					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P35S					Titlu tad-dokument: **Politika tas-Sigurtà tal-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**

Avviż legali (drittijiet tal-awtur u restrizzjonijiet fuq l-użu)

(C) 2025 Clarysec LLC. All rights reserved.

Dan id-dokument huwa proprjetà intellettwali ta' Clarysec LLC. L-ebda parti minn dan id-dokument ma tista' tiġi kkupjata, użata mill-ġdid, distribwita jew modifikata għal skopijiet kummerċjali jew ta' implimentazzjoni mingħajr awtorizzazzjoni espliċita minn qabel bil-miktub.

L-użu mhux awtorizzat huwa strettament ipprojbit u jista' jwassal għal azzjoni legali.

Għal-liċenzjar, ikkuntattja: info@clarysec.com

Allinjata mal-istandards u mar-regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżoli 6.1, 6.2, 8	
ISO/IEC 27002:2022	Kontrolli 5.23, 5.31	
NIST SP 800-53 Rev.5	SI-7, CM-7, AC-6, PE-20, SC-7	
GDPR tal-UE	Artikolu 32	
Direttiva NIS2 tal-UE	Artikolu 21(2)(a), (d), (f)	
DORA tal-UE	Artikolu 9(2), 10(1)	

1. Għan

1.1. Din il-politika tiddefinixxi r-regoli obbligatorji għall-użu u l-ġestjoni siguri tal-Internet of Things (IoT) u tas-sistemi tat-teknoloġija operattiva (OT) fi ħdan l-organizzazzjoni. Dawn l-apparati jistgħu jinkludu sensuri intelliġenti, kameras tas-sigurtà, magni tal-produzzjoni, kontrolluri tal-HVAC, jew kwalunkwe sistema industrijali konnessa man-network.

1.2. L-għan ta' din il-politika huwa li:

1.2.1. Tipproteġi l-operazzjonijiet fiżiċi u diġitali minn tfixkil jew manipulazzjoni permezz ta' apparati konnessi b'sigurtà dgħajfa

1.2.2. Tiżgura l-implimentazzjoni, il-monitoraġġ u l-manutenzjoni siguri tas-sistemi tal-IoT u l-OT

1.2.3. Tiżgura l-konformità ma' ISO/IEC 27001:2022, mad-Direttiva NIS2 u ma' oqfsa regolatorji relatati

1.2.4. Tipprovdi kontrolli prattiċi u infurzabbli għall-SMEs li joperaw f'ambjenti ta' uffiċċju, maħżen jew produzzjoni

2. Kamp ta' applikazzjoni

2.1. Din il-politika tapplika għall-individwi kollha involuti fl-ippjanar, l-installazzjoni, il-konfigurazzjoni, l-użu, l-appoġġ jew id-dekummissjonar ta' apparati tal-IoT jew tal-OT. Dan jinkludi:

2.1.1. Impjegati, kuntratturi jew interns b'aċċess fiżiku jew remot għall-apparati

2.1.2. Fornituri terzi jew tekniċi tas-servizz li jinstallaw jew iżommu sistemi konnessi

2.1.3. Maniġers Ġenerali jew persunal responsabbli mis-sorveljanza tal-politiki tas-sigurtà

2.2. Il-politika tkopri:

2.2.1. Apparati tal-IoT bħal serraturi intelliġenti, sistemi ta' sorveljanza, meters intelliġenti jew printers

2.2.2. Sistemi tal-OT inklużi PLCs (Programmable Logic Controllers), pannelli SCADA jew gateways industrijali

2.2.3. Ħardwer ta' appoġġ, applikazzjonijiet ta' ġestjoni, u networks tal-komunikazzjoni użati minn dawn is-sistemi

2.3. Din il-politika tapplika fil-postijiet kollha tax-xogħol: ambjenti ta' uffiċċju, siti remoti, żoni tal-produzzjoni, u pjattaformi cloud li jinterfaċċjaw ma' dawn l-apparati.

3. Objettivi

3.1. Implimentazzjoni sigura: Tiżgura li s-sistemi kollha tal-IoT/OT jiġu kkonfigurati b'mod sigur qabel ma jiddaħħlu fl-ambjent operattiv.

3.2. Limitazzjoni tal-espożizzjoni: Tipprevjeni aċċess mhux awtorizzat, użu ħażin jew teħid tal-kontroll ta' apparati konnessi billi tapplika kontrolli b'saħħithom tal-aċċess u segmentazzjoni tan-network.

