					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P09S					Titlu tad-dokument: **Politika dwar ix-Xogħol Remot**							
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**

Allinjata ma’ standards u regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżola 6.1, 6.2, 8	
ISO/IEC 27002:2022	Kontroll 6	
NIST SP 800-53 Rev.5	AC-17, AC-2	
Direttiva NIS2 tal-UE	Artikoli 21(2)(b), 21(2)(h)	NIS2 tal-UE
DORA tal-UE	Artikolu 9	DORA tal-UE
COBIT 2019	DSS05, APO13	COBIT 2019
GDPR tal-UE	Artikolu 32	GDPR tal-UE

1. Għan

1.1 Din il-politika tistabbilixxi r-rekwiżiti ta’ sigurtà għall-impjegati u l-kuntratturi li jaħdmu b’mod remot, inkluż mid-dar, minn spazji ta’ xogħol kondiviżi jew waqt l-ivvjaġġar.

1.2 L-għan tagħha huwa li tipproteġi l-Kunfidenzjalità, l-Integrità u d-Disponibbiltà (CIA) tal-informazzjoni tan-negozju aċċessata barra minn ambjenti kkontrollati mill-kumpanija.

1.3 Din il-politika tiżgura l-konformità ma’ standards internazzjonali u tnaqqas riskji bħal aċċess mhux awtorizzat, telf ta’ data u interruzzjoni tas-servizz.

2. Kamp ta’ applikazzjoni

2.1 Din il-politika tapplika għall-membri kollha tal-persunal (impjegati, kuntratturi, konsulenti u ħaddiema temporanji) li jaċċessaw sistemi, netwerks jew data tal-kumpanija waqt li jkunu qed jaħdmu barra mis-sit.

2.2 Tkopri:

2.2.1 L-użu ta’ sistemi pprovduti mill-kumpanija u apparati personali

2.2.2 Aċċess permezz ta’ VPN, desktop remot jew servizzi cloud

2.2.3 L-immaniġġjar sigur tal-informazzjoni barra mill-bini tal-kumpanija

2.2.4 Monitoraġġ, ġestjoni tal-eċċezzjonijiet u infurzar

2.3 Tapplika kemm għal arranġamenti ta’ xogħol remot full-time kif ukoll part-time, inkluż aċċess remot ad hoc.

3. Objettivi

3.1 Tipprevjeni aċċess mhux awtorizzat għal sistemi tal-kumpanija jew għal data sensittiva waqt ix-xogħol remot.

3.2 Tiżgura li l-apparati u l-konnessjonijiet ta’ komunikazzjoni użati barra mill-uffiċċju jissodisfaw ir-rekwiżiti tal-konfigurazzjoni bażi tas-sigurtà.

3.3 Iżżomm kontroll fuq il-privileġġi tal-aċċess remot u fuq il-monitoraġġ.

3.4 Tipprovdi gwida ċara lill-impjegati u lill-maniġers dwar prattiki siguri ta’ xogħol remot.

3.5 Tiżgura konformità mal-aspettattivi ta’ ISO, NIS2, GDPR, DORA u COBIT għax-xogħol remot u mobbli.

4. Rwoli u responsabbiltajiet

4.1 Maniġer Ġenerali

4.1.1 Japprova l-arranġamenti ta’ xogħol remot u jimmonitorja l-konformità.

4.1.2 Jiskala kwalunkwe inċident tas-sigurtà tal-informazzjoni jew nuqqasijiet ripetuti ta' konformità.

4.1.3 Jagħmel rieżami tal-eċċezzjonijiet u jiżgura s-segwitu tal-inċidenti.

4.2 Fornitur ta' Appoġġ tal-IT jew Fornitur Estern ta' Servizzi tal-IT

4.2.1 Jistabbilixxi aċċess remot sigur (eż. VPN, awtentikazzjoni b'diversi fatturi).

4.2.2 Japplika kontrolli tas-sigurtà tal-endpoint, iċċifrar u impostazzjonijiet tal-konfigurazzjoni tal-apparati.

4.2.3 Jappoġġa lill-utenti u jinvestiga kwalunkwe kwistjoni teknika relatata mas-sigurtà.

[... 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 Rieżami Annwali tal-Politika

9.1.1 Il-Maniġer Ġenerali u l-Fornitur ta' Appoġġ tal-IT għandhom jirrieżaminaw din il-politika kull sena biex tibqa' allinjata mat-teknoloġija, mal-forza tax-xogħol u mal-bidliet legali.

