

				Dañhal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P10				Titlu tad-dokument: <b>Politika tal-Mejda Nadifa u l-Iskrin Nadif</b>							
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 ipprobit u jista' jwassal għal azzjoni legali.

Għal-liċenzjar, ikkuntattja: [info@clarysec.com](mailto:info@clarysec.com)

## Allinjament ma' standards u regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżola 6.1.3, Klawżola 8	Pjan ta' Trattament tar-Riskju, ippjanar operattiv, u kontrolli għal spazji tax-xogħol siguri
ISO/IEC 27002:2022	Kontroll 7	Kontrolli tal-imġiba u ambjentali għall-protezzjoni ta' informazzjoni fiżika li titħalla mingħajr superviżjoni
NIST SP 800-53 Rev.5	PE-2, PS-7, MP-6, AC-11, CM-6, IA-5	Aċċess fiżiku, sigurtà tal-kuntratturi, rimi tal-midja, illokkjar tas-sessjoni, u kontrolli tal-konfigurazzjoni u tal-awtentikazzjoni
GDPR tal-UE	Artikoli 5(1)(f), 32; Premessa 39	Integrità tad-data, kunfidenzjalità, u salvagwardji fiżiċi għad-data
Direttiva NIS2 tal-UE	Artikoli 21(2)(d), 21(3)	Politiki għas-sigurtà fiżika, l-imġiba tal-utenti, u l-prevenzjoni tat-tnixxija tad-data
DORA tal-UE	Artikoli 5, 8, 9	governanza interna, ICT, u ġestjoni tal-inċidenti li tinvolvi s-sigurtà fiżika
COBIT 2019	DSS01, DSS05, MEA	Operazzjonijiet immaniġġjati, servizzi ta' sigurtà, u monitoraġġ tal-konformità

### 1. Għan

1.1 Din il-politika tistabbilixxi kontrolli obligatorji biex tiproteġi informazzjoni sensitiva billi tirrikjedi l-immaniġġjar sigur ta' dokumenti fiżiċi, stazzjonijiet tax-xogħol, skrins u midja rimovibbli kemm f'ambjenti tal-uffiċċju kif ukoll fi spazji tax-xogħol kondiviżi.

1.2 Din tappoġġa l-Kontroll 7.7 tal-Anness A ta' ISO/IEC 27001 billi timponi prattiki ta' mġiba u tekniċi li jnaqqsu r-riskju ta' żvelar mhux awtorizzat, serq jew telf ta' data minħabba informazzjoni viżibbli jew li titħalla mingħajr attenzjoni.

1.3 Din il-politika ssaħħaħ is-sigurtà fiżika u s-sigurtà tal-informazzjoni fl-operazzjonijiet ta' kuljum u tappoġġa l-konformità ma' obbligi legali, kuntrattwali u regolatorji applikabbli.

### 2. Kamp ta' applikazzjoni

**2.1 Din il-politika tapplika għall-persunal kollu li jopera fi spazji tax-xogħol fiżiċi jew li jkollu aċċess għalihom, inkluż:**

2.1.1 Impjegati permanenti u temporanji

2.1.2 Kuntratturi, konsulenti, fornituri, u apprendisti

2.1.3 Fornituri ta' servizzi ta' partijiet terzi u viżitaturi fuq il-post b'aċċess għal informazzjoni sensitiva

**2.2 Ir-rekwiżiti japplikaw fi:**

2.2.1 Uffiċċji individwali, kubikoli, u spazji tax-xogħol open-plan

2.2.2 Kmamar tal-laqgħat u żoni kondiviżi ta' kollaborazzjoni

2.2.3 Żoni tal-printers, desks tar-riċeviment, u kmamar tal-ikkupjar

2.2.4 Żoni fejn jintużaw stazzjonijiet tax-xogħol remoti jew kjosks kondiviżi

2.3 Din il-politika tapplika wkoll għal ambjenti ta' xogħol temporanji jew ibridi (eż. hot-desking) u għal ambjenti aċċessibbli pubblikament fejn jeżisti riskju ta' osservazzjoni minn fuq l-ispalla jew ta' data li titfälla mingħajr attenzjoni.