3.3. Monitoraġġ kontinwu: Iżżomm viżibbiltà fuq l-operazzjonijiet tal-IoT/OT permezz ta' logs tal-attività u monitoraġġ ta' mġiba mhux tas-soltu.

3.4. Responsabbiltà tal-fornituri: Tiżgura li fornituri terzi jsegwu prattiki siguri ta' installazzjoni, konfigurazzjoni u manutenzjoni.

3.5. Konformità regolatorja: Turi allinjament sħiħ ma' standards applikabbli bħal ISO 27001, il-GDPR (jekk tinġabar data personali), u n-NIS2 għar-reżiljenza tal-infrastruttura kritika.

4. Rwoli u responsabbiltajiet

4.1. Maniġer Ġenerali (GM)

4.1.1. Iġorr ir-responsabbiltà ġenerali għas-sigurtà tas-sistemi tal-IoT u l-OT

4.1.2. Japprova din il-politika u jiżgura li tiġi applikata fl-oqsma kollha tax-xogħol

4.1.3. Jivverifika li l-fornituri u l-kuntratturi jsegwu prattiki siguri ta' installazzjoni u manutenzjoni

4.1.4. Jawtorizza l-aċċess għan-network għal kull sistema tal-IoT/OT

4.2. Impjegat maħtur jew Maniġer tal-Operazzjonijiet (jekk maħtur)

4.2.1. Jissorvelja l-inventarju, il-pożizzjonament u l-konfigurazzjoni tal-apparati tal-IoT/OT

4.2.2. Jirreġistra l-post ta' kull apparat, l-assenjazzjoni tan-network, u d-dokumentazzjoni ta' appoġġ

4.2.3. Jiżgura li kull bidla (eż. aġġornamenti tal-firmware jew sostituzzjonijiet ta' apparati) tiġi dokumentata

[... 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 trid tiġi rieżaminata mill-inqas darba fis-sena mill-GM

9.1.2. Ir-rieżami jrid jivvaluta jekk il-politika għadhiex effettiva, jekk tkoprix it-tipi attwali ta' apparati, u jekk hijiex allinjata ma' riskji jew teknoloġiji ġodda

9.2. Aġġornamenti bbażati fuq skattaturi

9.2.1. Aġġornamenti tal-politika jridu jinbdew ukoll meta:

9.2.2. Jiddaħħlu tipi ġodda ta' sistemi tal-IoT jew tal-OT

9.2.3. Il-fornituri joħorġu avviżi dwar theddid jew noti ta' tmiem il-ħajja

9.2.4. Inċident jew awditjar jidentifika lakuni fil-kontrolli tal-IoT/OT

9.2.5. Liġijiet jew standards ġodda jistabbilixxu rekwiżiti addizzjonali

9.3. Dokumentazzjoni u kontroll tal-verżjoni

9.3.1. L-aġġornamenti kollha jridu jiġu dokumentati, inklużi d-data, in-numru tal-verżjoni, u sommarju tat-tibdiliet

9.3.2. Il-GM irid iżomm verżjonijiet storiċi tal-politika għal finijiet ta' awditjar

9.4. Komunikazzjoni tat-tibdiliet

9.4.1. Kwalunkwe aġġornament tal-politika għandu jinqasam mal-persunal u l-fornituri rilevanti kollha

9.4.2. Verżjonijiet aġġornati jridu jkunu aċċessibbli permezz ta' folders kondiviżi jew materjal stampat fis-siti tal-installazzjoni jew fiċ-ċentri tal-kontroll

10. Politiki relatati u rabtiet

10.1. Din il-politika trid tiġi implimentata b'allinjament mal-politiki SME relatati li ġejjin:

10.1.1. P4S – Politika dwar il-Kontroll tal-Aċċess: Tistabbilixxi kontrolli tal-login fil-livell tal-apparat, l-użu ta' passwords b'saħħithom, u proċeduri ta' aċċess awtorizzat għall-pjattaformi tal-IoT u l-OT

10.1.2. P9S – Politika dwar ix-Xogħol Remot: Tipprevjeni l-użu ta' aċċess remot għal dashboards tal-IoT/OT permezz ta' kanali mhux siguri jew mhux approvati

10.1.3. P17S – Politika dwar il-Protezzjoni tad-Data u l-Privatezza: Tapplika jekk apparati tal-IoT (eż. kameras tas-sigurtà) jipproċessaw jew jirreġistraw data personali, u tiżgura konformità mal-GDPR

