					Daħħal hawn l-isem tal-entità ġuridika rreġistrata						
Numru tad-dokument: P09					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**

1. Għan

1.1 Din il-politika tiddefinixxi r-rekwiżiti obbligatorji biex ix-xogħol remot jitwettaq b'mod sigur, inkluż l-użu tas-sistemi tal-organizzazzjoni, l-aċċess għad-data u l-eżekuzzjoni tad-dmirijiet tax-xogħol barra mill-bini korporattiv.

1.2 Din tiżgura l-Kunfidenzjalità, l-Integrità u d-Disponibbiltà (CIA) tal-assi tal-informazzjoni aċċessati mill-bogħod u tistabbilixxi kontrolli biex jittaffew ir-riskji marbuta ma' ambjenti ta' xogħol distribwiti.

1.3 Il-politika tissodisfa r-rekwiżiti tal-Anness A Kontroll 6.7 tal-ISO/IEC 27001:2022 billi timplimenta salvagwardji tekniċi u proċedurali mfassla għall-kundizzjonijiet tax-xogħol remot.

2. Kamp ta' applikazzjoni

2.1 Din il-politika tapplika għall-persunal kollu awtorizzat li jaħdem mill-bogħod, inklużi:

2.1.1 Impjegati (full-time, part-time, kuntrattwali)

2.1.2 Fornituri esterni ta' servizzi, konsulenti u fornituri terzi

2.1.3 Persunal temporanju u persunal assenjat għal proġetti b'aċċess remot approvat

2.2 Din tkopri:

2.2.1 L-aċċess għas-sistemi tal-organizzazzjoni permezz ta' VPN jew għodod approvati ta' aċċess remot

2.2.2 L-immaniġġjar ta' informazzjoni sensittiva u data rregolata barra minn faċilitajiet siguri

2.2.3 L-użu ta' tagħmir li huwa proprjetà tal-organizzazzjoni jew apparat personali approvat (BYOD)

2.2.4 Protezzjonijiet fiżiċi u loġiċi f'ambjenti remoti

2.3 Il-politika tapplika fil-ġeografiji u ż-żoni tal-ħin kollha fejn l-organizzazzjoni tippermetti x-xogħol remot, kemm jekk regolari, ad hoc, jew waqt avvenimenti ta' kontinwità tan-negozju.

3. Objettivi

3.1 Jiġi żgurat li persuni awtorizzati biss ikunu jistgħu jaċċessaw sistemi interni u informazzjoni mill-bogħod.

3.2 Tiġi applikata l-kriptaġġ, l-awtentikazzjoni b'diversi fatturi u l-protezzjoni tal-endpoint fuq il-mogħdijiet kollha ta' aċċess remot.

3.3 Tinżamm pożizzjoni ta' sigurtà robusta kontra theddid bħal phishing, malware, esfiltrazzjoni tad-data u esponiment mhux awtorizzat tas-sistemi.

3.4 Jiġi regolat kif data sensittiva tintbagħat, tinħażen jew tiġi stampata f'ambjenti barra mis-sit.

3.5 Jiġu implimentati miżuri ta' sigurtà fiżika li jnaqqsu l-viżibbiltà u l-osservazzjoni mhux awtorizzata waqt sessjonijiet remoti.

3.6 Tiġi żgurata l-konformità mar-rekwiżiti regolatorji internazzjonali relatati mal-aċċess remot għad-data, inklużi l-GDPR, in-NIS2 u d-DORA.

4. Rwoli u responsabbiltajiet

4.1 Maniġment Eżekuttiv

4.1.1 Japprova din il-politika u jiżgura li jiġu allokati r-riżorsi meħtieġa u li din tiġi integrata fir-Riżorsi Umani, fl-Operazzjonijiet tal-IT u fl-operazzjonijiet tas-sigurtà.

4.1.2 Jawtorizza l-kriterji ta' eliġibbiltà organizzattiva għax-xogħol remot u l-applikabbiltà tagħhom għall-unitajiet tan-negozju.

4.2 Uffiċjal Ewlieni tas-Sigurtà tal-Informazzjoni / Maniġer tal-ISMS

4.2.1 Huwa s-sid tal-politika u jżommha aġġornata, filwaqt li jiżgura l-allinjament tagħha mal-pożizzjoni tar-riskju u mar-rekwiżiti regolatorji.

4.2.2 Jiddefinixxi l-kontrolli tas-sigurtà għall-aċċess remot (eż. kriptaġġ, protezzjoni tal-endpoint, timeout tas-sessjonijiet).

