					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P35					Titlu tad-dokument: **Politika tas-Sigurtà għall-IoT / OT**							
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	
ISO/IEC 27002:2022	Kontrolli 5.7, 5.23, 5.27, 5.31, 5.36	
NIST SP 800-53 Rev.5	SC-7, SI-4, CM-2, AC-6, PL-8	
GDPR tal-UE	Artikoli 5, 25, 32	
Direttiva NIS2 tal-UE	Artikoli 21, 23	
DORA tal-UE	Artikoli 9, 10	
COBIT 2019	DSS05.01, BAI09.01, APO13.02	

1. Skop

1.1 Din il-politika tistabbilixxi r-rekwiżiti obbligatorji tas-sigurtà tal-informazzjoni għall-implimentazzjoni, it-tħaddim, il-monitoraġġ u d-dekummissjonar ta’ sistemi tal-Internet tal-Oġġetti (IoT) u tat-Teknoloġija Operattiva (OT) fi ħdan l-organizzazzjoni.

1.2 Tiżgura li dawn is-sistemi jiġu integrati fil-qafas usa’ ta’ ġestjoni taċ-ċibersigurtà tal-organizzazzjoni u li jkunu protetti kontra kompromess, użu ħażin jew sabotaġġ operattiv.

1.3 Il-politika għandha l-għan li timponi kontrolli tekniċi, organizzattivi u proċedurali robusti biex tipproteġi s-sistemi IoT/OT li jinteraġixxu ma’ infrastruttura fiżika, proċessi ta’ produzzjoni u ambjenti kritiċi għas-sigurtà.

1.4 Tappoġġa obbligi regolatorji u kuntrattwali fil-qasam taċ-ċibersigurtà, is-sikurezza, il-kontroll ambjentali u l-kontinwità.

2. Kamp ta’ applikazzjoni

2.1 Din il-politika tapplika għas-sistemi kollha IoT u OT, kemm jekk proprjetà tal-kumpanija, mikrija jew ipprovduti minn partijiet terzi, li jintużaw fl-ambjenti operattivi, amministrattivi jew ta’ produzzjoni tal-organizzazzjoni.

2.2 Is-sistemi koperti jinkludu, iżda mhumiex limitati għal:

2.2.1 apparati IoT bħal sensuri ambjentali, sistemi ta’ kontroll tal-aċċess, dawl intelliġenti, tagħmir ta’ sorveljanza u apparati li jintlibsu

2.2.2 pjattaformi OT bħal PLCs, SCADA, DCS, pannelli HMI, interfaċċi MES u kontrolluri tal-kamp

2.2.3 netwerks ta’ kontroll industrijali jew assi konnessi mal-cloud li jimmonitorjaw operazzjonijiet fiżiċi

2.3 Il-politika tkopri:

2.3.1 l-ambjenti kollha (on-premises, edge, cloud immaniġġjat)

2.3.2 il-partijiet ikkonċernati kollha (utenti interni, integraturi, bejjiegħa ta’ partijiet terzi, kuntratturi)

2.3.3 il-fażijiet kollha taċ-ċiklu tal-ħajja (disinn, akkwist, implimentazzjoni, operazzjonijiet, dekummissjonar)

3. Objettivi

3.1 Jiġu protetti l-infrastrutturi IoT u OT kontra theddid taċ-ċibersigurtà intern u estern, inklużi ċaħda ta’ servizz, aċċess mhux awtorizzat, propagazzjoni ta’ ransomware u manipulazzjoni tal-firmware.

3.2 Jiġi żgurat li l-pjattaformi IoT/OT ma jsirux vetturi għal attakki ta' pont bejn l-IT u l-OT u ma jikkompromettux sistemi kritiċi għas-sigurtà.

3.3 Jiġu applikati l-prinċipji ta' sigurtà mid-disinn u ta' difiża f'diversi saffi tul iċ-ċiklu tal-ħajja ta' dawn it-teknoloġiji.

3.4 Tippermetti integrazzjoni affidabbli, sigura u awditabbli tal-pjattaformi IoT u OT maċ-Ċentru tal-Operazzjonijiet tas-Sigurtà (SOC) tal-organizzazzjoni u mal-pjanijiet tagħha ta' rispons għall-inċidenti.

3.5 Jiġi żgurat li l-implimentazzjonijiet kollha jkunu allinjati mal-kontrolli tal-ISO/IEC 27001 u mal-gwida settorjali applikabbli (eż. IEC 62443, ISO/IEC 27019, NIST SP 800-82).

4. Rwoli u responsabbiltajiet

4.1 Chief Information Security Officer (CISO) / Kap tas-Sigurtà tal-Informazzjoni

4.1.1 Jiddefinixxi l-politiki u l-istandards tekniċi għaċ-ċibersigurtà tal-IoT/OT.

4.1.2 Jeżerċita sorveljanza fuq l-evalwazzjonijiet tar-riskju, il-verifika tal-kontrolli u l-koordinazzjoni bejn id-dipartimenti.

