsistenti ma' din il-politika.

11.3.3 AT-2 (Taħriġ dwar l-Għarfien tas-Sigurtà): Appoġġat permezz tat-taħriġ tal-utenti u r-rikonoxximent dokumentat tal-politika.

11.3.4 AU-2 (Avvenimenti ta' Awditjar) u AU-12 (Ġenerazzjoni tal-Awditjar): L-implimentazzjoni tiddependi fuq il-monitoraġġ tal-azzjonijiet tal-utenti u twissijiet dwar ksur.

11.4 GDPR tal-UE (2016/679):

11.4.1 Artikolu 5(1)(f): Jeħtieġ is-sigurtà u l-integrità tad-data personali; din il-politika ttaffi r-riskji introdotti mill-imġiba umana u mill-użu mhux awtorizzat.

11.4.2 Artikolu 32: Jeħtieġ miżuri tekniċi u organizzattivi, bħal kontrolli fuq l-imġiba u restrizzjonijiet fl-użu, biex tiġi protetta d-data personali.

11.4.3 Premessa 39: Tenfasizza l-ħtieġa li jiġi żgurat li l-aċċess għad-data jkun biss dak meħtieġ u li l-użu tagħha jkun legali minn individwi awtorizzati.

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

11.5.1 Artikolu 21(2)(a–d): Jeħtieġ politiki operazzjonali u taħriġ għall-użu sigur tas-sistemi, li din l-AUP tipprovdi billi tiddefinixxi l-imġiba, il-monitoraġġ u l-proċessi ta' implimentazzjoni.

11.6 DORA tal-UE (2022/2554):

11.6.1 Artikolu 5: Din il-politika tappoġġa l-qafas ta' ġestjoni tar-riskju tal-ICT billi tiddefinixxi regoli għall-interazzjoni bejn il-bniedem u s-sistema u billi tnaqqas l-esponiment għar-riskju ċibernetiku bbażat fuq l-imġiba.

11.7 COBIT 2019:

11.7.1 APO07 – Riżorsi Umani Ġestiti: Japplika r-responsabbiltajiet tal-utenti u l-għarfien tul iċ-ċiklu tal-impjegat.

11.7.2 BAI05 – Bidla Organizzattiva Ġestita: Jintegra l-governanza tal-użu aċċettabbli fil-proċessi tal-bidla li jaffettwaw l-imġiba tal-utenti.

11.7.3 DSS05 – Servizzi ta' Sigurtà Ġestiti: Jappoġġa l-monitoraġġ tal-attivitajiet tal-utenti, twissijiet dwar l-imġiba u mekkaniżmi ta' rispons awtomatizzat.

11.7.4 MEA01 – Immonitorja, Evalwa u Ivvaluta l-Prestazzjoni u l-Konformità: Il-politika tiddefinixxi metriċi u mekkaniżmi biex tivverifika l-konformità tal-utenti mal-aspettattivi tal-imġiba.