### 3. Objettivi

3.1 Li jiġi evitat aċċess mhux awtorizzat għal informazzjoni kunfidenzjali, sensitiva jew regolata li titfälla esposta f'forma fiżika jew diġitali.

3.2 Li tiġi promossa pożizzjoni ta' sigurtà standardizzata fl-ambjenti kollha tax-xogħol permezz ta' salvagwardji fiżiċi, konfigurazzjoni tal-istazzjonijiet tax-xogħol, u mgħiba tal-utent finali.

3.3 Li jitnaqqas ir-riskju ta' ksur tal-privatezza, telf ta' proprjetà intellettuali, u esfiltrazzjoni tad-data kkawżati minn negliġenza jew nuqqas ta' sorveljanza.

3.4 Li tiġi integrata mgħiba ta' mejda nadifa u skrin nadif fil-kultura organizzattiva, b'apport għad-dixxiplina operattiva, l-awditabbiltà, u d-difiżibbiltà legali.

3.5 Li tappoġġa l-konformità ma' ISO/IEC 27001, l-Artikolu 32 tal-GDPR, l-Artikolu 15 tan-NIS2, u rekwiżiti oħra ta' sigurtà fiżika rilevanti għal data kritika jew personali.

### 4. Rwoli u responsabbiltajiet

#### 4.1 Il-Maniġment Eżekuttiv

4.1.1 Japprova din il-politika u jippromwovi kultura ta' għarfien dwar is-sigurtà fl-unitajiet kollha tan-negozju.

4.1.2 Jalloka riżorsi xierqa għall-applikazzjoni tal-politika, kampanji ta' sensibilizzazzjoni, u mekkaniżmi ta' kontroll fiżiku.

#### 4.2 L-Uffiċjal Ewlieni tas-Sigurtà tal-Infurmazzjoni / Maniġer tal-ISMS

4.2.1 Huwa s-sid ta' din il-politika u jiżgura l-allinjament tagħha ma' ISO/IEC 27001:2022, mar-rekwiżiti tal-awditjar, u mal-istrateġiji ta' trattament tar-riskju.

4.2.2 Jiżviluppa programmi ta' sensibilizzazzjoni u kontrolli biex jiżgura implimentazzjoni konsistenti fil-faċilitajiet u f'ambjenti ta' xogħol ibridi.

4.2.3 Jikkoordina mal-ġestjoni tal-faċilitajiet u mal-IT biex jiżgura li jkunu fis-seħħ salvagwardji fiżiċi xierqa.

[ ... 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 Skeda għar-rieżami tal-politika

##### 9.1.1 Din il-politika għandha tiġi rieżaminata:

9.1.1.1 Mill-inqas darba fis-sena

9.1.1.2 Wara kull nonkonformità tal-awditjar relatata ma' esponiment ta' spazju tax-xogħol jew skrin

9.1.1.3 Wara incident fiżiku jew ambjentali (eż. serq ta' apparat, tailgating, sorveljanza)

9.1.1.4 Meta jiġu implimentati layouts ġodda tal-uffiċċju, politiki tal-faċilitajiet, jew mudelli ta' spazju tax-xogħol (eż. hot-desking, remote hubs)

#### 9.2 Sidien responsabbli

9.2.1 Is-sid ta' din il-politika huwa l-Uffiċjal Ewlieni tas-Sigurtà tal-Infurmazzjoni jew il-Maniġer tal-ISMS maħtur.

### **9.2.2 Il-proċess ta' rieżami għandu jinvolti:**

9.2.2.1 Timijiet tal-Facilitajiet u tas-Sigurtà Korporattiva

9.2.2.2 IT u Infrastruttura għall-applikazzjoni relatata mal-apparati

9.2.2.3 Riżorsi Umani u Legali għall-applikazzjoni tal-imġiba u l-allinjament dixxiplinari

9.2.3 L-aġġornamenti kollha tal-politika għandhom ikunu taħt kontroll tal-verżjoni, approvati mill-Kumitat ta' Tmexxija tal-ISMS, u mqassma mill-ġdid b'rikonoxximent mill-ġdid fejn meħtieġ.