4.2.3 Japprova l-ġestjoni tal-eċċezzjonijiet u jimmonitorja l-effettività tal-kontrolli.

[... 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 Frekwenza tar-rieżami

9.1.1 Din il-politika għandha tiġi rieżaminata kull sena, jew aktar ta' spiss meta jkun hemm:

9.1.1.1 Introduzzjoni ta' teknoloġiji ġodda ta' aċċess remot

9.1.1.2 Espansjoni sinifikanti tax-xogħol remot (eż. inizjattivi ta' forza tax-xogħol ibrida)

9.1.1.3 Theddid, vulnerabbiltajiet jew inċidenti ġodda marbuta ma' ambjenti remoti

9.1.1.4 Bidliet fil-qafas legali jew regolatorju rilevanti

9.2 Sjieda u proċess tar-rieżami

9.2.1 Is-sid tal-politika huwa l-Uffiċjal Ewlieni tas-Sigurtà tal-Informazzjoni. Ir-rieżami għandu jiġi kkoordinat ma':

9.2.1.1 Operazzjonijiet tal-IT u Arkitettura

9.2.1.2 Riżorsi Umani u ġestjoni tal-faċilitajiet u tal-assi (għall-implikazzjonijiet operattivi u tal-ispazju tax-xogħol)

9.2.1.3 Data Protection Officer (għall-privatezza u l-kontrolli transkonfinali tad-data)

9.2.2 L-aġġornamenti tal-politika għandhom ikunu:

9.2.2.1 Approvati mill-Kumitat ta' Tmexxija tal-ISMS

9.2.2.2 Ikkomunikati lill-persunal u lill-kuntratturi kollha affettwati

9.2.2.3 Integrati fil-materjal ta' onboarding u fit-taħriġ ta' aġġornament

9.3 Kontroll tad-dokument u distribuzzjoni

9.3.1 Il-politika għandha tinkludi kontroll tal-verżjoni, data tad-dħul fis-seħħ u storja tal-bidliet.

9.3.2 Verżjonijiet sostitwiti għandhom jinżammu skont il-Politika tal-Ġestjoni tad-Dokumenti (P14).

9.3.3 Verżjonijiet riveduti għandhom iwasslu għal rikonoxximent obbligatorju mill-ġdid mill-utenti eliġibbli għax-xogħol remot.

10. Politiki relatati u rabtiet

10.1 Din il-politika topera flimkien ma':

10.1.1 P1 – Politika tas-Sigurtà tal-Informazzjoni: Tistabbilixxi l-konfigurazzjoni bażi għall-immaniġġjar sigur tal-assi, applikabbli għall-ambjenti kollha tax-xogħol, inkluż dak remot.

10.1.2 P3 – Politika dwar Użu Aċċettabbli: Tirregola l-użu xieraq tal-apparati u s-sistemi tal-organizzazzjoni matul sessjonijiet ta' xogħol remot.

10.1.3 P4 – Politika dwar il-Kontroll tal-Aċċess: Tiżgura li l-privileġġi ta' aċċess remot isegwu l-prinċipju tal-inqas privileġġ u mekkaniżmi xierqa ta' awtentikazzjoni.

10.1.4 P6 – Politika tal-Ġestjoni tar-Riskju: Tiddefinixxi kif ir-riskji tax-xogħol remot jiġu identifikati, trattati u mmonitorjati fi ħdan l-ISMS.

10.1.5 P12 – Politika tal-Ġestjoni tal-Assi: Teħtieġ inventarju u ġestjoni tal-konfigurazzjoni għall-apparati kollha użati mill-bogħod.

10.1.6 P22 – Politika tal-Illoggjar u l-Monitoraġġ: Tiżgura li s-sessjonijiet remoti jiġu mmonitorjati, awditjati u miżmuma skont ir-rekwiżiti ta' konformità.

10.1.7 P14 – Politika taż-Żamma tad-Data u tar-Rimi: Tiddefinixxi regoli ta' immaniġġjar tad-data rilevanti għax-xogħol remot, inklużi mezzi li jistgħu jitneħħew u r-rimi tal-apparati.

10.2 Dawn il-politiki flimkien jiżguraw li x-xogħol remot ikun sigur, konformi u applikabbli fil-funzjonijiet u l-ġeografiji kollha.

11. Standards u oqfsa ta’ referenza

11.1 Din il-politika hija allinjata ma’ oqfsa rikonoxxuti internazzjonalment għas-sigurtà, il-protezzjoni tad-data u l-ġestjoni tar-riskju tal-ICT biex tiżgura prattiki ta’ xogħol remot siguri, traċċabbli u konformi.

11.2 ISO/IEC 27001

11.2.1 Klawżola 6.1.3 – Ippjanar tat-Trattament tar-Riskju: Din il-politika tikkontribwixxi għat-trattament tar-riskji marbuta mal-aċċess remot u ma’ ambjenti ta’ xogħol distribwiti.

11.2.2 Klawżola 8.1 – Ippjanar u Kontroll Operattiv: Teħtieġ l-implimentazzjoni ta’ kontrolli għal sistemi aċċessati barra mill-bini tal-organizzazzjoni.

11.2.3 Anness A Kontroll 6.7 – Xogħol Remot: Din il-politika tindirizza bis-sħiħ il-kontrolli meħtieġa għas-sigurtà tal-informazzjoni waqt li l-persunal jaħdem barra mill-bini tal-organizzazzjoni, inkluży protezzjonijiet fiżiċi u loġiċi, governanza tal-aċċess u monitoraġġ tal-imġiba tal-utenti.

