

				Dañhal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P05S				Titlu tad-dokument: Politika tal-Ġestjoni tat-Tibdil							
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	Ivvedut minn	Sid tal-proċess

Approvazzjonijiet			
Isem	Pożizzjoni	Data	Firma

Avviż legali (drittijiet tal-awtur u restrizzjonijiet fuq l-użu)

(C) 2025 Clarysec LLC. All rights reserved.

Dan id-dokument huwa proprjetà intellettuali ta' Clarysec LLC. L-ebda parti minn dan id-dokument ma tista' tiġi kkupjata, użata mill-ġdid, distribwita jew modifikata għal skopijiet kummerċjali jew ta' implimentazzjoni mingħajr awtorizzazzjoni espliċita minn qabel bil-miktub.

L-użu mhux awtorizzat huwa strettament ipprojbit u jista' jwassal għal azzjoni legali.

Għal-liċenzjar, ikkuntattja: info@clarysec.com

Allinjata mal-istandards u r-regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżola 6.1, 8	
ISO/IEC 27002:2022	Kontroll 8	
NIST SP 800-53 Rev.5	CM-2 sa CM-5, CM-11	
Direttiva NIS2 tal-UE	Artikolu 21(2)(b)	
DORA tal-UE	Artikoli 6(9), 8(4)(b)	
COBIT 2019	BAI06, DSS	

1. Skop

1.1 Din il-politika tiżgura li t-tibdil kollu fis-sistemi tal-IT, fl-issettjar tal-konfigurazzjoni, fl-applikazzjonijiet tan-negozju jew fis-servizzi cloud ikun ippjanat, soġġett għal valutazzjoni tar-riskju, ittestjat u approvat qabel l-implimentazzjoni.

1.2 L-għan huwa li jitnaqqsu t-tfixkil operattiv, ir-riskji għas-sigurtà u l-interruzzjonijiet tas-servizz billi jiġi stabbilit proċess semplifikat iżda infurzabbli li japplika wkoll għal negozji żgħar b'riżorsi limitati.

1.3 Din il-politika tappoġġa ċ-ċertifikazzjoni ISO/IEC 27001:2022 billi tifformalizza kif it-tibdil tekniku u operattiv jiġi ġestit u dokumentat.

2. Kamp ta' applikazzjoni

2.1 Din il-politika tapplika għal:

2.1.1 Impjegati u manijers tad-dipartimenti li jipproponu jew jimplimentaw tibdil

2.1.2 Fornituri esterni ta' servizzi tal-IT li jimmaniġġjaw sistemi jew software

2.1.3 Il-Maniġer Ġenerali (GM), li għandu r-responsabbiltà ġenerali għall-approvazzjonijiet tat-tibdil

2.2 Din tkopri tibdil fi:

2.2.1 Software (aġġornamenti, patches, applikazzjonijiet ġodda)

2.2.2 Hardwer (sostituzzjonijiet, aġġornamenti)

2.2.3 Konfigurazzjonijiet tan-network u tal-firewall

2.2.4 Servizzi cloud, permessi ta' aċċess tal-utenti, jew integrazzjonijiet mal-fornituri

2.2.5 Bidliet fi proċessi tan-negozju kritiċi li jinvolvu sistemi tal-informazzjoni

2.3 Kemm it-tibdil ippjanat kif ukoll il-bidliet ta' emerġenza jaqgħu fil-kamp ta' applikazzjoni ta' din il-politika.

3. Objettivi

3.1 Jiġi żgurat li t-tibdil kollu fis-sistemi tal-IT u tan-negozju jkun awtorizzat, dokumentat u riversibbli jekk jinqalgħu problemi.

3.2 Jiġi evitat waqfien mhux ippjanat, telf ta' data jew inċident tas-sigurtà tal-informazzjoni kkawżat minn tibdil mhux ikkontrollat.

3.3 Jiġu ddefiniti proċeduri sempliċi u ripetibbli għas-sottomissjoni ta' talba għal tibdil, l-approvazzjoni, l-ittestjar u t-treġġiġh lura.

3.4 Jinżamm reġistru tat-tibdil li jkun awditjabbli u li jappoġġa r-responsabbiltà operattiva u l-konformità regolatorja.

3.5 Tiġi ffaċilitata t-teħid ta' deċiżjonijiet ibbażat fuq ir-riskju għal tibdil sinifikanti jew sensitiv.

4. Rwoli u responsabbiltajiet

4.1 Maniġer Ġenerali (GM)

4.1.1 Għandu r-responsabbiltà aħharija għat-tibdil ewlieni kollu.

4.1.2 Jirrieżamina u japprova tibdil mhux ta' rutina, kritiku jew ta' riskju għoli.

4.1.3 Jirrieżamina r-reġistru tat-tibdil kull tliet xhur jew wara inċidenti kbar.

4.2 Appoġġ tal-IT jew fornitur esternalizzat ta' appoġġ tal-IT

4.2.1 Jimplimenta t-tibdil, inklużi aġġornamenti tal-konfigurazzjoni, l-applikazzjoni ta' patches u migrazzjonijiet tas-sistemi.

