					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P21S					Titlu tad-dokument: **Politika tas-Sigurtà tan-Netwerk**							
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 mal-istandards u r-regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżola 8	-
ISO/IEC 27002:2022	Kontroll 8	-
NIST SP 800-53 Rev.5	AC-4, SC-7	-
GDPR tal-UE	Artikolu 32	-
Direttiva NIS2 tal-UE	Artikoli 21(2)(d), (e)	-
DORA tal-UE	Artikoli 9, 10	-
COBIT 2019	DSS05.02, APO13	-

1. Għan

1.1. L-għan ta' din il-politika huwa li jiżgura li l-komunikazzjonijiet kollha tan-netwerk, kemm interni kif ukoll esterni, ikunu protetti kontra aċċess mhux awtorizzat, tbagħbis, interċettazzjoni jew użu ħażin permezz ta' kontrolli tas-sigurtà definiti b'mod ċar.

1.2. Din il-politika tistabbilixxi regoli għad-disinn sigur, l-użu u l-ġestjoni tal-infrastruttura tan-netwerk, inklużi routers, punti ta' aċċess mingħajr fili, konnessjonijiet ta' aċċess remot u netwerks segmentati.

1.3. Din il-politika għandha l-għan li timminimizza l-esponiment għal theddid ibbażat fuq l-internet, tiżgura l-kunfidenzjalità tad-data trażmessa fuq netwerks interni u esterni, u żżomm id-disponibbiltà ta' servizzi kritiċi.

1.4. Din il-politika tappoġġa ċ-ċertifikazzjoni ISO/IEC 27001:2022 u tikkontribwixxi direttament biex jintlaħqu obbligi legali u regolatorji skont il-GDPR, in-NIS2 u d-DORA, filwaqt li tipprovdi assigurazzjoni teknika lill-klijenti u lill-awdituri.

2. Kamp ta' applikazzjoni

2.1. Din il-politika tapplika għall-komponenti kollha tan-netwerk tal-IT tal-organizzazzjoni, inklużi:

2.1.1. Infrastruttura bil-kejbil u mingħajr fili fil-postijiet tal-uffiċċju

2.1.2. Routers, switches, punti ta' aċċess, firewalls u gateways

2.1.3. Konnessjonijiet ta' aċċess remot inklużi VPNs, RDP u mini cloud

2.1.4. Applikazzjonijiet f'ambjent cloud aċċessati minn netwerks interni jew esterni

2.1.5. Apparati konnessi man-netwerk minn impjegati, kuntratturi jew mistednin

2.2. Din il-politika tirregola kemm is-segmenti tan-netwerk fiżiċi kif ukoll dawk loġiċi, inklużi żoni tal-mistednin, apparati tal-IoT u sistemi back-office.

2.3. Il-politika tkopri l-persunal kollu li għandu aċċess għan-netwerk tal-organizzazzjoni, inklużi:

2.3.1. Impjegati interni

2.3.2. Ħaddiema remoti u persunal ibridu

2.3.3. Fornituri terzi, konsulenti u fornituri tas-servizzi

2.3.4. Mistednin li jużaw aċċess temporanju għall-Wi-Fi

3. Objettivi

3.1. Tiżgura li n-netwerk tal-organizzazzjoni jkun protett kontra aċċess mhux awtorizzat u theddid ċibernetiku estern

3.2. Tiżgura segmentazzjoni xierqa bejn netwerks fdati u netwerks mhux fdati (eż. Wi-Fi tal-mistednin, aċċess tal-forniturі)

3.3. Tippermetti konnettività remota sigura mingħajr ma tikkomprometti s-sistemi interni

3.4. Tipprevjeni l-propagazzjoni tal-malware u l-eżfiltrazzjoni tad-data permezz ta' kanali tan-netwerk

3.5. Tipprovdi monitoraġġ, twissijiet u awditjar tal-attività tan-netwerk biex tappoġġa s-sejbien ta' inċidenti u l-konformità

3.6. Tiżgura li apparati approvati u siguri biss jitħallew jikkonnettjaw man-netwerks interni

3.7. Tissodisfa l-obbligi skont ISO 27001, il-GDPR u oqfsa relatati taċ-ċibersigurtà

4. Rwoli u responsabbiltajiet

4.1. Maniġer Ġenerali (GM)

4.1.1. Huwa s-sid ta' din il-politika u jiżgura li jiġu allokati riżorsi xierqa għad-disinn u l-ġestjoni siguri tan-netwerk

4.1.2. Jirrevedi eċċezzjonijiet għall-kontrolli tas-sigurtà tan-netwerk u japprova ftehimiet ta' aċċess għan-netwerk għall-forniturі

4.1.3. Jirrevedi inċidenti jew sejbiet tal-awditjar relatati ma' dgħufijiet fis-sigurtà tan-netwerk

4.2. Fornitur ta' Appoġġ tal-IT / Rwol Intern tal-IT

4.2.1. Jimplimenta, jikkonfigura u jżomm il-firewalls, ir-routers, is-switches u l-kontrolluri mingħajr fili kollha

4.2.2. Jiġġestixxi s-segmentazzjoni bejn netwerks interni, tal-mistednin u esterni

4.2.3. Jimmonitorja l-logs u t-twissijiet għal tentattivi ta' aċċess mhux awtorizzat jew anomaliji tan-netwerk

4.2.4. Jiżgura li l-aġġornamenti tal-firmware u tal-konfigurazzjoni jiġu applikati b'mod sigur u fil-ħin

[... 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

9.1.1. Din il-politika għandha tiġi riveduta mill-inqas darba fis-sena mill-Maniġer Ġenerali flimkien mal-Fornitur ta' Appoġġ tal-IT u l-Koordinatur tal-Privatezza.

