					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P21					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 ma’ standards u regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżola 8	N/A
ISO/IEC 27002:2022	Kontrolli 8.20-8.22	N/A
NIST SP 800-53 Rev.5	SC-7, AC-4, SC-32	N/A
GDPR tal-UE	Artikolu 32	N/A
Direttiva NIS2 tal-UE	Artikolu 21(2)(d)	N/A
DORA tal-UE	Artikolu 9	N/A
COBIT 2019	DSS01.03, DSS05.01, MEA03	N/A

1. Għan

1.1 L-għan ta’ din il-politika huwa li tiddefinixxi r-rekwiżiti tal-organizzazzjoni għall-protezzjoni tan-netwerks interni u esterni tagħha kontra aċċess mhux awtorizzat, tfixkil tas-servizz, interċettazzjoni tad-data u użu ħażin.

1.2 Din tiżgura li l-infrastruttura kollha tan-netwerk — inkluż dik fiżika, virtwali, cloud u ibrida — tkun protetta permezz ta’ mudell ta’ difiża f’saffi, bħas-segmentazzjoni tan-netwerk, l-applikazzjoni tar-regoli tal-firewall, routing sigur u monitoraġġ ċentralizzat.

1.3 Din il-politika tistabbilixxi l-applikazzjoni tal-Klawżola 8.1 tal-ISO/IEC 27001 u tal-Kontrolli tal-Anness A 8.20 sa 8.22, u tiżgura l-konformità mal-obbligi legali u regolatorji applikabbli skont l-Artikolu 32 tal-GDPR, l-Artikolu 21 tan-NIS2 u l-Artikolu 9 tad-DORA.

2. Kamp ta’ applikazzjoni

2.1 Din il-politika tapplika għan-netwerks kollha u għall-komponenti relatati tal-infrastruttura, inklużi:

2.1.1 Routers, switches, punti ta’ aċċess mingħajr fili u firewalls

2.1.2 Netwerks virtwali fil-cloud (eż. AWS VPC, Azure VNET), konċentraturi VPN u sistemi SD-WAN

2.1.3 LANs interni, Żoni Demilitarizzati (DMZs), mogħdijiet ta’ aċċess remot u konnessjonijiet bejn siti jew ma’ partijiet terzi

2.1.4 Sistemi ta’ appoġġ bħal DNS, DHCP, proxy servers u apparati ta’ monitoraġġ

2.2 Din il-politika hija vinkolanti għall-persunal kollu u għall-fornituri terzi ta’ servizzi li jimmaniġġjaw, jikkonfiguraw, jimmonitorjaw jew jinteraġixxu man-netwerks tal-organizzazzjoni, kemm on-premises kif ukoll fil-cloud.

2.3 Is-sistemi u l-applikazzjonijiet kollha konnessi man-netwerks tal-organizzazzjoni — irrispettivament mil-lok jew mis-sjieda — għandhom ikunu konformi ma’ dawn ir-rekwiżiti tas-sigurtà tan-netwerk.

3. Objettivi

3.1 Tiġi żgurata l-Kunfidenzjalità, l-Integrità u d-Disponibbiltà (CIA) tad-data trażmessa fuq in-netwerks permezz ta’ kontrolli ta’ aċċess robusti, routing sigur u monitoraġġ.

3.2 Jiġi evitat aċċess mhux awtorizzat, moviment laterali u sfruttament ta’ riżorsi fin-netwerk billi tiġi implimentata segmentazzjoni tan-netwerk, zoning tat-traffiku u protezzjoni tal-konfini.

3.3 Jinżammu konfigurazzjonijiet tan-netwerk konsistenti bbażati fuq standards tal-industrija u intelligence dwar it-theddid biex l-organizzazzjoni tiddefendi ruħha kontra theddid ċibernetiku li qed jevolvi.

3.4 Jiġu protetti l-komunikazzjonijiet esterni, l-interkonnettività fil-cloud u l-aċċess remot billi jintużaw kanali iċċifrati, awtentikazzjoni stretta u verifika tal-endpoint.

3.5 Tingħata viżibbiltà fuq l-attività tan-netwerk permezz ta' logging ċentralizzat, spezzjoni tat-traffiku f'ħin reali u twissijiet awtomatizzati.

