| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Daħħal hawn l-isem tal-entità ġuridika rreġistrata | | | | | | |
| Numru tad-dokument:<br>P02S | | | | | Titlu tad-dokument:<br>**Politika P02S dwar ir-Rwoli u r-Responsabbiltajiet tal-Governanza** | | | | | | |
| Verżjoni:<br>1.0 | | Data tad-dħul fis-seħħ:<br>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 5 | |
| ISO/IEC 27002:2022 | Kontrolli: 5.2, 5.3, 5.4 | |
| NIST SP 800-53 Rev.5 | PM-1, PL-1, PL-4, CA-1, AC-1 | |
| GDPR tal-UE | Artikoli 5(2), 32 | |

**1. Għan**

1.1 Din il-politika tistabbilixxi kif ir-responsabbiltajiet tal-governanza għas-sigurtà tal-informazzjoni jiġu assenjati, delegati u ġestiti fl-organizzazzjoni, sabiex tiġi żgurata konformità sħiħa ma’ ISO/IEC 27001:2022 u ma’ obbligi regolatorji oħra.

1.2 Tiżgura responsabilità ċara f’kull livell u tappoġġa l-effettività operattiva billi tidentifika b’mod ċar min hu responsabbli għal kull funzjoni relatata mas-sigurtà.

1.3 Din il-politika ssaħħaħ il-kapaċità tal-organizzazzjoni li turi konformità waqt l-awditjar u ssaħħaħ il-fiduċja tal-klijenti billi turi governanza formali tas-sigurtà, anke f’organizzazzjonijiet b’persunal tekniku limitat jew b’servizzi tal-IT esternalizzati.

**2. Kamp ta’ applikazzjoni**

**2.1 Din il-politika tapplika għall-individwi kollha li jimmaniġġjaw sistemi jew data tal-organizzazzjoni, inklużi:**

2.1.1 Sidien tan-negozju u maniġers ġenerali

2.1.2 Impjegati u kuntratturi

2.1.3 Fornituri esterni ta’ servizzi tal-IT jew konsulenti

**2.2 Tkopri s-sistemi, l-ambjenti u s-servizzi kollha użati biex jipproċessaw, jittrasmettu jew jaħżnu informazzjoni tan-negozju jew tal-klijenti, inklużi:**

2.2.1 Infrastruttura tal-IT tal-uffiċċju u apparat għax-xogħol mill-bogħod

2.2.2 Pjattaformi cloud u servizzi tal-email

2.2.3 Reġistri fiżiċi u drives kondiviżi

2.3 Il-kamp ta’ applikazzjoni jinkludi kemm attivitajiet interni kif ukoll attivitajiet esternalizzati li jinvolvu l-governanza tas-sigurtà tal-informazzjoni.

**3. Objettivi**

3.1 Tistabbilixxi responsabilità ċara għad-dmirijiet kollha relatati mas-sigurtà, inklużi l-ġestjoni tal-politiki, il-kontroll tal-aċċess, il-ġestjoni tal-inċidenti u l-monitoraġġ.

3.2 Tippermetti separazzjoni effettiva tad-dmirijiet biex jitnaqqsu kunflitti ta’ interess jew riskji ta’ frodi.

3.3 Tiżgura li l-kompiti u r-rwoli tas-sigurtà jkunu dokumentati b’mod ċar u rieżaminati regolarment.

3.4 Tippermetti teħid ta’ deċiżjonijiet infurmati, eskalazzjoni u sorveljanza tar-riskji tal-IT u tas-sigurtà.

3.5 Tappoġġa ċ-ċertifikazzjoni ISO/IEC 27001:2022 u ssaħħaħ il-fiduċja fost il-klijenti, l-imsieħba u l-awdituri.

**4. Rwoli u responsabbiltajiet**

**4.1 Maniġer Ġenerali / Sid tan-Negozju**

4.1.1 Għandu r-responsabbiltà aħħarija għall-implimentazzjoni u s-sorveljanza ta’ din il-politika.

4.1.2 Japprova r-rwoli, ir-responsabbiltajiet u d-deċiżjonijiet kollha relatati mad-delega fil-qasam tas-sigurtà.

4.1.3 Jissorvelja l-konformità u jieħu d-deċiżjonijiet finali dwar eċċezzjonijiet għall-politika u eskalazzjonijiet.

**4.2 Koordinatur tas-Sigurtà Maħtur (jekk jinħatar)**

4.2.1 Jista' jkun membru tal-persunal jew konsulent ta' fiduċja.

4.2.2 Dan ir-rwol jista' jitwettaq mill-Maniġer Ġenerali jew minn fornitur estern f'ambjenti ta' mikrointrapriżi.

4.2.3 Jassisti fl-applikazzjoni ta' kuljum tal-kontroll tal-aċċess, tar-rispons għall-inċidenti jew ta' kompiti bażiċi ta' sigurtà teknika.

4.2.4 Jirrapporta direttament lill-Maniġer Ġenerali dwar kwalunkwe kwistjoni jew riskju tas-sigurtà.

[ ... 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 rieżaminata mill-Maniġer Ġenerali kull 12-il xahar biex jiġi żgurat li tibqa' tirrifletti l-obbligi legali, il-ħtiġijiet operattivi u r-rekwiżiti taċ-ċertifikazzjoni ISO/IEC 27001.