9.2. Attivaturi għal rieżami interim

9.2.1. Ir-rieżami tal-politika għandu jiġi attivat ukoll minn:

9.2.1.1. Bidliet kbar fl-arkitettura tan-netwerk (eż. sistemi ġodda ta' VPN jew firewall)

9.2.1.2. Inċident relatat man-netwerk (eż. intrużjoni, tixrid ta' ransomware, jew eżfiltrazzjoni tad-data)

9.2.1.3. Aġġornamenti legali, regolatorji jew tal-oqfsa li jaffettwaw il-protezzjoni tan-netwerk

9.2.1.4. Pjattaformi ġodda ta' forniturі li jeħtieġu metodi jew protokolli alternattivi ta' aċċess

9.3. Ġestjoni tal-verżjonijiet u dokumentazzjoni

9.3.1. Ir-reviżjonijiet tal-politika għandhom jiġu rreġistrati b'numru tal-verżjoni, data, u sommarju tal-bidliet

9.3.2. Verżjonijiet preċedenti għandhom jiġu arkivjati għal mhux inqas minn 3 snin

9.3.3. L-aġġornamenti għandhom jiġu kkomunikati lill-impjegati affettwati, b'rikonoxximent meħtieġ fejn jiġu introdotti bidliet sinifikanti fl-imġiba meħtieġa

10. Politiki relatati u rabtiet

10.1. Din il-politika għandha tiġi implimentata flimkien mal-politiki ta' sigurtà SME li ġejjin:

10.1.1. P9S – Politika dwar ix-Xogħol Remot: Tistabbilixxi metodi siguri ta’ aċċess remot, rekwiżiti tal-VPN, u protezzjoni tal-endpoint għall-utenti barra mis-sit.

10.1.2. P12S – Politika tal-Ġestjoni tal-Assi: Tiżgura li s-sistemi kollha konnessi man-netwerk jiġu identifikati, ikklassifikati, u traċċati bi status tas-sigurtà aġġornat.

10.1.3. P17S – Politika dwar il-Protezzjoni tad-Data u l-Privatezza: Tiżgura li s-segmentazzjoni tan-netwerk, il-kontrolli tal-aċċess, u l-logging jappoġġaw il-prinċipji tal-privatezza u tal-protezzjoni tad-data skont il-GDPR.

10.1.4. P22S – Politika tal-Logging u l-Monitoraġġ: Tispeċifika r-rekwiżiti għall-ġbir u r-rieżami tal-logs minn apparati tan-netwerk, konnessjonijiet remoti, u kontrolluri mingħajr fili.

10.1.5. P30S – Politika dwar ir-Rispons għall-Inċidenti: Tiddeskrivi l-azzjonijiet meħtieġa b’rispons għal ksur tan-netwerk, tentattivi ta’ aċċess mhux awtorizzat, jew propagazzjoni tal-malware permezz ta’ netwerks interni.

11. Standards u oqfsa ta’ referenza

11.1. ISO/IEC 27001

11.1.1. Klawżola 8.1 – Teħtieġ l-implimentazzjoni ta’ kontrolli biex jiġu żgurati operazzjonijiet siguri u reżiljenti, inklużi n-netwerks.

11.2. ISO/IEC 27002

11.2.1. Kontroll 8.20 – Jipprovdi gwida teknika u proċedurali biex jiġi żgurat aċċess sigur għan-netwerk, segmentazzjoni u monitoraġġ.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-4 – Jobbliga l-kontroll tal-fluss tal-informazzjoni fi ħdan in-netwerks u bejn is-sistemi.

11.3.2. SC-7 – Jeħtieġ protezzjoni tal-konfini, routing sigur, u segmentazzjoni tan-netwerk biex jitnaqqas ir-riskju ta’ aċċess mhux awtorizzat.

11.4. GDPR tal-UE

11.4.1. Artikolu 32 – Jeħtieġ miżuri tekniċi u organizzattivi xierqa biex jiġu żgurati l-kunfidenzjalità, l-integrità, u d-disponibbiltà tas-sistemi u s-servizzi f’netwerk li jipproċessaw data personali.

11.5. Direttiva NIS2 tal-UE

11.5.1. Artikolu 21(2)(d) – Jobbliga miżuri tekniċi bbażati fuq ir-riskju, inklużi s-sigurtà tan-netwerk u l-kontroll tal-aċċess.

11.5.2. Artikolu 21(2)(e) – Jeħtieġ segmentazzjoni u iżolament tas-sistemi biex jiġi evitat li l-inċidenti ċibernetiċi jinfirxu.

11.6. DORA tal-UE

11.6.1. Artikolu 9 – Jeħtieġ li l-organizzazzjonijiet jimplimentaw kontrolli ta’ ġestjoni tar-riskju tal-ICT, inklużi dawk għan-netwerks u l-komunikazzjonijiet siguri.

11.6.2. Artikolu 10 – Jeħtieġ li l-istrateġiji ta’ reżiljenza diġitali jinkludu protezzjoni għall-infrastruttura tan-netwerk u l-konnettività remota.

11.7. COBIT 2019

11.7.1. DSS05.02 – Jeħtieġ protezzjoni effettiva tal-infrastruttura tal-IT u tal-ambjenti tan-netwerk kontra theddid intern u estern.

11.7.2. APO13.01 – Jeħtieġ strateġiji ta’ ġestjoni tar-riskju li jinkludu segmentazzjoni tan-netwerk u monitoraġġ bħala parti mill-mitigazzjoni tat-theddid.