### **9.3 Komunikazzjoni tal-bidliet**

#### **9.3.1 L-utenti għandhom jiġu nnotifikati b'aġġornamenti materjali permezz ta':**

9.3.1.1 Ċentru jew portal tal-politiki fuq l-intranet

9.3.1.2 Komunikazzjonijiet immirati bl-imejl

9.3.1.3 Aġġornamenti tal-onboarding u briefings kull tliet xhur

9.3.1.4 Triggers obligatorji ta' rikonoxximent għal kwalunkwe klawżola ġdida kritika ta' applikazzjoni

### **10. Politiki relatati u rabtiet**

#### **10.1 Din il-politika hija allinjata ma' u tappoġġa dan li ġej:**

10.1.1 P1 – Politika tas-Sigurtà tal-Infommazzjoni: Tistabbilixxi aspettattivi dwar l-imġiba tal-utent u s-sigurtà fiżika li huma fundamentali għal din il-politika.

10.1.2 P3 – Politika dwar Użu Aċċettabbli: Tindirizza r-responsabbiltà tal-utent fil-protezzjoni tad-data u tas-sistemi, inklużi l-ambjenti fiżiċi.

10.1.3 P6 – Politika tal-Ġestjoni tar-Riskju: Tinkorpora riskji relatati mal-ispazju tax-xogħol fiżiku bħala parti mill-analiżi tar-riskju tal-infommazzjoni fil-livell tal-intrapriża.

10.1.4 P12 – Politika tal-Ġestjoni tal-Assi: Tappoġġa t-traċċar u l-immaniġġjar sigur ta' apparati u midja li jithallew fuq l-imwejjed.

10.1.5 P13 – Politika tal-Klassifikazzjoni u t-Tikkettar tad-Data: Torbot mal-applikazzjoni tal-mejda nadifa għal dokumenti fiżiċi mmarkati bħala Kunfidenzjali jew Interni.

10.1.6 P14 – Politika taż-Żamma tad-Data u r-Rimi: Tiggwida ż-żamma ta' dokumenti fiżiċi, it-tqattigħ, u l-prattiki ta' mmaniġġjar tal-bins.

10.1.7 P22 – Politika tal-Illoggjar u l-Monitoraġġ: Tista' tintuża biex timmonitorja l-istatus tal-illokkjar tal-istazzjonijiet tax-xogħol, il-ħin ta' inattività, jew camera feeds tal-ispazji tax-xogħol fejn dan ikun permess.

10.2 Dawn il-politiki relatati jistabbilixxu kultura ta' sigurtà integrata, li tgħaqqad l-għarfien tal-utenti, salvagwardji fiżiċi, u responsabbiltà biex jiġu żgurati spazji tax-xogħol reżiljenti.

### **11. Standards u oqfsa ta' referenza**

11.1 Din il-politika hija allinjata ma' standards rikonoxxuti globalment u ma' rekwiżiti legali li jimponu l-protezzjoni ta' infommazzjoni sensittiva f'ambjenti fiżiċi u permezz tal-imġiba tal-utent.

#### **11.2 ISO/IEC 27001**

11.2.1 Klawżola 6.1.3 – Pjan ta' Trattament tar-Riskju: Tappoġġa l-implimentazzjoni ta' kontrolli għall-mitigazzjoni ta' riskji fiżiċi u ambjentali, inklużi dawk marbuta mal-imġiba tal-utent fi spazji tax-xogħol miftuħa.

11.2.2 Klawżola 8.1 – Ippjanar u Kontroll Operattiv: Tistabbilixxi salvagwardji operattivi għall-ġestjoni ta' spazji tax-xogħol siguri u l-użu tat-tagħmir.

#### **11.3 ISO/IEC 27002:2022 – Kontroll 7**

11.3.1 Dan il-kontroll jeħtieġ protezzjonijiet ta' mġiba u ambjentali biex jipprevjenu aċċess mhux awtorizzat għall-infommazzjoni permezz ta' midja, skrins, jew materjal stampat li jithalla mingħajr

attenzjoni. Il-politika tapplika igjene fiżika tal-ispazju tax-xogħol, l-użu ta' illokkjar tal-iskrin, u r-rimi ta' dokumenti sensitivi.

#### **11.4 NIST SP 800-53 Rev.5**

11.4.1 PE-2 (Awtorizzazzjonijiet ta' Aċċess Fiżiku): Marbut permezz ta' restrizzjonijiet tal-ispazju tax-xogħol u applikazzjoni ta' hażna msakkra f'ambjenti ta' riskju għoli.

