					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P04S					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

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżola 5	
ISO/IEC 27002:2022	Kontrolli: 5.15, 5.16, 5.17	
NIST SP 800-53 Rev. 5	AC-1 sa AC-5	
GDPR tal-UE	Artikolu 32	
Direttiva NIS2 tal-UE	Artikolu 21(2)(b)	
DORA tal-UE	Artikolu 9	
COBIT 2019	APO07, DSS01	

1. Skop

1.1. Din il-politika tiddefinixxi kif l-organizzazzjoni timmaniġġja l-aċċess għas-sistemi, għad-data u għall-faċilitajiet sabiex tiżgura li persuni awtorizzati biss ikunu jistgħu jaċċessaw l-informazzjoni abbażi tal-ħtieġa tan-negozju.

1.2. Hija tistabbilixxi regoli ċari għall-għoti, il-modifika, il-monitoraġġ u r-revoka tal-aċċess sabiex tnaqqas ir-riskju ta’ aċċess mhux awtorizzat u tappoġġa l-konformità mal-liġijiet u mal-istandards applikabbli.

1.3. Din il-politika tapplika l-prinċipju tal-inqas privileġġ u teħtieġ li l-aċċess ikun limitat għall-minimu meħtieġ biex jitwettqu l-funzjonijiet tax-xogħol.

2. Kamp ta’ applikazzjoni

2.1. Din il-politika tapplika għall-individwi kollha li jużaw jew jimmaniġġjaw l-aċċess għas-sistemi tal-IT, għan-netwerks, għad-data jew għall-faċilitajiet tal-organizzazzjoni, inklużi:

2.1.1. Impjegati

2.1.2. Kuntratturi

2.1.3. Ħaddiema temporanji

2.1.4. Fornituri esterni ta’ servizzi tal-IT

2.2. Din tkopri aċċess għal:

2.2.1. Applikazzjonijiet tal-kumpanija, file shares u databases

2.2.2. Sistemi tal-email, VPN u aċċess remot

2.2.3. Servizzi cloud użati għal skopijiet kummerċjali

2.2.4. Aċċess fiżiku għal faċilitajiet siguri, bħal uffiċċji jew kmamar tas-servers

2.3. Din il-politika tapplika għall-apparati kollha, kemm jekk ipprovduti mill-kumpanija kif ukoll jekk approvati taħt il-BYOD, kif ukoll għall-pjattaformi u l-postijiet kollha.

3. Objettivi

3.1. Tiżgura li d-drittijiet ta’ aċċess jingħataw biss wara approvazzjoni formali abbażi tar-rwol u ġustifikazzjoni kummerċjali.

3.2. Tipprevjeni aċċess mhux awtorizzat jew eċċessiv għal data sensittiva, sistemi jew infrastruttura.

3.3. Tiddefinixxi proċeduri ċari għall-għoti, il-modifika u t-terminazzjoni tal-aċċess tal-utenti.

3.4. Teħtieġ rieżamijiet regolari tal-aċċess u logs awtomatizzati jew manwali biex tappoġġa l-awditi.

3.5. Tappoġġa l-implimentazzjoni teknika tar-restrizzjonijiet tal-aċċess permezz tal-konfigurazzjoni u l-monitoraġġ.

4. Rwoli u responsabbiltajiet

4.1. Maniġer Ġenerali (GM)

4.1.1. Japprova din il-politika u jiżgura li r-riżorsi jkunu disponibbli sabiex jiġu implimentati kontrolli effettivi tal-aċċess.

4.1.2. Japprova l-eċċezzjonijiet u jirrieżamina l-awditi annwali tal-aċċess.

4.2. Maniġer tal-IT / Fornitur ta' Appoġġ tal-IT

4.2.1. Jimmaniġġja l-għoti, il-modifika u t-terminazzjoni tal-kontijiet tal-utenti.

4.2.2. Iżomm Reġistru tal-Kontroll tal-Aċċess li jinkludi l-attività kollha rilevanti, inkluż il-ħolqien, il-bidliet u t-tneħħijiet.

4.2.3. Jimplimenta kontrolli tal-aċċess ibbażati fuq ir-rwoli (RBAC) u japplika awtentikazzjoni b'diversi fatturi b'saħħitha, fejn xieraq (eż. MFA).

4.2.4. Jirrevedi l-logs tal-aċċess għal attività suspettuża u jirrapporta kwalunkwe kwistjoni lill-Maniġer Ġenerali (GM).

[... 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. Rieżami annwali tal-politika

9.1.1. Il-Maniġer tal-IT għandu jirrieżamina din il-politika kull sena. Kwalunkwe bidla fil-kuntest legali, tekniku jew organizzattiv għandha twassal għal aġġornament immedjat.

