					Daħħal hawn l-isem tal-entità ġuridika rreġistrata						
Numru tad-dokument: P11S					Titlu tad-dokument: **Politika dwar il-Ġestjoni tal-Kontijiet tal-Utenti u tal-Privileġġi**						
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**

Allinjament mal-istandards u mar-regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżoli 5.3, 8	Rwoli, responsabbiltajiet u ppjanar/kontroll operattiv għall-ġestjoni tal-aċċess tal-utenti
ISO/IEC 27002:2022	Kontroll 8	Kontrolli għall-assenjazzjoni, ir-rieżami u t-tneħħija ta' privileġġi elevati
NIST SP 800-53 Rev.5	AC-2, AC-5, AC-6	Ħolqien tal-kontijiet, monitoraġġ, inqas privileġġ u separazzjoni tad-dmirijiet
Direttiva NIS2 tal-UE	Artikolu 21(2)(d)	Ġestjoni tal-aċċess tal-utenti għal entitajiet essenzjali u importanti
DORA tal-UE	Artikolu 9(2)(b)	Kontroll tal-aċċess privileġġjat f'entitajiet finanzjarji
COBIT 2019	DSS05.03, DSS05.04	Għoti ta' aċċess, tneħħija tal-aċċess u rieżami perjodiku tal-aċċess tal-utenti
GDPR tal-UE	Artikolu 32	Kontrolli tal-aċċess xierqa għall-protezzjoni tad-data personali

1. Għan

1.1 Din il-politika tistabbilixxi regoli għall-ġestjoni tal-kontijiet tal-utenti u tad-drittijiet ta' aċċess b'mod sigur, konsistenti u traċċabbli. Hija tiżgura li utenti awtorizzati biss ikollhom aċċess għal sistemi u data, u li l-aċċess ikun xieraq għar-rwol u għar-responsabbiltajiet tagħhom.

1.2 Ġestjoni effettiva tal-kontijiet u tal-privileġġi hija essenzjali biex jiġi evitat aċċess mhux awtorizzat, jitnaqqas it-theddid intern u tiġi żgurata l-konformità ma' ISO/IEC 27001, il-GDPR u rekwiżiti regolatorji oħra.

1.3 Din il-politika tippermetti lill-organizzazzjoni tassenja sjieda u responsabbiltà għall-użu tal-kontijiet, timmonitorja u tawditja elevazzjonijiet ta' privileġġi, u tiddiżattiva jew tirrevoka l-aċċess b'mod sigur meta dan ma jibqax meħtieġ.

1.4 Hija tipproteġi wkoll l-operazzjonijiet tan-negozju minn żbalji operattivi jew użu ħażin ikkawżat minn aċċess eċċessiv jew mhux immonitorjat, u tgħin biex jitnaqqas ir-riskju ta' tnixxija aċċidentali ta' data, użu ħażin tal-privileġġi jew nuqqas ta' konformità regolatorja.

2. Kamp ta' applikazzjoni

2.1 Din il-politika tapplika għal:

2.1.1 L-impjegati kollha, l-interns, il-kuntratturi u l-utenti ta' partijiet terzi b'aċċess għas-sistemi tal-IT tal-organizzazzjoni

2.1.2 Is-sistemi, l-apparati, is-servizzi u l-pjattaformi kollha ġestiti mill-organizzazzjoni jew f'isimha, inklużi pjattaformi cloud, infrastruttura fuq il-post u għodod ta' partijiet terzi

2.2 Hija tkopri kull tip ta' kont ta' utent, inklużi:

2.2.1 Kontijiet ta' utenti nominati (eż. kontijiet tal-imejl, logins tas-sistema)

2.2.2 Kontijiet ta' amministratur u kontijiet fil-livell tas-sistema

2.2.3 Kredenzjali ta' aċċess temporanji, ta' mistednin jew ta' partijiet terzi

2.2.4 Kontijiet ta’ servizz użati minn applikazzjonijiet jew sistemi ta’ awtomazzjoni

2.3 Il-politika tapplika matul iċ-ċiklu kollu tal-ħajja tal-kontijiet — mill-ħolqien u l-approvazzjoni sal-modifika, il-monitoraġġ u d-diżattivazzjoni. Dan jinkludi l-għoti ta’ aċċess inizjali waqt l-onboarding, rieżamijiet tal-aċċess waqt bidliet fir-rwol, u r-revoka waqt il-Proċedura ta’ tluq.