**9.2 Rieżamijiet Interim**

**9.2.1 Ir-rieżamijiet għandhom isiru wkoll meta:**

9.2.1.1 Ikun hemm bidliet organizzattivi maġġuri

9.2.1.2 Jiġi onboardjat fornitur ġdid

9.2.1.3 Jseħħ inċident serju tas-sigurtà

9.2.1.4 Jiġu aġġornati regolamenti bħall-GDPR, in-NIS2 jew id-DORA

**9.3 Kontroll tal-Verżjoni u Dokumentazzjoni**

**9.3.1 Ir-rieżamijiet kollha għandhom jinkludu:**

9.3.1.1 Id-data tar-rieżami

9.3.1.2 Sommarju ta' kwalunkwe bidla

9.3.1.3 Firma jew approvazzjoni dokumentata mill-Maniġer Ġenerali

9.3.1.4 Verżjonijiet preċedenti arkivjati għal referenza ta' awditjar

**9.4 Komunikazzjoni tal-Bidliet**

9.4.1 L-aġġornamenti kollha tal-politika għandhom jiġu kkomunikati minnufih lill-persunal u lill-fornituri permezz ta' email, portali interni jew memoranda formali.

**10. Politiki relatati u rabtiet bejniethom**

**10.1 Din il-politika għandha tiġi implimentata flimkien mal-politiki SME li ġejjin sabiex tkun effettiva bis-sħiħ:**

10.1.1 P4S – Politika tal-Kontroll tal-Aċċess: Tistabbilixxi kif jingħata, jiġi ġestit u jiġi rtirat l-aċċess, b'rabta diretta mar-rwoli assenjati u mas-sorveljanza.

10.1.2 P8S – Politika dwar l-Għarfien u t-Taħriġ fis-Sigurtà tal-Informazzjoni: Issaħħaħ ir-responsabbiltajiet u l-aspettattivi speċifiċi għar-rwol.

10.1.3 P17S – Politika dwar il-Protezzjoni tad-Data u l-Privatezza: Tiddeskrivi d-dmirijiet legali taħt il-GDPR, li jiġu assenjati lir-rwoli definiti f'din il-politika ta' governanza.

10.1.4 P30S – Politika tar-Rispons għall-Inċidenti: Teħtieġ responsabbiltajiet definiti għar-rappurtar, l-eskalazzjoni u r-riżoluzzjoni tal-inċidenti.

10.2 Flimkien, dawn il-politiki jippermettu applikazzjoni konsistenti, responsabilità interna u konformità esterna.

## 11. Standards u oqfsa ta' referenza

### 11.1 ISO/IEC 27001

11.1.1 Klawżola 5.3 – Ir-rwoli, ir-responsabbiltajiet u l-awtoritajiet organizzattivi: Teħtieġ li r-rwoli jiġu assenjati b'mod ċar u appoġġati mill-ogħla tmexxija.

### 11.2 ISO/IEC 27002

11.2.1 Kontrolli 5.2–5.4: Jeħtieġu dokumentazzjoni ċara tar-rwoli tas-sigurtà tal-informazzjoni, separazzjoni tad-dmirijiet u sorveljanza maniġerjali.

### 11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1: Jistabbilixxi programm ġenerali tas-sigurtà tal-informazzjoni b'responsabbiltajiet definiti.

11.3.2 PL-1 sa PL-4: Jeħtieġu kontrolli ta' ppjanar, inklużi l-formulazzjoni tal-politika u assenjazzjonijiet ta' rwoli dokumentati.

11.3.3 CA-1: Jeħtieġ rwoli definiti għall-evalwazzjoni u l-awtorizzazzjoni.

11.3.4 AC-1: Jorbot il-kontroll tal-aċċess ibbażat fuq ir-rwoli mar-responsabbiltajiet ta' governanza assenjati.

### 11.4 GDPR tal-UE

11.4.1 Artikolu 5(2) – Responsabilità: Jeħtieġ li l-organizzazzjonijiet juru l-konformità permezz tar-rwoli u r-responsabbiltajiet.

11.4.2 Artikolu 32 – Sigurtà tal-ipproċessar: Jenfasizza l-assenjazzjoni ċara tad-dmirijiet biex tiġi protetta d-data personali.

### 11.5 NIS tal-UE

11.5.1 Artikolu 21(2)(a): Jeħtieġ strutturi ta' governanza li jinkludu rwoli formalizzati għall-ġestjoni tar-riskju ċibernetiku u tal-inċidenti.

### 11.6 DORA tal-UE

11.6.1 Artikoli 9 u 10: Jeħtieġu li entitajiet finanzjarji jassenjaw u jissorveljaw b'mod ċar ir-responsabbiltajiet relatati mal-ICT u mas-sigurtà.

### 11.7 COBIT 2019

11.7.1 EDM03 – Żgurar tal-ottimizzazzjoni tar-riskju: Jeħtieġ rwoli definiti sew u mogħdijiet ta' eskalazzjoni għall-ġestjoni tar-riskju tas-sigurtà.

11.7.2 APO13 – Ġestjoni tas-sigurtà: Jassenja dmirijiet strateġiċi u operattivi tas-sigurtà lil individwi u rwoli.

11.7.3 DSS05 – Ġestjoni tas-servizzi tas-sigurtà: Jeħtieġ struttura u traċċabbiltà fir-responsabbiltajiet għal servizzi tas-sigurtà esterni u interni.