4.2 Inġiniera tal-OT / Maniġers tal-Faċilitajiet u tal-Impjant

4.2.1 Jivverifikaw il-konfigurazzjonijiet tas-sistemi OT u jiżguraw il-konformità mal-politika fl-oqsma tal-produzzjoni.

4.2.2 Iżommu salvagwardji fiżiċi u loġiċi għall-integrità u s-sikurezza tal-OT.

[... Is-sezzjonijiet 4.3–8 mhumiex inklużi f'dan il-preview. Ixtri d-dokument sħiħ biex taċċessa l-kontenut kollu. ...]

9. Rekwiżiti għal rieżami u aġġornament

9.1 Din il-politika trid tiġi rieżaminata tal-inqas darba fis-sena u aġġornata abbażi ta':

9.1.1 bidliet fl-arkitettura, fil-bejjiegħa jew fil-pjattaformi tas-sistemi OT jew IoT

9.1.2 aġġornamenti regolatorji ewlenin (eż. reviżjonijiet tad-DORA, tan-NIS2 jew ta' direttivi settorjali)

9.1.3 l-emerġenza ta' vulnerabbiltajiet ġodda jew xejriet ta' theddid fis-sistemi ta' kontroll

9.1.4 sejbiet minn awditi interni jew esterni, testijiet ta' penetrazzjoni jew eżerċizzji ta' red team

9.2 Is-CISO, il-Kap tas-Sigurtà tal-OT u l-kapijiet tad-dipartimenti rilevanti huma responsabbli biex flimkien jibdew il-proċess ta' rieżami.

9.3 Iridu jinbdew rieżamijiet interim wara:

9.3.1 kwalunkwe inċident relatat mal-IoT/OT li jirriżulta f'ħsara lis-sistema jew f'telf ta' data

9.3.2 introduzzjoni ta' tagħmir ġdid ewlieni, software ta' monitoraġġ jew pjattaformi tal-firmware

9.3.3 integrazzjoni ta' smart edge computing jew awtomazzjoni msaħħa bl-AI fil-livell tal-kamp

9.4 Il-bidliet kollha fil-politika jridu jkunu:

9.4.1 dokumentati fl-istorja tal-verżjonijiet u fir-Reġistru tal-Bidliet tal-Politika

9.4.2 ikkomunikati lill-utenti, lill-bejjiegħa u lill-operaturi IT/OT kollha affettwati

9.4.3 approvati mill-ġdid mill-Amministrazzjoni Eżekuttiva

10. Politiki relatati u rabtiet

10.1 Din il-politika topera flimkien ma' u hija appoġġata mill-politiki li ġejjin dwar is-sigurtà tal-informazzjoni:

10.1.1 P1 – Politika tas-Sigurtà tal-Informazzjoni: Tistabbilixxi l-prinċipji bażiċi tas-sigurtà li jestendu għas-sigurtà tas-sistemi IoT u OT.

10.1.2 P3 – Politika dwar l-Użu Aċċettabbli: Tiddetermina r-restrizzjonijiet fuq l-użu personali u mhux awtorizzat ta' apparati, inkluż f'ambjenti operattivi.

10.1.3 P6 – Politika tal-Ġestjoni tar-Riskju: Tiggwida l-evalwazzjoni, l-aċċettazzjoni u l-mitigazzjoni ta' riskji relatati ma' sistemi embedded u sistemi ta' kontroll.

10.1.4 P12 – Politika tal-Ġestjoni tal-Assi: Tiżgura li s-sistemi kollha IoT u OT ikunu inventarjati formalment u assenjati lil sidien responsabbli.

10.1.5 P20 – Politika tal-Protezzjoni tal-Endpoints / Malware: Tapplika għal kontrolluri konnessi, gateways intelliġenti u sistemi edge fil-produzzjoni.

10.1.6 P22 – Politika tal-Logging u l-Monitoraġġ: Testendi għall-ġbir tal-logs u għall-proċeduri ta' rieżami tagħhom f'ambjenti OT.

10.1.7 P30 – Politika ta' Rispons għall-Inċidenti: Tirregola direttament kif ksur, anomaliji jew fallimenti tas-sistema marbuta mal-IoT/OT iridu jiġu eskalati u ġestiti.

10.1.8 P33 – Politika tal-Monitoraġġ tal-Awditjar u l-Konformità: Tipprovdi mekkaniżmi ta' assigurazzjoni biex tiġi vvalidata l-konformità kontinwa ma' din il-politika.

11. Standards u oqfsa ta' referenza

11.1 Din il-politika hija allinjata ma' standards rikonoxxuti internazzjonalment u ma' oqfsa regolatorji li jiżguraw is-sigurtà, ir-reżiljenza u l-konformità tas-sistemi tal-Internet tal-Oġġetti (IoT) u tat-Teknoloġija Operattiva (OT) f'ambjenti industrijali, ta' produzzjoni u korporattivi.

11.2 ISO/IEC 27002:2022 – Kontrolli 5.7, 5.23, 5.27, 5.31, 5.36

11.2.1 Kontroll 5.7 – Intelligence dwar it-theddid: Jinforma l-monitoraġġ tal-ambjenti OT u l-identifikazzjoni ta' vulnerabbiltajiet speċifiċi għall-IoT.