3. Objettivi

3.1 Tassenja identitajiet uniċi u traċċabbli lill-utenti kollha tas-sistema, biex tiġi żgurata r-responsabbiltà u jiġi eliminat l-użu ta’ kredenzjali kondiviżi.

3.2 Timplimenta l-prinċipju tal-inqas privileġġ, billi tiżgura li l-utenti jingħataw biss il-livell minimu ta’ aċċess meħtieġ biex iwettqu dmirijiethom.

3.3 Tevita aċċess mhux awtorizzat għal sistemi jew data sensittiva permezz ta’ proċessi ta’ approvazzjoni u rieżami dokumentati b’mod ċar.

3.4 Tiżgura d-diżattivazzjoni fil-ħin tal-kontijiet tal-utenti meta dawn ma jibqgħux meħtieġa — pereżempju mat-terminazzjoni, mat-tlestija tal-kuntratt jew meta jinbidel ir-rwol.

3.5 Iżżomm ambjent sigur u lest għall-awditjar billi tiddokumenta l-bidliet kollha fil-kontijiet, l-approvazzjonijiet u r-rieżamijiet perjodiċi.

3.6 Tiżgura li l-elevazzjoni tal-privileġġi tkun ikkontrollata b’mod strett, approvata b’mod indipendenti u rreġistrata fil-logs, u li aċċess elevat jitneħħa minnufih meta ma jibqax meħtieġ.

4. Rwoli u responsabbiltajiet

4.1 Maniġer Ġenerali (GM)

4.1.1 Iġorr ir-responsabbiltà ġenerali għall-applikazzjoni ta’ din il-politika.

4.1.2 Jiżgura li l-prattiki tal-ġestjoni tal-kontijiet ikunu allinjati mar-rekwiżiti taċ-ċertifikazzjoni ISO/IEC 27001 u mal-obbligi legali rilevanti (eż. GDPR).

4.1.3 Għandu jiġi informat immedjatament b’kull aċċess mhux awtorizzat, inċident ta’ sigurtà jew ksur tal-politika relatat mal-kontijiet tal-utenti.

4.1.4 Jissorvelja r-rieżamijiet tal-politika, l-awditi u l-azzjonijiet ta’ implimentazzjoni.

4.2 Responsabbli tal-IT jew Fornitur Estern ta’ Servizzi tal-IT

4.2.1 Huwa responsabbli għall-implimentazzjoni teknika tal-kontrolli tal-kontijiet u tal-privileġġi fis-sistemi użati mill-organizzazzjoni.

4.2.2 Għandu jwettaq l-għoti ta’ aċċess, il-modifika u t-tneħħija tal-aċċess għall-kontijiet tal-utenti biss abbażi ta’ approvazzjonijiet dokumentati.

4.2.3 Għandu japplika rekwiżiti ta’ kumplessità tal-passwords, timeout tal-iskrin, awtentikazzjoni b’diversi fatturi fejn disponibbli, u logging tas-sistema.

4.2.4 Għandu jżomm reġistri siguri tal-approvazzjonijiet kollha tal-aċċess, tas-sjieda tal-kontijiet, tal-elevazzjonijiet tal-privileġġi u tar-revoki.

4.2.5 Għandu jimmonitorja għal kontijiet orfni jew kontijiet mhux awtorizzati u jirrapporta kull diskrepanza lill-GM.

[... 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 trid tiġi rieżaminata mill-inqas darba fis-sena mill-GM u mir-Responsabbli tal-IT biex tiġi żgurata l-konformità ma’:

9.1.1 Il-kontrolli u l-gwida attwali ta’ ISO/IEC 27001:2022

9.1.2 Aġġornamenti regolatorji (eż. GDPR, DORA, NIS2)

9.1.3 Bidliet fis-sistemi, fis-servizzi jew fl-istruttura tan-negozju

9.2 Ir-rieżamijiet iridu jsiru wkoll wara:

9.2.1 Inċidenti ta' sigurtà sinifikanti jew sejbiet tal-awditjar

9.2.2 Bidliet kbar fis-sistemi tal-IT jew fl-arkitettura tal-kontijiet

9.2.3 Introduzzjoni ta' pjattaformi ġodda li jeħtieġu integrazzjoni tal-kontroll tal-aċċess

9.3 Il-bidliet kollha jridu jiġu approvati mill-GM u kkomunikati b'mod ċar lill-persunal affettwat.

10. Politiki relatati u rabtiet

10.1 P2S – Politika dwar ir-Rwoli u r-Responsabbiltajiet tal-Governanza: Tistabbilixxi r-responsabbiltà u l-awtoritàgħat-teħid tad-deċiżjonijiet għall-approvazzjonijiet tal-aċċess u s-sorveljanza.

10.2 P4S – Politika dwar il-Kontroll tal-Aċċess: Tirregola l-applikazzjoni tal-kontroll tal-aċċess fuq livell ta' sistema u l-metodi ta' awtentikazzjoni.

10.3 P7S – Politika dwar l-induzzjoni u t-terminazzjoni: Tiżgura li l-ħolqien u t-tneħħija tal-kontijiet ikunu integrati fil-bidliet tal-persunal ġestiti mir-Riżorsi Umani.

10.4 P8S – Politika dwar l-Għarfien tas-Sigurtà tal-Informazzjoni u t-Taħriġ: Tħarreġ lill-utenti dwar prattiki siguri tal-kontijiet u l-aspettattivi relatati mal-użu.

10.5 P30S – Politika dwar ir-Rispons għall-Inċidenti: Tiddefinixxi l-azzjonijiet li għandhom jittieħdu jekk użu ħażin ta' kont iwassal għal ksur tas-sigurtà jew żvelar mhux awtorizzat.

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001

11.1.1 Klawżola 5.3: Teħtieġ li rwoli u responsabbiltajiet għas-sigurtà tal-informazzjoni jkunu assenjati b'mod ċar u applikati.

11.1.2 Klawżola 8.1: L-ippjanar u l-kontroll operattiv iridu jinkludu l-ġestjoni tal-aċċess tal-utenti.

11.2 ISO/IEC 27002

11.2.1 Kontroll 8.2: Jagħti dettalji dwar kontrolli tekniċi u proċedurali għall-assenjazzjoni, ir-rieżami u t-tneħħija ta' privileġġi elevati.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-2: Jeħtieġ il-ħolqien, il-monitoraġġ u r-revoka tal-kontijiet abbażi ta' rwoli u proċessi definiti.

11.3.2 AC-5: Jindirizza s-separazzjoni tad-dmirijiet biex jiġu evitati kunflitti jew abbuż ta' privileġġi.

11.3.3 AC-6: Jobbliga l-applikazzjoni tal-prinċipju tal-inqas privileġġ għad-drittijiet tal-aċċess kollha.

11.4 GDPR tal-UE

11.4.1 Artikolu 32: Jeħtieġ kontrolli tal-aċċess xierqa biex jipproteġu d-data personali minn aċċess jew tibdil mhux awtorizzat.

11.5 Direttiva NIS2 tal-UE

11.5.1 Artikolu 21(2)(d): Tobbliga l-ġestjoni tal-aċċess tal-utenti bħala parti mill-kontrolli ewlenin tas-sigurtà għal entitajiet essenzjali u importanti.

11.6 DORA tal-UE

11.6.1 Artikolu 9(2)(b): Jeħtieġ li entitajiet finanzjarji jimplimentaw kontrolli tal-aċċess li jirrestrinġu u jimmonitorjaw drittijiet privileġġjati.

11.7 COBIT 2019

11.7.1 DSS05.03: Jispeċifika l-għoti ta' aċċess u t-tneħħija tal-aċċess tal-utenti bħala parti mill-governanza tal-IT.

11.7.2 DSS05.04: Jitlob rieżami kontinwu u allinjament tal-aċċess tal-utenti mar-rwoli organizzattivi.