9.2. Attivaturi tar-rieżami

9.2.1. Il-politika għandha wkoll tiġi rieżaminata jekk iseħħ xi wieħed minn dawn li ġejjin:

9.2.2. Bidliet sinifikanti fis-sistemi jew migrazzjoni ta' sistemi lejn ambjent cloud

9.2.3. Bidliet fir-rwoli jew fl-istruttura organizzattiva

9.2.4. Inċident ta' sigurtà tal-informazzjoni li jinvolvi aċċess mhux awtorizzat

9.2.5. Bidliet regolatorji, bħalma huma aġġornamenti tal-GDPR, tan-NIS2 jew tad-DORA

9.3. Dokumentazzjoni u komunikazzjoni tal-bidliet

9.3.1. Ir-reviżjonijiet għandhom jiġu rreġistrati bi storja tal-verżjonijiet, bl-approvazzjoni tal-Maniġer Ġenerali (GM), u kkomunikati lill-persunal kollu affettwat.

9.4. Aċċessibbiltà u taħriġ

9.4.1. Din il-politika għandha tkun disponibbli għall-persunal kollu, u għandu jingħata taħriġ rilevanti bħala parti mill-induzzjoni inizjali u fuq bażi annwali wara dan.

10. Politiki relatati u rabtiet

10.1. Din il-politika għandha tiġi applikata f'koordinazzjoni mal-politiki li ġejjin tal-SME sabiex tiġi żgurata l-applikazzjoni sħiħa ta' prattiki siguri ta' aċċess:

10.1.1. P3S – Politika tal-Użu Aċċettabbli (AUP): Tiżgura li l-utenti jifhmu l-imġiba aċċettabbli b'rabta mal-aċċess mogħti.

10.1.2. P5S – Politika tal-Ġestjoni tat-Tibdil: Tiżgura li d-drittijiet ta' aċċess ikunu allinjati ma' bidliet approvati fis-sistemi.

10.1.3. P7S – Politika ta' Induzzjoni u Terminazzjoni: Tiddefinixxi l-punti ta' attivazzjoni għall-għoti u r-revoka tal-aċċess.

10.1.4. P17S – Politika dwar il-Protezzjoni tad-Data u l-Privatezza: Tiżgura li l-kontrolli tal-aċċess ikunu allinjati mas-salvagwardji tad-data personali.

10.1.5. P30S – Politika ta’ Rispons għall-Inċidenti: Tiddefinixxi kif inċidenti relatati mal-aċċess, bħall-użu ħażin jew ksur, jiġu mmaniġġjati u investigati.

11. Standards u oqfsa ta’ referenza

11.1. ISO/IEC 27001

11.1.1. Klawżola 5.15 – Teħtieġ politiki u proċessi formalizzati għall-kontroll tal-aċċess.

11.2. ISO/IEC 27002

11.2.1. Kontrolli 5.15–5.17 – Jispeċifikaw gwida dettaljata dwar aċċess ibbażat fuq ir-rwoli, il-ġestjoni taċ-ċiklu tal-ħajja tal-utent u l-ġestjoni tal-aċċess privileġġjat.

11.3. NIST SP 800-53 Rev. 5

11.3.1. AC-1 sa AC-5 – Jeħtieġu politiki strutturati għall-ġestjoni tal-aċċess, inklużi l-awtorizzazzjoni tal-kontijiet, ir-rieżami u l-monitoraġġ.

11.4. GDPR tal-UE

11.4.1. Artikolu 32 – Jeħtieġ kontrolli tekniċi u organizzattivi, bħall-ġestjoni tal-aċċess, sabiex jiżguraw is-sigurtà u l-kunfidenzjalità tad-data.

11.5. Direttiva NIS2 tal-UE

11.5.1. Artikolu 21(2)(b) – Teħtieġ sistemi operattivi għall-kontroll tal-aċċess u l-ġestjoni tal-identità sabiex jiġi evitat aċċess mhux awtorizzat għas-sistemi.

11.6. DORA tal-UE

11.6.1. Artikolu 9 – Tenfasizza l-ġestjoni sigura tar-riskji tal-ICT, inkluż kontroll robust tal-aċċess għal entitajiet finanzjarji.

11.7. COBIT 2019

11.7.1. APO07 Ġestjoni tar-Riżorsi Umani – Titlob responsabbiltajiet ta’ aċċess definiti u applikati.

11.7.2. DSS01 – Ġestjoni tal-Operazzjonijiet: Jinkludi proċeduri għall-ġestjoni tal-aċċess loġiku u għaż-żamma ta’ ambjenti operattivi siguri.