9.2 Attivaturi għal Aġġornament Bikri

9.2.1 Huwa meħtieġ rieżami immedjat wara:

9.2.1.1 Inċident ewlieni tas-sigurtà relatat max-xogħol remot

9.2.1.2 Bidliet fir-rekwiżiti ta' NIS2, GDPR jew DORA

9.2.1.3 Tranżizzjoni għal teknoloġija ġdida ta' aċċess remot (eż. pjattaforma VPN differenti)

9.3 Kontroll tal-Verżjoni u Arkivjar

9.3.1 Il-verżjonijiet kollha ta' din il-politika għandhom ikunu:

9.3.1.1 Datati u approvati mill-Maniġer Ġenerali

9.3.1.2 Assenjati numru tal-verżjoni

9.3.1.3 Arkivjati għal mill-inqas tliet snin

9.4 Komunikazzjoni lill-Persunal

9.4.1 Aġġornamenti tal-politika għandhom jiġu kkomunikati lill-utenti remoti kollha. Huwa meħtieġ rikonoxximent għal kwalunkwe bidla sinifikanti.

10. Politiki relatati u rabtiet

10.1 Din il-politika hija marbuta ma' u tappoġġa dan li ġej:

10.1.1 P2S – Politika dwar ir-Rwoli u r-Responsabbiltajiet tal-Governanza: Tiddefinixxi min jawtorizza u min iwettaq is-sorveljanza tal-aċċess remot

10.1.2 P4S – Politika dwar il-Kontroll tal-Aċċess: Tistabbilixxi l-arranġamenti siguri tal-aċċess remot u l-proċeduri ta' revoka

10.1.3 P6S – Politika tal-Ġestjoni tar-Riskju: Tsegwi u tevalwa r-riskji relatati mal-aċċess barra mis-sit

10.1.4 P8S – Politika dwar l-Għarfien tas-Sigurtà tal-Informazzjoni u t-Taħriġ: Tħarreġ lill-utenti dwar ir-riskji tax-xogħol remot u l-aħjar prattiki

10.1.5 P30S – Politika dwar ir-Rispons għall-Inċidenti: Timmmaniġġja r-rispons għal inċidenti ta' aċċess remot bħal tnixxijiet ta' kredenzjali jew telf ta' apparat

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001

11.1.1 Klawżola 6.1 – Ippjanar ibbażat fuq ir-riskju għal xenarji ta' aċċess remot

11.1.2 Klawżola 6.2 – Tindirizza r-responsabbiltajiet tar-riżorsi umani f'kuntesti mobbli u remoti

11.1.3 Klawżola 8.1 – Ippjanar operattiv u kontroll tal-proċessi remoti

11.2 ISO/IEC 27002

11.2.1 Kontroll 6.7 – Jipprovdi gwida prattika dwar is-sigurtà għax-xogħol remot u mobbli

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-17 – Kontroll tal-aċċess remot, protezzjoni tas-sessjonijiet u monitoraġġ tas-sigurtà

11.3.2 AC-2 – Kontroll tal-kontijiet għal utenti barra mis-sit

11.4 GDPR tal-UE

11.4.1 Artikolu 32 – Jeħtieġ protezzjoni tad-data “mid-disinn u b’mod predefinit”, inkluż f’ambjenti remoti

11.5 Direttiva NIS2 tal-UE

11.5.1 Artikolu 21(2)(b) – Jeħtieġ użu sigur tas-sistemi tan-network u tal-informazzjoni

11.5.2 Artikolu 21(2)(h) – Jitlob miżuri ta’ sigurtà relatati mar-riżorsi umani, inklużi kontrolli barra mis-sit

11.6 DORA tal-UE

11.6.1 Artikolu 9 – Jeħtieġ li entitajiet finanzjarji jżommu r-reżiljenza tal-ICT fil-modi operattivi kollha, inkluż l-aċċess remot

11.7 COBIT 2019

11.7.1 DSS05 – Jinkludi protezzjoni tal-endpoint u prattiki siguri tax-xogħol remot

11.7.2 APO13 – Sigurtà Ġestita: Tiżgura provvista sigura u sorveljanza tar-riskju tal-aċċess mobbli u remot