					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P04					Titlu tad-dokument: **Politika dwar il-Kontroll tal-Aċċess**							
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 fejn applikabbli

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżoli 5.15, 5.17, 5.18	Ġestjoni tal-aċċess loġiku u fiżiku
ISO/IEC 27002:2022	Kontrolli 8.2, 8.3	Aċċess ibbażat fuq ir-rwoli u ġestjoni tal-identità
NIST SP 800-53 Rev. 5	AC-1 sa AC-20, IA-1 sa IA-8	Kontrolli tal-kontijiet u tal-aċċess, identità u awtentikazzjoni
GDPR tal-UE	Artikoli 5(1)(f), 32(1)(b); Premessa 39	Protezzjoni tad-data u minimizzazzjoni
Direttiva NIS2 tal-UE	Artikolu 21(2)(c–e)	Kontroll tal-aċċess, awtentikazzjoni tal-utenti u protezzjoni tal-assi
DORA tal-UE	Artikoli 6, 9(2)	Aċċess tal-utenti, ICT u kontrolli b’saħħithom għal partijiet terzi
COBIT 2019	APO07 Ġestjoni tar-Riżorsi Umani, BAI03, DSS01, DSS05, MEA03	Integrazzjoni inizjali, operazzjonijiet, monitoraġġ u konformità

1. Għan

1.1 Din il-politika tistabbilixxi prinċipji, responsabbiltajiet u rekwiżiti ta’ kontroll obbligatorji għall-ġestjoni tal-aċċess għal sistemi ta’ informazzjoni, applikazzjonijiet, faċilitajiet fiżiċi u assi tad-data fl-organizzazzjoni kollha.

1.2 Hija tiżgura li l-aċċess jingħata abbażi tal-ħtieġa tan-negozju, il-funzjoni tax-xogħol u l-livell ta’ riskju, filwaqt li jiġu applikati l-prinċipji tal-inqas privileġġ, tal-bżonn li tkun taf u tas-segregazzjoni tad-dmirijiet.

1.3 Il-politika tappoġġa l-implimentazzjoni tal-Klawżola 5.15 tal-ISO/IEC 27001:2022 u kontrolli relatati li jirregolaw l-aċċess loġiku u fiżiku, l-awtentikazzjoni tal-utenti u l-ġestjoni taċ-ċiklu tal-ħajja tal-aċċess.

1.4 Din il-politika ssaħħaħ il-protezzjoni ta’ riżorsi diġitali u fiżiċi kontra użu mhux awtorizzat, abbuż jew kompromess.

2. Kamp ta’ applikazzjoni

2.1 Din il-politika tapplika għall-utenti, is-sistemi u l-faċilitajiet kollha fi ħdan il-kamp ta’ applikazzjoni tal-ISMS, inklużi:

2.1.1 Impjegati, kuntratturi, forniturі u persunal temporanju

2.1.2 Infrastruttura fuq il-post, sistemi ospitati fil-cloud u ambjenti ibridi

2.1.3 L-assi korporattivi kollha — ħardwer, softwer, data u żoni siguri fiżiċi

2.1.4 Aċċess loġiku (eż. sistemi, netwerks, applikazzjonijiet, interfaċċi tal-ipprogrammar tal-applikazzjonijiet) u aċċess fiżiku (eż. bini, ċentri tad-data)

2.2 Hija tirregola l-aċċess matul iċ-ċiklu kollu tal-ħajja tal-identità u tal-interazzjoni mar-riżorsi, mill-integrazzjoni inizjali u l-għoti tal-aċċess sal-bidliet fir-rwoli u l-proċedura ta’ tluq.

2.3 Il-politika tkopri wkoll il-kuntesti ta’ Uża l-Apparat Tiegħek Stess (BYOD) u aċċess remot, u tiżgura li l-kontrolli jibqgħu konsistenti bejn il-lokalitajiet u l-mudelli ta’ sjieda tal-apparat.

3. Objettivi

3.1 Jiġu implimentati kontrolli tal-aċċess siguri u bbażati fuq ir-rwoli li jappoġġaw l-integrità operattiva u l-konformità regolatorja.

3.2 Jiġi żgurat li d-drittijiet ta’ aċċess jiġu approvati, immonitorjati u revokati fil-ħin xieraq.

3.3 Jiġi evitat aċċess mhux awtorizzat, eskalazzjoni ta’ privileġġi jew il-persistenza ta’ drittijiet ta’ aċċess skaduti.

3.4 Jiġu appoġġati l-prinċipji ta’ Zero Trust billi l-aċċess jiġi miċħud b’mod awtomatiku sakemm ma jkunx approvat u ġġustifikat b’mod espliċitu.

3.5 Tingħata assigurazzjoni lill-awdituri u lill-partijiet interessati permezz ta’ rieżamijiet perjodiċi tal-aċċess, awtomatizzati u bbażati fuq evidenza, kif ukoll permezz tal-infurzar tal-politika.

3.6 Il-kontroll tal-aċċess jiġi integrat fil-proċessi tan-negozju, fl-avvenimenti taċ-ċiklu tal-ħajja tar-riżorsi umani u fl-arkitetturi tekniċi.