11.4.2 PS-7 (Sigurtà tal-Persunal Estern): Applikat permezz ta' rekwiżiti ta' mejda nadifa u skrin nadif estiżi għal kuntratturi u utenti ta' partijiet terzi.

11.4.3 MP-6 (Sanitizzazzjoni tal-Midja) u AC-11 (Illokkjar tas-Sessjoni): Implimentati permezz ta' proċeduri ta' rimi sigur u timers obbligatorji ta' illokkjar tal-iskrin.

11.4.4 CM-6 (Impostazzjonijiet tal-Konfigurazzjoni) u IA-5 (Ġestjoni tal-Awtentikaturi): Jappoġġaw l-applikazzjoni teknika tal-illokkjar tal-iskrin u l-kontroll tas-sessjoni fuq l-endpoints.

#### **11.5 GDPR tal-UE (2016/679)**

11.5.1 Artikolu 5(1)(f): Japplika l-integrità u l-kunfidenzjalità tad-data personali, inklużi protezzjonijiet kontra esponiment fiżiku jew viżwalizzazzjoni minn persuni mhux awtorizzati.

11.5.2 Artikolu 32 – Sigurtà tal-Ipproċessar: Jeħtieġ miżuri fiżiċi u organizzattivi xierqa biex jipproteġu d-data personali minn qerda aċċidentali jew illegali, telf, jew żvelar mhux awtorizzat — miksuba permezz ta' kontrolli tal-mejda u tal-iskrin.

11.5.3 Premessa 39: Teħtieġ li l-aċċess għad-data personali jiġi limitat għal individwi awtorizzati — dan jinkludi li tkun issigurata f'forma fiżika meta titħalla mingħajr attenzjoni.

#### **11.6 Direttiva NIS2 tal-UE (2022/2555)**

11.6.1 Artikolu 21(2)(d): Jeħtieġ politiki u proċeduri relatati mas-sigurtà fiżika u ambjentali, inklużi protezzjonijiet tas-sigurtà tal-informazzjoni fil-livell tal-post tax-xogħol.

11.6.2 Artikolu 21(3): Jinkoraġġixxi kultura ta' sigurtà li tinkorpora mġiba tajba tal-utent, għarfien, u prevenzjoni ta' tnixxijiet ta' data mhux intenzjonati — appoġġata mill-kontrolli ta' mġiba ta' din il-politika.

#### **11.7 DORA tal-UE (2022/2554)**

11.7.1 Artikolu 5 – Governanza Interna u Kontroll: Jeħtieġ li r-riskji kollha relatati mal-ICT, inklużi theddid uman u ambjentali, jiġu gvernati permezz ta' politiki infurzabbli.

11.7.2 Artikolu 8 – Ġestjoni tar-Riskju tal-ICT: Japplika salvagwardji kemm f'kuntesti diġitali kif ukoll fiżiċi, u jiżgura li utenti remoti, tal-fergħat, u fuq il-post ma joħolqux esponiment mhux immaniġġjat.

11.7.3 Artikolu 9 – Ġestjoni tal-Inċidenti: Jeħtieġ li nuqqasijiet ambjentali jew ta' mġiba li jwasslu għal esponiment ta' data jiġu rreġistrati, ikklassifikati, u indirizzati b'azzjonijiet korrettivi xierqa.

#### **11.8 COBIT 2019**

11.8.1 DSS01 – Operazzjonijiet Immaniġġjati: Jiżgura dixxiplina operattiva fil-protezzjoni ta' spazji tax-xogħol fiżiċi u sistemi permezz ta' kontrolli ripetibbli.

11.8.2 DSS05 – Servizzi tas-Sigurtà Immaniġġjati: Jappoġġa l-protezzjoni tad-data, tal-apparati, u tal-endpoints tal-aċċess permezz ta' applikazzjoni bbażata fuq l-imġiba b'hal prattiki ta' mejda nadifa.

11.8.3 MEA03 – Monitoraġġ, Evalwazzjoni, u Valutazzjoni tal-Konformità: Jinkoraġġixxi l-awditjar ta' salvagwardji fiżiċi u l-adozzjoni tal-politika fil-prattiki tan-negozju ta' kuljum.