					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P10S					Titlu tad-dokument: **Politika tal-Mejda Nadifa u tal-Iskrin Nadif**							
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 r-regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżoli 7.2, 8	
ISO/IEC 27002:2022	Kontroll 7	
NIST SP 800-53 Rev.5	PE-2, AC-11	
Direttiva NIS2 tal-UE	Artikolu 21(2)(d)	
DORA tal-UE	Artikolu 9(2)(f)	
COBIT 2019	DSS01.06, DSS05	
GDPR tal-UE	Artikolu 32	

1. Għan

1.1 Din il-politika tistabbilixxi rekwiżiti vinkolanti biex jinżamm ambjent tax-xogħol sigur billi jiġi żgurat li l-imwejjed, l-istazzjonijiet tax-xogħol u l-iskrins tal-wiri jinżammu ħielsa minn informazzjoni kunfidenzjali viżibbli meta jitħallew mingħajr sorveljanza.

1.2 L-għan ewlieni tagħha huwa li tipprevjeni aċċess mhux awtorizzat għal informazzjoni sensittiva permezz ta' dokumenti stampati li jitħallew mingħajr sorveljanza, skrins mhux imsakkra jew mezzi ta' ħżin rimovibbli mqiegħda b'mod mhux sigur, kemm f'ambjenti fiżiċi tal-uffiċċju kif ukoll f'postijiet ta' xogħol remoti.

1.3 Il-prattiki tal-mejda nadifa u tal-iskrin nadif definiti f'din il-politika jsaħħu l-kapaċità tal-organizzazzjoni tagħna li tissodisfa r-rekwiżiti taċ-ċertifikazzjoni ISO/IEC 27001 billi jimminimizzaw riskji ta' espożizzjoni evitabbli. Dawn il-prattiki jagħtu wkoll assigurazzjoni lill-klijenti, lis-sħab u lill-awdituri li nieħdu s-sigurtà tal-informazzjoni bis-serjetà, anke f'ambjenti b'riżorsi limitati.

1.4 Din il-politika tappoġġa kultura ta' responsabbiltà u għarfien dwar is-sigurtà, u tiżgura li l-persunal kollu, irrispettivament mir-rwol jew mil-livell ta' kompetenza teknika, jifhem ir-responsabbiltà tiegħu li jipproteġi l-informazzjoni tal-kumpanija u tal-klijenti minn espożizzjoni viżiva, serq jew telf.

2. Kamp ta' applikazzjoni

2.1 Din il-politika tapplika għal:

2.1.1 L-impjegati, il-kuntratturi, l-interns u l-ħaddiema temporanji kollha li jużaw stazzjonijiet tax-xogħol, skrivaniji jew apparati mobbli li huma proprjetà tal-kumpanija jew assenjati individwalment

2.1.2 Il-postijiet fiżiċi kollha użati għall-attività tan-negozju, inklużi uffiċċji ddedikati, ambjenti ta' coworking u spazji tax-xogħol remoti jew mid-dar

2.1.3 L-apparati diġitali kollha b'kapaċità ta' wiri, inklużi desktop computers, laptops, tablets u monitors esterni użati għal skopijiet tan-negozju

2.2 Il-politika testendi għal kwalunkwe assi fiżiku jew diġitali li jista' juri, jaħżen jew jittrasmetti informazzjoni sensittiva, inklużi:

2.2.1 reġistri stampati jew noti miktuba bl-idejn

2.2.2 USB drives, CDs u hard drives esterni

2.2.3 telefowns ċellulari użati għal messaġġi tan-negozju jew email

2.2.4 monitors tal-kompjuter u projectors konnessi ma' sistemi tax-xogħol

2.3 Din il-politika tibqa’ tapplika barra l-ħinijiet normali tax-xogħol u waqt operazzjonijiet mhux standard (eż. manutenzjoni barra l-ħin jew xogħol ta’ rispons għal emerġenza).