4.2.2 Iżomm reġistru bażiku tat-tibdil li jirreġistra d-dati, it-tipi ta' tibdil, ir-riżultati u l-approvaturi.

4.2.3 Jittestja t-tibdil qabel l-implimentazzjoni u japplika l-passi tat-treġġiġh lura kif meħtieġ.

4.2.4 Javża lill-utenti affettwati qabel u wara tibdil ewlieni.

[... 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

9.1.1 Din il-politika għandha tiġi rieżaminata kull sena mill-Maniġer Ġenerali (GM) jew minn kuntatt tal-IT maħtur biex jiġi żgurat l-allinjament mas-sistemi attwali, il-flussi tax-xogħol u r-rekwiżiti regolatorji.

9.2 Rieżamijiet interim

9.2.1 Ir-rieżamijiet għandhom jiġu attivati wkoll minn:

9.2.1.1 Inċidenti tas-sigurtà kkawżati minn ġestjoni hażina tat-tibdil

9.2.1.2 Introduzzjoni ta' sistemi ġodda tal-IT

9.2.1.3 Bidliet fi standards rilevanti bħall-ISO, NIS2 jew DORA

9.3 Dokumentazzjoni tal-aġġornamenti

9.3.1 It-tibdil f'din il-politika għandu jkun soġġett għal kontroll tal-verżjoni u approvat mill-Maniġer Ġenerali (GM). Kull verżjoni għandha tirreġistra d-data, sommarju tat-tibdil u l-approvatur.

9.4 Komunikazzjoni tal-politika

9.4.1 Kwalunkwe aġġornament għandu jiġi kkomunikat lill-impjegati affettwati kollha u lill-fornituri esterni. Id-dokumentazzjoni għandha tiġi aġġornata fil-postijiet kollha ta' referenza (eż. portal tal-persunal, drives kondiviżi).

10. Politiki relatati u rabtiet

10.1 Din il-politika hija marbuta mill-qrib mal-politiki SME li ġejjin:

10.1.1 P2S – Politika dwar ir-Rwoli u r-Responsabbiltajiet ta' Governanza: Tiddefinixxi l-awtorità ta' approvazzjoni għat-tibdil.

10.1.2 P4S – Politika dwar il-Kontroll tal-Aċċess: Tiżgura li l-modifiki tal-aċċess li jirriżultaw mit-tibdil ikunu dokumentati u implimentati b'mod korrett.

10.1.3 P7S – Politika ta' induzzjoni u terminazzjoni: Tikkoordina t-tibdil relatat mat-tranzizzjonijiet tar-rwoli u l-għoti ta' drittijiet ta' aċċess.

10.1.4 P15S – Politika dwar il-Backup u r-Restawr: Tiżgura li l-passi ta' treġġiġh lura u rkupru jkunu jstgħu jiġu eżegwiti jekk tibdil ifalli.

10.1.5 P30S – Politika ta' Rispons għall-Inċidenti: Tirregola kif tibdil li jfalli jew mhux awtorizzat jiġi ttrattat bħala inċidenti tas-sigurtà.

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001

11.1.1 Klawżola 6.1 – L-ippjanar ibbażat fuq ir-riskju għandu jinkludi attivitajiet ta' tibdil.

11.1.2 Klawżola 8.1 – Il-kontrolli operattivi għandhom jiġu applikati b'mod konsistenti għal attivitajiet relatati mat-tibdil biex tiġi żgurata l-integrità tas-servizz.

11.2 ISO/IEC 27002

11.2.1 Kontroll 8.32 – Jipprovi gwida għall-proċessi ta' ġestjoni tat-tibdil sikuri, inklużi d-dokumentazzjoni, l-ittestjar u l-approvazzjoni.

11.3 NIST SP 800-53 Rev.5

11.3.1 CM-2 – Konfigurazzjoni bażi għas-sistemi qabel it-tibdil.

11.3.2 CM-3 – Kontroll tat-tibdil fil-konfigurazzjoni.

11.3.3 CM-4 – Analizi tal-impatt fuq is-sigurtà.

11.3.4 CM-5 – Approvazzjoni u dokumentazzjoni tat-tibdil.

11.3.5 CM-11 – Awditjar u monitoraġġ tat-tibdil.

11.4 Direttiva NIS2 tal-UE

11.4.1 Artikolu 21(2)(b) – Jeħtieġ proċeduri formali għal miżuri tekniċi u organizzattivi tas-sigurtà, inkluża l-ġestjoni tat-tibdil.

11.5 DORA tal-UE

11.5.1 Artikoli 6(9) u 8(4)(b) – Jeħtieġu li entitajiet finanzjarji jżommu ġestjoni tat-tibdil u tal-konfigurazzjoni għas-sistemi tal-ICT.

11.6 COBIT 2019

11.6.1 BAI06 – Immaniġġja t-Tibdil: Jenfasizza l-ippjanar, il-valutazzjoni tar-riskju u l-kapaċitajiet ta' treġġiġh lura.

11.6.2 DSS01 – Immaniġġja l-Operazzjonijiet: Jiżgura l-integrità operattiva waqt tranżizzjonijiet u tibdil tekniku.