10.1.4. P30S – Politika dwar ir-Rispons għall-Inċidenti: Tiddefinixxi proċeduri għas-sejbien, ir-rappurtar u r-riżoluzzjoni ta' inċidenti tal-IoT jew tal-OT, inkluż tbagħbis suspettat jew falliment operattiv

10.1.5. P36S – Politika dwar il-Midja Soċjali u l-Komunikazzjonijiet Esterni: Tiżgura li l-ebda informazzjoni dwar apparati jew tqassim tan-network ma tinqasam esternament sakemm ma tkunx approvata

10.2. Kull politika relatata ssaħħaħ l-applikazzjoni u l-użu prattiku ta' din il-politika billi tipprovdi gwida proċedurali mmirata.

11. Standards u oqfsa ta' referenza

11.1. ISO/IEC 27001

11.1.1. Klawżola 6.1 – Identifikazzjoni u trattament tar-riskju: Teħtieġ li r-riskji relatati mas-sistemi tal-IoT u l-OT jiġu evalwati u mitigati b'mod sistematiku

11.1.2. Klawżola 8.1 – Ippjanar u kontroll operattiv: Tiżgura kontroll operattiv sigur fuq apparati konnessi

11.2. ISO/IEC 27002

11.2.1. Kontroll 5.23 – Sigurtà tal-Informazzjoni għall-Użu tat-Teknoloġija Operattiva: Jiddefinixxi użu sigur tal-OT f'ambjenti fiżiċi u diġitali

11.2.2. Kontroll 5.31 – Konfigurazzjoni Sigura tas-Sistemi tal-Informazzjoni: Jeħtieġ konfigurazzjonijiet imsaħħa għall-apparati tal-IoT/OT u l-evitar ta' defaults mhux siguri

11.3. NIST SP 800-53 Rev.5

11.3.1. SI-7 – Integrità tas-Software, il-Firmware, u l-Informazzjoni: Jeħtieġ verifika tal-integrità tal-firmware u tal-aġġornamenti

11.3.2. CM-7 – L-inqas funzjonalità meħtieġa: L-apparati ma għandhomx ikollhom karatteristiċi mhux użati jew mhux siguri attivati

11.3.3. AC-6 – Inqas privileġġ: L-aċċess għall-apparat irid ikun limitat għal utenti awtorizzati biss

11.3.4. PE-20 – Monitoraġġ tal-assi: Monitoraġġ fiżiku u operattiv tal-assi tal-IoT u l-OT

11.3.5. SC-7 – Protezzjoni tal-konfini: Segmentazzjoni u kontroll tal-komunikazzjonijiet tan-network għal sistemi konnessi

11.4. GDPR tal-UE (2016/679)

11.4.1. Artikolu 32 – Sigurtà tal-ipproċessar: Jekk tinġabar data personali (eż. permezz ta' kameras ta' sorveljanza), l-organizzazzjoni trid timplimenta miżuri tekniċi u organizzattivi (TOMs) xierqa biex tipproteġi tali pproċessar

11.5. Direttiva NIS2 tal-UE (2022/2555)

11.5.1. Artikolu 21(2)(a) – Miżuri ta' ġestjoni tar-riskju

11.5.2. Artikolu 21(2)(d) – Konfigurazzjoni u użu siguri tal-apparati

11.5.3. Artikolu 21(2)(f) – Sigurtà tal-katina tal-provvista u tas-sistemi

11.6. DORA tal-UE (2022/2554)

11.6.1. Artikolu 9(2) – Kamp ta' applikazzjoni tal-ġestjoni tar-riskju tal-ICT: Jinkludi apparati industrijali u embedded użati f'ambjenti operattivi

11.6.2. Artikolu 10(1) – Kontinwità tal-ICT: Jeħtieġ li l-konfigurazzjonijiet tal-apparati jappoġġjaw ir-reżiljenza u l-operazzjonijiet ta' rkupru

11.7. COBIT 2019

11.7.1. DSS01 – Ġestjoni tal-operazzjonijiet: Japplika għas-sorveljanza tal-operazzjonijiet tat-teknoloġija, inklużi apparati fiżiċi

11.7.2. DSS05 – Ġestjoni tas-servizzi tas-sigurtà: Jiżgura li s-sistemi konnessi jiġu mmonitorjati u protetti kif suppost

11.7.3. APO13 – Ġestjoni tas-sigurtà: Isaħħaħ il-politiki għall-protezzjoni tal-assi operattivi fl-SMEs