11.3 ISO/IEC 27002:2022 – Kontroll 6

11.3.1 Dan il-kontroll jeħtieġ salvagwardji proċedurali u tekniċi għax-xogħol remot. Jinkludi rekwiżiti għas-sigurtà tal-apparati, il-metodi ta’ aċċess, l-immaniġġjar tad-data, is-salvagwardji ambjentali u l-ġestjoni ta’ parteċipanti ta’ partijiet terzi — li kollha huma applikati permezz ta’ din il-politika.

11.4 NIST SP 800-53 Rev.5

11.4.1 AC-17 (Aċċess Remot): Appoġġat direttament permezz ta’ kontrolli tal-VPN, awtentikazzjoni b’diversi fatturi, logging tas-sessjonijiet u awtorizzazzjoni ta’ aċċess ibbażata fuq ir-rwoli għall-utenti remoti.

11.4.2 AC-2 (Ġestjoni tal-Kontijiet): Jikkontrolla l-eliġibbiltà tal-aċċess, l-assenjazzjoni ta’ privileġġi remoti u d-diżattivazzjoni tal-kontijiet.

11.4.3 SC-12 sa SC-13 (Protezzjoni Kriptografika, Stabbiliment ta’ Ċwievet Kriptografiċi): Implimentati permezz tal-użu obbligatorju tal-VPNs u l-kriptaġġ sħiħ tad-diska għall-endpoints remoti.

11.4.4 MP-5 (Protezzjoni tat-Trasport tal-Mezzi) u PE-18 (Post tal-Komponenti tas-Sistema tal-Informazzjoni): Il-gwida dwar ix-xogħol remot tobbliga protezzjoni waqt it-trasport u salvagwardji fiżiċi f’ambjenti barra mis-sit.

11.4.5 AU-2, AU-6: Il-logging u l-monitoraġġ tas-sessjonijiet remoti jappoġġaw ir-rekwiżiti tal-awditjar u tar-rispons għall-inċidenti.

11.5 GDPR tal-UE (2016/679)

11.5.1 Artikolu 32 – Sigurtà tal-Ipproċessar: Din il-politika tapplika kontrolli ta’ sigurtà tal-aċċess remot, kriptaġġ u logging meħtieġa biex tiġi protetta d-data personali aċċessata jew ipproċessata mill-bogħod.

11.5.2 Artikolu 5(1)(f): Jiżgura li data personali aċċessata barra mis-sit tkun protetta kontra pproċessar mhux awtorizzat jew illegali u kontra telf aċċidentali.

11.5.3 Premessa 39: Tenfasizza l-limitazzjoni tal-aċċess, l-integrità u l-kunfidenzjalità, b’mod partikolari meta l-apparati jitilqu minn bini sigur.

11.6 Direttiva NIS2 tal-UE (2022/2555)

11.6.1 Artikolu 21(2)(a, b, d): Jeħtieġ li l-aċċess remot ikun protett bħala parti mill-qafas tal-ġestjoni tar-riskju tal-ICT tal-organizzazzjoni. Din il-politika tissodisfa r-rekwiżit għal miżuri ta’ sigurtà li jkopru l-kontroll tal-aċċess, is-sigurtà tad-data u politiki organizzattivi għal ambjenti remoti.

11.6.2 Artikolu 21(3): Jinkoraġġixxi għarfien dwar is-sigurtà u osservanza tal-politika fost il-persunal li jaħdem barra mill-bini ċentrali.

11.7 DORA tal-UE (2022/2554)

11.7.1 Artikolu 5 – Qafas ta’ Governanza u Kontroll Intern: Din il-politika tappoġġa l-aspettattivi ta’ kontroll tar-riskju tal-ICT għax-xenarji operattivi kollha, inklużi mudelli ibridi u remoti.

11.7.2 Artikolu 8 – Qafas tal-Ġestjoni tar-Riskju tal-ICT: Ir-riskji tal-aċċess remot huma identifikati, mitigati u rregolati permezz ta’ kontrolli tekniċi u organizzattivi applikati hawnhekk.

11.7.3 Artikolu 9 – Arranġamenti għall-Qsim tal-Informazzjoni: Jipproteġi kontra tnixxija remota ta’ informazzjoni kondiviża fi ħdan netwerks ta’ reżiljenza operattiva diġitali.

11.8 COBIT 2019

11.8.1 DSS01 – Operazzjonijiet Ġestiti: Din il-politika tappoġġa kontinwità sigura tal-operazzjonijiet tan-negozju irrispettivament mill-post fiżiku.

11.8.2 BAI06 – Tibdiliet fl-IT Ġestiti u BAI09 – Assi Ġestiti: Jiżguraw li l-apparati tax-xogħol remot jiġu traċċati, ikkonfigurati b’mod sigur u mmaniġġjati bħala assi kritiċi.

11.8.3 APO13 – Sigurtà Ġestita: Tippromwovi qafas definit ta’ governanza tas-sigurtà għal ambjenti remoti.

11.8.4 MEA03 – Monitoraġġ, Evalwazzjoni u Valutazzjoni tal-Konformità: Tistabbilixxi li l-attività tax-xogħol remot għandha tiġi rreġistrata fil-logs, rieżaminata u awditjata.