3.6 Tiġi żgurata l-konformità regolatorja billi l-operazzjonijiet kollha tan-netwerk jiġu allinjati mar-rekwiżiti tal-ISO/IEC 27001:2022, il-GDPR, in-NIS2, id-DORA u COBIT 2019.

4. Rwoli u responsabbiltajiet

4.1 Uffiċjal Kap tas-Sigurtà tal-Informazzjoni (CISO)

4.1.1 Huwa s-sid ta' din il-politika u jiżgura li tiġi rieżaminata u allinjata mal-istrateġija usa' tal-organizzazzjoni għaċ-ċibersigurtà.

4.1.2 Japprova mudelli ta' segmentazzjoni tan-netwerk, settijiet ta' regoli tal-firewall għal sistemi sensittivi u talbiet għal eċċezzjoni.

4.2 Maniġer tas-Sigurtà tan-Netwerk / Responsabbli għas-Sigurtà tal-Infrastruttura

4.2.1 Jimmaniġġja l-arkitettura tad-difiża tan-netwerk, inklużi firewalls, sistemi ta' skoperta/prevenzjoni tal-intrużjoni (IDS/IPS), VPNs u routing sigur.

4.2.2 Jeżerċita sorveljanza fuq is-segmentazzjoni tan-netwerk, l-assenjazzjonijiet tal-VLANs, zoning tat-traffiku u l-konnettività esterna.

4.2.3 Jiżgura rieżami kontinwu tal-filtrazzjoni tat-traffiku tad-dħul/ħruġ u l-applikazzjoni tal-prinċipji ta' Zero Trust fil-livelli kollha tan-netwerk.

[... 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 Din il-politika għandha tiġi rieżaminata kull sena mill-Maniġer tas-Sigurtà tan-Netwerk b'kollaborazzjoni mas-CISO u aġġornata abbażi ta':

9.1.1 Theddid emerġenti (eż. tekniki ġodda ta' attakk, vulnerabbiltajiet fil-protokolli)

9.1.2 Bidliet fl-infrastruttura (eż. migrazzjonijiet tas-sistemi lejn il-cloud, implimentazzjonijiet ta' SD-WAN)

9.1.3 Aġġornamenti regolatorji jew ta' standards li jaffettwaw il-protezzjonijiet tan-netwerk

9.1.4 Sejbiet tal-awditjar, xejriet ta' inċidenti jew degradazzjoni fil-prestazzjoni kkawżata mill-kontrolli

9.2 Ir-rieżamijiet għandhom jiġu skattati wkoll minn:

9.2.1 Bidliet maġġuri fl-arkitettura tan-netwerk

9.2.2 Implimentazzjoni ta' pjattaformi ġodda ta' firewall, VPN jew netwerk fil-cloud

9.2.3 Dekummissjonar ta' assi ewlenin jew ta' żoni fdati

9.3 L-aġġornamenti għandhom jiġu rreġistrati fir-Reġistru tal-Kontroll tad-Dokumenti tal-ISMS u kkomunikati lil:

9.3.1 Timijiet tal-infrastruttura u tal-Operazzjonijiet tan-Netwerk

9.3.2 Timijiet tas-SOC u tal-inġinerija tas-sigurtà

9.3.3 Timijiet tal-applikazzjonijiet b'dipendenzi tas-sistema fuq flussi tan-netwerk

9.3.4 Il-fornituri terzi kollha b'interkonnettività attiva

9.4 Il-verżjonijiet kollha preċedenti tal-politika għandhom jiġu arkivjati b'mod sigur b'annotazzjonijiet tal-istorja tat-tibdil sabiex tinżamm il-kapaċità li tintwera l-konformità u t-traċċabbiltà tat-tibdil.

10. Politiki relatati u rabtiet

10.1 P1 - Politika tas-Sigurtà tal-Informazzjoni. Tistabbilixxi prinċipji fundamentali ta' sigurtà u tobbliga protezzjonijiet f'saffi, inklużi kontrolli ta' aċċess u kontrolli kontra t-theddid ibbażati fuq in-netwerk.

10.2 P4 - Politika dwar il-Kontroll tal-Aċċess. Tiżgura li s-segmentazzjoni tan-netwerk tiġi applikata f'allinjament mar-rwoli tal-utenti, mal-prinċipju tal-inqas privileġġ u mar-regoli tal-għoti tal-aċċess.