11.2.2 Kontroll 5.23 – Sigurtà tal-informazzjoni għall-użu ta' servizzi cloud: Japplika meta apparati IoT jinteraġixxu ma' pjattaformi cloud għat-telemetrija, kontroll jew analitika.

11.2.3 Kontroll 5.27 – Arkitettura tas-sistema sigura u prinċipji ta' inġinerija: Jirregola l-prinċipji ta' sigurtà mid-disinn għal sistemi embedded u netwerks ta' kontroll.

11.2.4 Kontroll 5.31 – Sigurtà fil-proċessi ta' żvilupp u appoġġ: Jimponi verifika tas-software u tal-firmware, kontrolli fuq il-patches u rekwiżiti għall-bejjiegħa fl-implimentazzjonijiet OT.

11.2.5 Kontroll 5.36 – Konformità mar-rekwiżiti legali u kuntrattwali: Tiżgura l-konformità tal-assi OT ma' mandati ta' sigurtà, ambjentali u regolatorji.

11.2.6 Dawn il-kontrolli flimkien jistabbilixxu l-aħjar prattiki għas-sigurtà tas-sistemi IoT/OT tul iċ-ċiklu tal-ħajja tagħhom, inklużi d-disinn tal-arkitettura, l-implimentazzjoni sigura, il-patching, l-iskoperta ta' anomaliji u l-konformità mar-rekwiżiti settorjali.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-7 – Protezzjoni tal-konfini: Tiżgura li n-netwerks OT ikunu segmentati u mħarsa kontra aċċess mhux awtorizzat.

11.3.2 SI-4 – Monitoraġġ tas-sistema: Jeħtieġ l-implimentazzjoni ta' mekkaniżmi ta' monitoraġġ kontinwu u skoperta ta' anomaliji f'ambjenti ICS.

11.3.3 CM-2 – Konfigurazzjoni bażi: Jobbliga kontroll tal-konfigurazzjoni u hardening tal-apparati tal-pjattaformi IoT/OT.

11.3.4 AC-6 – Inqas privileġġ: Japplika għall-aċċess tal-utenti u għas-servizzi remoti mogħtija minn bejjiegħa fuq sistemi ta' kontroll embedded.

11.3.5 PL-8 – Arkitetturi tas-sigurtà u l-privatezza: Jirregola l-ippjanar ta' integrazzjoni sigura tas-sistemi, b'mod partikolari għal proġetti ta' modernizzazzjoni tal-OT.

11.4 GDPR tal-UE (2016/679)

11.4.1 Artikolu 5 – Prinċipji relatati mal-ipproċessar ta' data personali: Japplika għal pjattaformi IoT li jipproċessaw data minn sensuri jew data ta' mġiba marbuta ma' individwi.

11.4.2 Artikolu 25 – Protezzjoni tad-data mid-disinn u b'mod awtomatiku: Jeħtieġ salvagwardji tal-privatezza inkorporati fid-disinn tal-prodott IoT u fil-firmware.

11.4.3 Artikolu 32 – Sigurtà tal-ipproċessar: Jimponi iċċifrar, kontroll tal-aċċess u komunikazzjonijiet siguri għat-trażmissjoni tad-data ta' apparati intelliġenti.

11.5 Direttiva NIS2 tal-UE (2022/2555)

11.5.1 Artikoli 21 u 23: Jimponu obbligi ta' sigurtà fuq entitajiet essenzjali u importanti li jużaw sistemi OT. Dawn jinkludu evalwazzjoni tar-riskju, rappurtar tal-inċidenti u verifika tal-katina tal-provvista tal-bejjiegħa IoT/OT u tal-integrità tal-firmware.

11.6 DORA tal-UE (2022/2554)

11.6.1 Artikolu 9 – Ġestjoni tar-riskju tal-ICT: Jeħtieġ integrazzjoni sigura ta' sistemi embedded u teknoloġiji OT fil-programm ta' governanza tar-riskju tal-ICT.

11.6.2 Artikolu 10 – Rekwiżiti tas-sigurtà tal-ICT: Jobbliga miżuri protettivi għal pjattaformi OT interkonnessi użati f'ambjenti finanzjarji u ta' servizzi kritiċi.

11.7 COBIT 2019

11.7.1 DSS05.01 – Protezzjoni kontra l-malware: Jinkludi skoperta u rispons għal theddid speċifiku għall-ICS u kampanji ta' malware tal-IoT.

11.7.2 BAI09.01 – Tistabbilixxi u żżomm rekwiżiti tas-sigurtà: Tikkorrispondi mal-proviżjonament sigur u mat-tħaddim ta' infrastruttura intelliġenti jew embedded.

11.7.3 APO13.02 – Tistabbilixxi u żżomm pjan tas-sigurtà tal-informazzjoni: Teħtieġ l-inklużjoni tas-sistemi OT u tal-vulnerabbiltajiet tagħhom fl-istrateġija usa' taċ-ċibersigurtà korporattiva.