4. Rwoli u responsabbiltajiet

4.1 Maniġment eżekuttiv

4.1.1 Japprova l-Politika dwar il-Kontroll tal-Aċċess u jiżgura baġit u persunal adegwati għall-applikazzjoni tagħha.

4.1.2 Jagħmel rieżami tar-riskji tal-kontroll tal-aċċess waqt ir-rieżami mill-maniġment u jalloka r-responsabbiltà fil-livell strateġiku.

4.2 Uffiċjal Ewlieni tas-Sigurtà tal-Informazzjoni / Maniġer tal-ISMS

4.2.1 Huwa responsabbli mill-qafas tal-kontroll tal-aċċess u jiżgura l-allinjament mal-ISO/IEC 27001 u ma’ standards relatati.

4.2.2 Jikkoordina l-applikazzjoni tal-politika, l-ittestjar tal-kontrolli u r-rappurtar tal-metriċi tal-kontroll tal-aċċess.

4.2.3 Jeżerċita sorveljanza fuq l-immudellar tal-aċċess ibbażat fuq ir-riskju u jimmonitorja lakuni sistemiċi fil-kontrolli.

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

9. Rekwiżiti ta’ rieżami u aġġornament

9.1 Attivaturi u frekwenza tar-rieżami

9.1.1 Din il-politika għandha tiġi rieżaminata:

9.1.1.1 Kull sena, jew

9.1.1.2 Wara bidla kbira fl-infrastruttura tal-IT, fir-rekwiżiti regolatorji jew fil-livell ta’ riskju

9.1.1.3 Wara inċidenti li jiżvelaw dgħufijiet fil-kontrolli tal-aċċess

9.1.1.4 Meta jseħħu bidliet sinifikanti fit-teknoloġiji tal-awtentikazzjoni jew fil-pjattaformi tal-identità

9.2 Awtorità u proċess tar-rieżami

9.2.1 L-Uffiċjal Ewlieni tas-Sigurtà tal-Informazzjoni jew il-mexxej tal-ISMS maħtur għandu jimmaniġġja ċ-ċiklu tar-rieżami, filwaqt li jinkorpora:

9.2.1.1 Sejbiet tal-awditjar intern

9.2.1.2 Riżultati u metriċi tar-rieżami tal-aċċess

9.2.1.3 Aġġornamenti legali u regolatorji

9.2.1.4 Bidliet fil-pjattaformi tat-teknoloġija

9.2.2 Ir-reviżjonijiet kollha għandhom jiġu approvati mill-maniġment eżekuttiv u kkomunikati lill-partijiet interessati kollha.

9.2.3 L-utenti affettwati jistgħu jkunu meħtieġa jerġgħu jagħtu rikonoxximent tal-politika wara aġġornamenti materjali.

9.3 Kontroll tal-verżjoni u dokumentazzjoni

9.3.1 Il-verżjoni ewlenija għandha tinħażen fir-repożitorju tad-dokumenti tal-ISMS bil-metadata li ġejja:

9.3.1.1 Numru tal-verżjoni u log tal-bidliet

9.3.1.2 Data tad-dħul fis-seħħ u data tar-rieżami li jmiss

9.3.1.3 Sid u awtorità ta' approvazzjoni

9.3.1.4 Reġistri ta' distribuzzjoni u ta' rikonoxximent

9.3.2 Verżjonijiet sostitwiti għandhom jiġu arkivjati u jibqgħu aċċessibbli għal minimu ta' 3 snin.

10. Politiki relatati u rabtiet

10.1 Din il-politika tiddependi funzjonalment fuq dawn li ġejjin u għandha tiġi interpretata flimkien magħhom:

10.1.1 P01 – Politika tas-Sigurtà tal-Informazzjoni: Tiddeskrivi l-impenn tal-organizzazzjoni għas-sigurtà u l-aspettattivi ta' livell għoli għall-kontroll tal-aċċess.

10.1.2 P03 – Politika tal-Użu Aċċettabbli (AUP): Tistabbilixxi kundizzjonijiet ta' mġiba għall-aċċess u r-responsabbiltà tal-utent għall-użu responsabbli tas-sistemi.

10.1.3 P05 – Politika tal-Ġestjoni tat-Tibdil: Tirregola kif bidliet fil-konfigurazzjonijiet tal-aċċess, fir-rwoli jew fl-istrutturi tal-gruppi għandhom jiġu implimentati u ttestjati b'mod sigur.

10.1.4 P07 – Politika ta' induzzjoni u terminazzjoni: Tiggwida l-għoti u r-revoka tad-drittijiet ta' aċċess skont l-avvenimenti taċ-ċiklu tal-ħajja tal-utent.

10.1.5 P11 – Politika dwar il-Ġestjoni tal-Kontijiet tal-Utenti u tal-Privileġġi: Toperazzjonalizza kontrolli fil-livell tal-kont u tikkomplementa din il-politika b'linji gwida tekniċi għall-applikazzjoni tal-aċċess.

10.2 Flimkien, dawn il-politiki jipprovdu qafas koerenti u infurzabbli ta' governanza tal-aċċess fl-unitajiet tan-negozju u fit-teknoloġiji kollha.