10.3 P5 - Politika tal-Ġestjoni tat-Tibdil. Tirregola modifiki fil-firewall, aġġustamenti fir-regoli tal-VPN u bidliet fir-routing permezz ta' proċess dokumentat u li jista' jiġi awditjat.

10.4 P12 - Politika tal-Ġestjoni tal-Assi. Tappoġġa l-identifikazzjoni u l-klassifikazzjoni ta' sistemi fin-netwerk u tiżgura li l-assi kollha konnessi jiġu mmaniġġjati taħt kampi ta' applikazzjoni ddefiniti mill-politika.

10.5 P22 - Politika tal-Illoggjar u l-Monitoraġġ. Tirregola l-ġbir, il-korrelazzjoni u ż-żamma tal-logs tan-netwerk, inklużi avvenimenti tal-firewall, tentattivi ta' aċċess u skoperta ta' anomaliji.

10.6 P30 - Politika dwar ir-Rispons għall-Inċidenti. Tiddefinixxi l-proċeduri ta' eskalazzjoni, trażżin u eradikazzjoni b'rispons għal theddid jew intrużjonijiet li joriġinaw min-netwerk, bħal DDoS, moviment laterali jew aċċess mhux awtorizzat.

11. Standards u oqfsa ta' referenza

11.1 Din il-politika hija allinjata ma' standards internazzjonali u obbligi regolatorji li jiddefinixxu operazzjonijiet siguri tan-netwerk, segmentazzjoni tan-netwerk, protezzjoni tal-perimetru u aċċess remot sigur.

11.2 ISO/IEC 27001

11.2.1 Klawżola 8.1 - Ippjanar u Kontroll Operattiv: Teħtieġ li kontrolli tekniċi, inklużi s-salvagwardji tan-netwerk, ikunu integrati fil-proċessi operattivi.

11.3 ISO/IEC 27002:2022

11.3.1 Kontrolli 8.20-8.22. Jipprovdu gwida dwar il-protezzjoni tan-netwerks, is-segmentazzjoni tas-servizzi u l-protezzjoni tas-servizzi tan-netwerk permezz ta' kontrolli tal-aċċess u monitoraġġ.

11.4 NIST SP 800-53 Rev.5

11.4.1 SC-7 - Protezzjoni tal-konfini: Teħtieġ kontrolli tal-perimetru, segmentazzjoni tan-netwerk u interkonnessjonijiet siguri.

11.4.2 AC-4 - Applikazzjoni tal-Kontroll tal-Fluss tal-Informazzjoni: Tappoġġa zoning u restrizzjonijiet tat-traffiku bbażati fuq ir-regoli.

11.4.3 SC-32 - Partizzjonament tas-Sistemi tal-Informazzjoni: Tippromwovi separazzjoni loġika tas-sistemi tal-informazzjoni.

11.5 GDPR tal-UE (2016/679)

11.5.1 Artikolu 32 - Sigurtà tal-Ipproċessar: Jeħtieġ miżuri tekniċi — bħal firewalls u segmentazzjoni tan-netwerk — biex tiġi salvagwardjata informazzjoni personali identifikabbli (PII).

11.6 Direttiva NIS2 tal-UE (2022/2555)

11.6.1 Artikolu 21(2)(d): Jeħtieġ sigurtà effettiva għan-netwerk u għas-sistemi tal-informazzjoni, protezzjoni tal-perimetru, konfigurazzjoni sigura u kontrolli ta' separazzjoni.

11.7 DORA tal-UE (2022/2554)

11.7.1 Artikolu 9 - Ġestjoni tar-riskju tal-ICT: Jobbliga lill-entitajiet finanzjarji jipproteġu n-netwerks u l-interkonnessjonijiet kontra aċċess mhux awtorizzat, tnixxija ta' data u tfixkil operattiv.

11.8 COBIT 2019

11.8.1 DSS01.03 - Monitoraġġ tal-Infrastruttura: Jeħtieġ kontroll proattiv fuq is-saħħa tan-netwerk u l-konnettività.

11.8.2 DSS05.01 - Protezzjoni Kontra l-Malware: Jinkludi segmentazzjoni tan-netwerk u kontroll tal-konfini biex titnaqqas il-propagazzjoni.

11.8.3 MEA03 - Monitoraġġ, Evalwazzjoni u Valutazzjoni tal-Konformità: Isaħħaħ l-applikazzjoni tal-politika tan-netwerk u l-evalwazzjonijiet tal-konformità.