					Daħħal hawn l-isem tal-entità ġuridika rreġistrata						
Numru tad-dokument: P11					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 ma’ standards u regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżola 6.1.3, Klawżola 8	-
ISO/IEC 27002:2022	Kontrolli 5.15-5.18	-
NIST SP 800-53 Rev.5	AC-1, AC-2, AC-5, AC-6, IA-2 - IA-5, AU-2, AU-12	-
GDPR tal-UE	Artikoli 5(1)(f), 32; Premessa 39	-
Direttiva NIS2 tal-UE	Artikoli 21(2)(a, d), 21(3)	-
DORA tal-UE	Artikoli 5, 9	-
COBIT 2019	DSS01, DSS05, APO13	-

1. Għan

1. Din il-politika tistabbilixxi kontrolli obbligatorji għall-ġestjoni tal-kontijiet tal-utenti u tal-privileġġi fis-sistemi u s-servizzi kollha tal-informazzjoni. Hija tiżgura li l-aċċess għar-riżorsi tal-organizzazzjoni jingħata abbażi ta’ identità verifikata, ħtieġa marbuta mar-rwol, u l-prinċipji ta’ inqas privileġġ u separazzjoni tad-dmirijiet.

1.1 Hija tappoġġa l-impenn tal-organizzazzjoni lejn is-sigurtà tal-informazzjoni billi timplimenta proċessi strutturati u awditabbli għall-proviżjonament tal-aċċess, l-assenjazzjoni tal-privileġġi, il-monitoraġġ tal-użu, u r-revoka tal-aċċess.

1.2 Din il-politika hija kritika biex jitnaqqas ir-riskju ta’ aċċess mhux awtorizzat, użu ħażin tal-privileġġi, theddid intern, u nuqqas ta’ konformità ma’ oqfsa regolatorji applikabbli.

2. Kamp ta’ applikazzjoni

2.1 Din il-politika tapplika għall-impjegati kollha, kuntratturi, fornituri terzi ta’ servizzi, konsulenti, u individwi oħra li jingħataw aċċess għar-riżorsi tal-IT, l-applikazzjonijiet, jew id-data tal-organizzazzjoni.

2.2 Tirregola s-sistemi u l-ambjenti kollha fejn jiġu applikati mekkaniżmi ta’ awtentikazzjoni tal-utent u kontroll tal-aċċess, inkluż iżda mhux limitat għal:

2.2.1 Applikazzjonijiet korporattivi u bażijiet tad-data

2.2.2 Pjattaformi cloud u ambjenti SaaS

2.2.3 Sistemi operattivi u consoles amministrattivi

2.2.4 Għodod ta’ aċċess remot u VPNs

2.2.5 Sistemi ta’ ġestjoni tal-identità u tal-aċċess (IAM)

2.3 Il-politika tkopri kemm kontijiet standard tal-utenti kif ukoll kontijiet privileġġjati, u tinkludi kontrolli fuq:

2.3.1 Il-ħolqien, il-modifika u d-diżattivazzjoni tal-kontijiet

2.3.2 L-eskalazzjoni tal-privileġġi u d-delega

2.3.3 Il-kontroll u l-monitoraġġ tas-sessjonijiet

2.3.4 Metodi ta’ awtentikazzjoni u ġestjoni tal-kredenzjali

3. Objettivi

3.1 Jiġi żgurat li l-kontijiet kollha tal-utenti jkunu identifikabbli b’mod uniku, awtorizzati kif xieraq, u assenjati biss wara verifika formali tal-ħtieġa.

3.2 Jiġu implimentati l-prinċipji ta’ inqas privileġġ u jiġi evitat aċċess mhux meħtieġ jew eċċessiv billi jiġu applikati kontrolli stretti fuq l-għoti u l-użu ta’ kontijiet privileġġjati.

3.3 Ikunu meħtieġa aġġornamenti f'waqthom għall-istatus tal-kontijiet skont bidliet fl-impjieg jew fir-rwol, inkluża d-diżattivazzjoni immedjata mat-terminazzjoni.

3.4 Isir possibbli s-sejbien proattiv u r-rimedjazzjoni ta' kontijiet inattivi, użati ħażin, jew mhux awtorizzati permezz ta' logging, rieżamijiet, u awtomazzjoni.

3.5 Jinżamm allinjament ma' ISO/IEC 27001:2022 u standards assoċjati, u jiġu ssodisfati obbligi skont oqfsa legali u regolatorji rilevanti bħall-GDPR, in-NIS2, id-DORA, u COBIT 2019.