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001:2022:

11.1.1 Klawżola 5.15 – Politika dwar il-Kontroll tal-Aċċess: Din il-politika tissodisfa r-rekwiżit li jiġi kkontrollat l-aċċess għall-informazzjoni u għal assi assoċjati oħra, abbażi ta' rekwiżiti tan-negozju u tas-sigurtà tal-informazzjoni.

11.1.2 Klawżola 5.17 – Ġestjoni tal-Identità u Klawżola 5.18 – Informazzjoni ta' Awtentikazzjoni: Dawn jiġu operazzjonalizzati permezz tal-ġestjoni tal-identità, il-mekkaniżmi ta' awtentikazzjoni u l-assenjazzjonijiet ta' privileġġi.

11.1.3 Kontrolli tal-Anness A 8.2 (Politika dwar il-Kontroll tal-Aċċess) u 8.3 (Ġestjoni tal-Identità): Jipprovdu l-bażi għall-objettivi ta' kontroll ta' din il-politika, inklużi aċċess ibbażat fuq ir-rwoli, integrazzjoni taċ-ċiklu tal-ħajja tal-utent u protezzjoni tal-aċċess privileġġjat.

11.2 NIST SP 800-53 Rev. 5:

11.2.1 Familja AC (AC-1 sa AC-20): Din il-politika tappoġġa r-rekwiżiti tal-kontroll tal-aċċess tan-NIST kemm għal sistemi fiżiċi kif ukoll għal dawk loġiċi, inklużi definizzjoni tal-politika (AC-1), ġestjoni tal-kontijiet (AC-2) u segregazzjoni tad-dmirijiet (AC-5).

11.2.2 Familja IA (IA-1 sa IA-8): Tipprovdi gwida għall-awtentikazzjoni tal-identità, il-protezzjoni tal-kredenzjali u l-MFA.

11.2.3 AU-2, AU-12: Ir-rekwiżiti tal-illoggjar u tal-awditjar applikati taħt din il-politika jappoġġaw ir-responsabbiltà tal-utent u l-investigazzjoni tal-inċidenti.

11.2.4 PE-2 sa PE-6: Jindirizzaw restrizzjonijiet tal-aċċess fiżiku, li din il-politika tinforza parzjalment permezz ta' kontrolli tal-badges u permessi ta' aċċess għall-bini.

11.3 GDPR tal-UE (2016/679):

11.3.1 Artikolu 5(1)(f): Id-data personali għandha tkun protetta kontra aċċess mhux awtorizzat. Din il-politika tiżgura l-applikazzjoni teknika u proċedurali ta' dan il-prinċipju.

11.3.2 Artikolu 32(1)(b): Jeħtieġ l-implimentazzjoni ta' kontrolli tal-aċċess, psewdonimizzazzjoni u iċċifrar biex jiġi evitat ipproċessar mhux awtorizzat ta' data personali.

11.3.3 Premessa 39: Timponi l-minimizzazzjoni tal-aċċess għad-data personali, applikata hawnhekk permezz tal-prinċipju tal-inqas privileġġ u rekwiżiti ta' ġustifikazzjoni tal-aċċess.

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

11.4.1 Artikolu 21(2)(c–e): Din il-politika tippermetti miżuri tekniċi u organizzattivi għall-kontroll tal-aċċess, l-awtentikazzjoni tal-utenti u l-protezzjoni tal-assi fost entitajiet essenzjali u importanti.

11.5 DORA tal-UE (2022/2554):

11.5.1 Artikolu 6: Jeħtieġ politiki ta' ġestjoni tar-riskju tal-ICT li jinkludu b'mod espliċitu l-ġestjoni tal-aċċess tal-utenti u kontrolli taċ-ċiklu tal-ħajja tal-identità. Din il-politika tissodisfa dak ir-rekwiżit għas-setturi finanzjarji u tas-servizzi tal-ICT.

11.5.2 Artikolu 9(2): Din il-politika tappoġġa l-applikazzjoni ta' kontrolli b'saħħithom tal-aċċess bħala parti mill-ġestjoni tas-servizzi tal-ICT ta' partijiet terzi u bejn entitajiet tal-istess grupp.

11.6 COBIT 2019:

11.6.1 APO07 Ġestjoni tar-Riżorsi Umani – Managed Human Resources: Jinforza kontrolli ta' integrazzjoni inizjali u ta' proċedura ta' tluq biex jappoġġa l-governanza tal-aċċess.

11.6.2 BAI03 – Managed Solutions Identification and Build: Jintegra rekwiżiti tal-kontroll tal-aċċess fid-disinn tas-sistemi u fil-proċessi tat-tibdil.

11.6.3 DSS01 – Managed Operations u DSS05: Jirregolaw l-applikazzjoni ta' restrizzjonijiet ta' aċċess loġiku u l-monitoraġġ tal-ksur.

11.6.4 MEA03 – Monitor, Evaluate, and Assess Compliance: Jappoġġa mekkaniżmi ta' awditjar u assigurazzjoni għall-verifika tal-effettività tal-kontroll tal-aċċess.