3. Objettivi

3.1 Jiġu applikati kontrolli prattiċi u konsistenti biex jiġi żgurat li ma titħalliex informazzjoni sensittiva esposta fuq imwejjed, skrins jew spazji komuni.

3.2 Jitnaqqas ir-riskju ta’ aċċess mhux awtorizzat, kemm minn sorsi interni (eż. aċċess mhux intenzjonat minn impjegati oħra) kif ukoll minn theddid estern (eż. viżitaturi, persunal tat-tindif jew kuntratturi).

3.3 Jiġu appoġġati restrizzjonijiet ta’ aċċess fiżiku u loġiku billi l-persunal ikun obbligat jiżgura b’mod attiv il-materjal tax-xogħol u jsakkar il-kompjuters meta jitħallew mingħajr sorveljanza.

3.4 Jinbena għarfien fost il-persunal dwar prattiki siguri tax-xogħol u jiġu pprovduti regoli sempliċi u applikabbli għall-operazzjonijiet ta’ kuljum, irrispettivament mill-post tax-xogħol.

3.5 Jiġi żgurat allinjament mal-Kontroll 7.7 tal-Anness A tal-ISO/IEC 27001 u mal-gwida ta’ implimentazzjoni tiegħu skont l-ISO/IEC 27002 għar-rekwiżiti tal-mejda nadifa u tal-iskrin nadif.

3.6 Jiġi żgurat li l-organizzazzjoni tkun tista’ turi diliġenza dovuta u tkun lesta għall-awditjar mingħajr ma tkun teħtieġ infrastruttura ta’ livell enterprise.

4. Rwoli u responsabbiltajiet

4.1 Maniġer Ġenerali (GM)

4.1.1 Huwa s-sid ta’ din il-politika u jiżgura li tiġi kkomunikata kif xieraq, mifhuma u osservata mill-impjegati u l-kuntratturi kollha.

4.1.2 Huwa responsabbli biex japprova kwalunkwe eċċezzjoni, jirrispondi għall-ksur u jissorvelja t-taħriġ relatat ma’ prattiki siguri tax-xogħol.

4.1.3 Għandu jwettaq jew jiddelega verifiki regolari ta’ kontroll (mill-inqas kull tliet xhur) biex jikkonferma li l-ispazji tax-xogħol fiżiċi u diġitali jissodisfaw ir-rekwiżiti tal-politika.

4.2 Membru tal-Persunal Maħtur (jekk jiġi assenjat)

4.2.1 Jista’ jiġi nnominat biex ikun responsabbli għall-implimentazzjoni ta’ konfigurazzjonijiet tekniċi (eż. settings ta’ timeout tal-iskrin) jew għad-distribuzzjoni ta’ mezzi ta’ ħażna fiżika (eż. kxaxen li jissakkru).

4.2.2 Jappoġġa lill-GM billi jirrapporta nuqqas ta’ konformità, jimmaniġġja tfakkiriet dwar is-sigurtà tal-ispazju tax-xogħol u jsegwi azzjonijiet korrettivi meta jiġu identifikati kwistjonijiet.

4.2.3 Jgħin biex jiġi żgurat li l-impjegati kollha jkollhom aċċess għal mekkaniżmi ta’ serratura xierqa jew spazji ta’ ħażna siguri fejn dan ikun fattibbli.

[... 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 Il-GM għandu jwettaq rieżami ta’ din il-politika mill-inqas darba fis-sena u wara kwalunkwe wieħed mill-avvenimenti li ġejjin:

9.1.1 Introduzzjoni ta’ spazji ġodda tal-uffiċċju, apparati jew sistemi kondiviżi

9.1.2 Bidliet fir-rekwiżiti legali jew taċ-ċertifikazzjoni applikabbli

9.1.3 Sejbiet tal-awditjar, valutazzjonijiet tar-riskju jew inċident tas-sigurtà tal-informazzjoni

9.2 Aġġornamenti interim għandhom jiġu kkomunikati lill-impjegati kollha permezz tal-email, b’rikonoxximent obbligatorju.