4. Rwoli u responsabbiltajiet

4.1 Uffiċjal Kap tas-Sigurtà tal-Informazzjoni (CISO)

4.1.1 Huwa s-sid ta' din il-politika u jiżgura l-applikazzjoni tagħha fl-organizzazzjoni kollha.

4.1.2 Jirrieżamina u japprova kull eċċezzjoni formali jew każ ta' aċċess ta' emerġenza.

4.1.3 Jirrapporta s-sejbiet tal-awditjar relatati mal-kontijiet u jeskala r-riskji lill-Maniġment Eżekuttiv.

4.2 Maniġer tal-Kontroll tal-Aċċess / Amministratur tal-IT

4.2.1 Iżomm u jopera l-kontrolli tekniċi għall-ġestjoni taċ-ċiklu tal-ħajja tal-kontijiet tal-utenti.

4.2.2 Iwettaq il-proviżjonament tal-aċċess, ir-revoka tal-aċċess, u azzjonijiet ta' ġestjoni tal-privileġġi abbażi ta' talba approvata.

4.2.3 Iżomm reġistru awtorevoli tal-kontijiet kollha tal-utenti, l-istatus tagħhom, u l-livell tal-privileġġ tagħhom.

4.2.4 Jappoġġa l-awditi u r-rieżamijiet tal-konformità permezz ta' logs u rapporti tal-attività.

[... 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 rieżaminata mill-inqas kull sena jew meta jkun hemm bidliet sinifikanti fi:

9.1.1 L-istruttura organizzattiva jew il-proċessi tan-negozju

9.1.2 Is-sistemi tal-IT, il-pjattaformi tal-identità, jew il-metodi ta' aċċess

9.1.3 Rekwiżiti regolatorji jew kuntrattwali relatati mal-ġestjoni tal-identità u tal-aċċess

9.2 L-Uffiċjal Kap tas-Sigurtà tal-Informazzjoni (CISO), flimkien mal-Maniġer tal-Kontroll tal-Aċċess, għandu jkun responsabbli biex jibda l-proċess tar-rieżami u jikkoordina l-feedback tal-partijiet interessati.

9.3 Rieżamijiet interim jistgħu jiġu attivati minn:

9.3.1 Inċidenti tas-sigurtà relatati ma' użu ħażin tal-kontijiet

9.3.2 Sejbiet tal-awditjar li jenfasizzaw nuqqasijiet fil-ġestjoni taċ-ċiklu tal-ħajja tal-kontijiet

9.3.3 Implimentazzjoni ta' għodod ġodda ta' ġestjoni tal-identità jew ta' ġestjoni tal-aċċess privileġġjat (PAM)

9.4 L-aġġornamenti għal din il-politika għandhom ikunu:

9.4.1 Taħt kontroll tal-verżjoni u rreġistrati fir-repożitorju tad-dokumenti tal-ISMS

9.4.2 Ikkomunikati lill-partijiet interessati rilevanti kollha, inklużi Kapijiet tad-Dipartimenti, Operazzjonijiet tal-IT, u HR

9.4.3 Appoġġati b'materjal ta' taħriġ aġġornat u gwidi proċedurali

9.5 Il-bidliet kollha għandhom jiġu approvati mill-Maniġment Eżekuttiv jew mill-Kumitat ta' Tmexxija tas-Sigurtà tal-Informazzjoni u jiġu rreġistrati fil-logs għal finijiet ta' awditjar.

10. Politiki relatati u rabtiet

10.1 Din il-politika hija marbuta operattivament ma' u appoġġata mill-politiki relatati li ġejjin fi ħdan is-suite tal-ISMS:

10.1.1 P4 Politika dwar il-Kontroll tal-Aċċess: Tistabbilixxi l-prinċipji u l-mekkaniżmi ġenerali tal-kontroll tal-aċċess, inklużi kontrolli bbażati fuq regoli u kontrolli bbażati fuq ir-rwoli.

10.1.2 P7 Politika dwar l-Onboarding u l-Offboarding: Tipprovdi passi proċedurali għall-bidu u t-terminazzjoni tal-aċċess tal-utent allinjati mal-azzjonijiet tar-Riżorsi Umani.

10.1.3 P8 Politika dwar l-Għarfien tas-Sigurtà tal-Informazzjoni u t-Taħriġ: Issaħħaħ ir-responsabbiltajiet tal-utenti għas-sigurtà tal-kontijiet u l-protezzjoni tal-kredenzjali.