9.3 Verżjonijiet preċedenti ta’ din il-politika għandhom jinħażnu b’mod sigur u b’mod awditabbli sabiex jintwera allinjament kontinwu mal-ISO/IEC 27001 u oqfsa relatati.

10. Politiki relatati u rabtiet

10.1 P2S – Politika dwar ir-Rwoli u r-Responsabbiltajiet tal-Governanza: Tiċċara l-awtorità tal-GM biex jinforza u jawdita l-imġiba fl-ispazji tax-xogħol fiżiċi u diġitali.

10.2 P4S – Politika dwar il-Kontroll tal-Aċċess: Tappoġġa l-implimentazzjoni teknika tal-issakkar tal-iskrin u prattiki siguri ta' login fuq l-istazzjonijiet tax-xogħol.

10.3 P8S – Politika dwar l-Għarfien tas-Sigurtà tal-Informazzjoni u t-Taħriġ: Issaħħaħ it-taħriġ fl-imġiba meħtieġa għall-konformità ma' din il-politika.

10.4 P17S – Politika dwar il-Protezzjoni tad-Data u l-Privatezza: Tiddefinixxi obbligi għall-immaniġġjar u s-salvagwardja ta' data personali u sensittiva f'konformità mal-GDPR.

10.5 P30S – Politika dwar ir-Rispons għall-Inċidenti: Tipprovdi l-qafas ta' eskalazzjoni u rispons jekk ksur jirriżulta f'espożizzjoni ta' data jew ksur ta' data.

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001

11.1.1 Klawżola 7.2: Teħtieġ li l-persunal kollu jkun konxju mir-responsabbiltajiet tas-sigurtà, inkluži salvagwardji fiżiċi.

11.1.2 Klawżola 8.1: Kontrolli operattivi għandhom jiżguraw protezzjonijiet fiżiċi u loġiċi xierqa.

11.2 ISO/IEC 27002

11.2.1 Kontroll 7.7: Jipprovdi gwida dettaljata dwar kif jiġu stabbiliti, ikkomunikati u applikati rekwiżiti tal-mejda nadifa u tal-iskrin nadif.

11.3 NIST SP 800-53 Rev.5

11.3.1 PE-2: Jistabbilixxi aspettattivi ta' kontroll tal-aċċess fiżiku, inkluża l-imġiba tal-persunal f'ambjenti siguri.

11.3.2 AC-11: Jobbliga funzjonalità ta' serratura tas-sessjoni għall-istazzjonijiet tax-xogħol sabiex jiġi evitat wiri jew interazzjoni mhux awtorizzata.

11.4 GDPR tal-UE

11.4.1 Artikolu 32: Jeħtieġ li l-organizzazzjonijiet jipproteġu d-data personali bl-użu ta' salvagwardji fiżiċi u tekniċi, inkluži stazzjonijiet tax-xogħol u dokumenti.

11.5 Direttiva NIS2 tal-UE

11.5.1 Artikolu 21(2)(d): Teħtieġ li l-organizzazzjonijiet jimplimentaw politiki ta' aċċess fiżiku u loġiku bbażati fuq ir-riskju.

11.6 DORA tal-UE

11.6.1 Artikolu 9(2)(f): Jobbliga politiki ta' sigurtà tal-ICT, inkluża iġjene sigura tal-ispazju tax-xogħol, għall-operaturi tas-settur finanzjarju u l-katini tal-provvista tagħhom.

11.7 COBIT 2019

11.7.1 DSS01.06: Jeħtieġ prattiki ta' protezzjoni tal-assi, inkluži kontrolli fiżiċi fuq spazji tax-xogħol u mezzi.

11.7.2 DSS05.02: Jappoġġa l-applikazzjoni ta' prattiki tas-sigurtà tal-utenti finali f'ambjenti operattivi differenti.