10.1.4 P13 Politika dwar il-Klassifikazzjoni u t-Tikkettar tad-Data: Tiggwida l-livelli ta' aċċess abbażi tal-klassifikazzjoni tad-data, biex tiżgura li l-limiti tal-privileġġi jkunu allinjati mal-livelli tas-sensittività.

10.1.5 P22 Politika dwar il-Logging u l-Monitoraġġ: Tiżgura li jinġabru traċċi ta' awditjar għall-attivitajiet kollha relatati mal-kontijiet u li dawn jiġu rieżaminati biex jinstabu anomaliji jew użu mhux awtorizzat.

10.1.6 P30 Politika dwar ir-Rispons għall-Inċidenti: Tirregola l-eskalazzjoni, il-konteniment, u l-azzjonijiet ta' wara l-inċident f'każijiet ta' użu ħażin tal-privileġġi jew attività mhux awtorizzata tal-kontijiet.

10.2 Kull waħda minn dawn il-politiki taħdem flimkien biex tapplika qafas koerenti ta' ġestjoni tal-identità u tal-aċċess ibbażat fuq ir-riskju fl-organizzazzjoni kollha.

11. Standards u oqfsa ta' referenza

11.1 Din il-politika hija allinjata ma' standards taċ-ċibersigurtà u oqfsa regolatorji rikonoxxuti globalment li jeħtieġu ġestjoni sigura tal-identità, tal-aċċess, u tal-privileġġi bħala komponent ewlieni tas-sigurtà tal-informazzjoni tal-organizzazzjoni.

11.2 ISO/IEC 27001:

11.2.1 Klawżola 6.1.3 teħtieġ li l-organizzazzjonijiet jidentifikaw, jevalwaw, u jittrattaw ir-riskji tas-sigurtà tal-informazzjoni, u b'hekk il-ġestjoni tal-aċċess u tal-privileġġi ssir kontroll formali bbażat fuq ir-riskju integrat fil-proċess tal-ippjanar tal-ISMS.

11.2.2 Klawżola 8.1 - Ippjanar u Kontroll Operattiv: Issaħħaħ l-implimentazzjoni ta' salvagwardji tekniċi u proċedurali li jirregolaw l-aċċess tal-utenti u l-aċċess privileġġjat.

11.3 ISO/IEC 27002:2022 - Kontrolli 5.15 sa 5.18:

11.3.1 Kontroll 5.15 - Ġestjoni tal-aċċess tal-utenti: Jappoġġa proċessi formali għall-proviżjonament tal-aċċess, l-awtorizzazzjoni tal-aċċess, u r-rieżami perjodiku tad-drittijiet tal-aċċess.

11.3.2 Kontroll 5.16 - Ġestjoni tal-identità: Jistabbilixxi l-uniċità tal-identità, kontrolli taċ-ċiklu tal-ħajja, u l-applikazzjoni ta' awtentikazzjoni sigura.

11.3.3 Kontroll 5.17 - Informazzjoni ta' awtentikazzjoni: Jiżgura li l-allokazzjoni u l-użu tal-informazzjoni ta' awtentikazzjoni jkunu kkontrollati b'mod strett, traċċabbli, u allinjati mal-prinċipju ta' inqas privileġġ tul iċ-ċiklu tal-ħajja tal-kont tal-utent.

11.3.4 Kontroll 5.18 - Drittijiet ta' aċċess: Huwa indirizzat b'mod sħiħ permezz ta' assenjazzjoni tal-privileġġi bbażata fuq ir-rwoli, awditjar, u rekwiżiti ta' approvazzjoni għal aċċess elevat.

11.4 Dawn il-kontrolli jiggwidaw implimentazzjoni strutturata tar-reġistrazzjoni u t-tneħħija tar-reġistrazzjoni tal-kontijiet, is-separazzjoni tal-privileġġi, u l-użu ta' informazzjoni ta' awtentikazzjoni. Il-politika tapplika governanza taċ-ċiklu tal-ħajja tal-identità, aċċess just-in-time, u monitoraġġ ta' sessjonijiet elevati biex tipprevjeni użu mhux awtorizzat tas-sistema.

11.5 NIST SP 800-53 Rev.5:

11.5.1 AC-1 (Politika dwar il-Kontroll tal-Aċċess) u AC-2 (Ġestjoni tal-Kontijiet): Riflessi permezz tal-obbligi tal-politika għall-approvazzjonijiet tal-aċċess, l-immappjar tar-rwoli, u l-awditjar tal-kontijiet tal-utenti.

11.5.2 AC-5 (Separazzjoni tad-Dmirijiet) u AC-6 (Inqas Privileġġ): Issodisfati permezz ta' restrizzjoni tal-privileġġi, allinjament mar-rwol tax-xogħol, u approvazzjoni doppja għal kompiti ta' riskju għoli.

11.5.3 IA-2 sa IA-5 (Identifikazzjoni u Awtentikazzjoni): Applikati permezz ta' mekkaniżmi ta' awtentikazzjoni b'saħħithom, regoli taċ-ċiklu tal-ħajja tal-kredenzjali, u rekwiżiti tal-MFA.

11.5.4 AU-2, AU-12 (Reġistrazzjoni tal-awditjar u analiżi): Indirizzati permezz tar-reġistrazzjoni tas-sessjonijiet u l-monitoraġġ tal-attività privileġġjata f'ambjenti sensittivi.

11.6 GDPR tal-UE (2016/679):

11.6.1 Artikolu 32 - Sigurtà tal-ipproċessar: Jeħtieġ kontrolli tal-aċċess u mekkaniżmi ta' verifika tal-identità biex jipproteġu d-data personali. Dan jiġi ssodisfat billi jsiru obbligatorji approvazzjonijiet tal-kontijiet, rieżamijiet tal-privileġġi, u salvagwardji b'saħħithom tal-awtentikazzjoni.

11.6.2 Artikolu 5(1)(f) - Integrità u Kunfidenzjalità: Jiżgura li d-data personali tiġi aċċessata biss minn utenti awtorizzati b'rwoli leġittimi, imsaħħa permezz tal-applikazzjoni tal-ġestjoni tal-kontijiet.

11.6.3 Premessa 39: Titlob limitazzjoni ċara tal-aċċess u responsabbiltà; din il-politika tappoġġa traċċabbiltà sħiħa tal-identitajiet tal-utenti u tal-assenjazzjonijiet tal-privileġġi.

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

11.7.1 Artikolu 21(2)(a, d): Jeħtieġ li l-entitajiet japplikaw politiki ta' ġestjoni tal-aċċess u mmaniġġjar sigur tal-kredenzjali u tas-sessjonijiet privileġġjati, appoġġati permezz tal-kontrolli ta' proviżjonament tal-aċċess, monitoraġġ, u eċċezzjonijiet f'din il-politika.

11.7.2 Artikolu 21(3): Jippromwovi dixxiplina tal-aċċess u assigurazzjoni b'saħħitha tal-identità f'setturi kritiċi, issodisfata permezz tal-użu ta' identifikaturi uniċi, RBAC, u aċċess elevat limitat fiż-żmien.

11.8 DORA tal-UE (2022/2554):

11.8.1 Artikolu 5 - Governanza u Kontroll tal-ICT: Jobbliga proċessi formalizzati għall-ġestjoni tal-utenti tal-ICT, koperti permezz ta' proviżjonament tal-aċċess, diżattivazzjoni, u ġestjoni tal-eċċezzjonijiet dokumentati.

11.8.2 Artikolu 9 - Ġestjoni tar-riskju tal-ICT: Jagħti direzzjoni lill-organizzazzjonijiet biex jipproteġu s-sistemi permezz ta' restrizzjonijiet tal-aċċess u monitoraġġ, indirizzati permezz tal-MFA, logging tal-aċċess privileġġjat, u rieżamijiet ċentralizzati.

11.9 COBIT 2019:

11.9.1 DSS01 - Operazzjonijiet Immaniġġjati: Jippromwovi applikazzjoni ta' kontrolli operattivi standardizzati, inkluża l-ġestjoni taċ-ċiklu tal-ħajja tal-kontijiet tal-utenti u d-dokumentazzjoni tal-aċċess.

11.9.2 DSS05 - Servizzi ta' Sigurtà Immaniġġjati: Jirrifletti amministrazzjoni sigura tal-privileġġi tal-utent u tas-sistema, u jappoġġa l-mitigazzjoni tar-riskju permezz ta' inqas privileġġ u verifika tat-traċċa tal-awditjar.

11.9.3 APO13 - Sigurtà Immaniġġjata: Teħtieġ governanza tal-aċċess fuq assi diġitali, issodisfata permezz ta' prattiki formalizzati ta' awtorizzazzjoni tal-kontijiet u tar-rwoli b'obbligi ta' rieżami perjodiku.