| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Daħħal hawn l-isem tal-entità ġuridika rreġistrata | | | | | | | |
| Numru tad-dokument:<br>P01 | | | | | Titlu tad-dokument:<br>**Politika tas-Sigurtà tal-Informazzjoni** | | | | | | | |
| 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** |
| | | | |
| | | | |

## 1. Għan

1.1 Din il-politika tistabbilixxi l-impenn ġenerali tal-organizzazzjoni għas-sigurtà tal-informazzjoni permezz tal-istabbiliment ta' Sistema ta' Ġestjoni tas-Sigurtà tal-Informazzjoni (ISMS) formali.

1.2 Tipprovdi d-direzzjoni strateġika u r-rekwiżiti fundamentali għall-protezzjoni tal-kunfidenzjalità, l-integrità, id-disponibbiltà u r-reżiljenza tal-assi kollha tal-informazzjoni f'ambjenti fiżiċi, diġitali u fil-cloud.

1.3 Din il-politika tissodisfa l-Klawżola 5.2 u l-Klawżola 5.1 tal-ISO/IEC 27001:2022 billi tesprimi l-intenzjoni tat-tmexxija, l-impenn tal-ogħla ġestjoni u l-allinjament tal-attivitajiet ta' sigurtà mal-objettivi organizzattivi.

1.4 Isservi bħala r-referenza awtorevoli għall-politiki, standards u proċeduri subordinati kollha fi ħdan l-ISMS u hija essenzjali biex tippermetti ambjent ta' sigurtà bbażat fuq ir-riskju, immexxi mill-konformità u soġġett għal titjib kontinwu.

## 2. Kamp ta' applikazzjoni

**2.1 Din il-politika tapplika għall-individwi, l-assi u l-proċessi kollha ddefiniti fil-kamp ta' applikazzjoni tal-ISMS, inklużi:**

2.1.1 L-unitajiet tan-negozju, id-dipartimenti, is-sussidjarji u l-fergħat kollha

2.1.2 L-impjegati, il-kuntratturi, il-persunal temporanju, il-konsulenti u l-forniturі ta' servizzi ta' partijiet terzi

2.1.3 Id-data, is-sistemi tal-informazzjoni, l-applikazzjonijiet, l-infrastruttura u l-kanali ta' komunikazzjoni kollha

2.1.4 L-ambjenti fiżiċi, fil-cloud, remoti u ibridi kollha fejn tiġi pproċessata jew aċċessata d-data tal-kumpanija

2.2 Il-politika hija vinkolanti għall-entitajiet kollha li jimmaniġġjaw l-informazzjoni organizzattiva u tapplika għall-istadji kollha taċ-ċiklu tal-ħajja tal-informazzjoni — mill-ħolqien u t-trażmissjoni sal-ħażna u r-rimi.

2.3 Kwalunkwe esklużjoni jew limitazzjoni minn dan il-kamp ta' applikazzjoni għandha tiġi dokumentata fid-dikjarazzjoni tal-kamp ta' applikazzjoni tal-ISMS u ġġustifikata b'approvazzjoni formali mill-ġestjoni eżekuttiva.

## 3. Objettivi

3.1 Jiġi stabbilit ISMS li jkun konsistenti mal-ISO/IEC 27001:2022 u kapaċi jappoġġa teħid ta' deċiżjonijiet ibbażat fuq ir-riskju fl-organizzazzjoni kollha.

3.2 Jiġi żgurat li l-prinċipji tas-sigurtà tal-kunfidenzjalità, l-integrità u d-disponibbiltà jkunu integrati fl-attivitajiet, is-sistemi u s-sħubijiet organizzattivi kollha.

3.3 Tippermetti l-konformità regolatorja u kuntrattwali billi tiddefinixxi objettivi ta' sigurtà li jistgħu jitkejlu u li huma mmexxija mill-politika, u billi tintegrahom fl-operat tan-negozju.

3.4 Titnaqqas il-probabbiltà u l-impatt ta' inċidenti tas-sigurtà tal-informazzjoni permezz ta' kontrolli preventivi, ta' skoperta u korrettivi effettivi.

3.5 Jitmexxa titjib kontinwu fil-maturità tas-sigurtà tal-informazzjoni permezz ta' indikaturi ta' prestazzjoni ddefiniti, riżultati tal-awditjar u rieżamijiet tal-ġestjoni.

3.6 Tiġi promossa kultura ta' responsabbiltà, għarfien u reżiljenza fejn ir-responsabbiltajiet tas-sigurtà jinftiehmu u jitwettqu mill-persunal kollu.

## 4. Rwoli u responsabbiltajiet

**4.1 Ġestjoni Eżekuttiva**

4.1.1 Tapprova u tappoġġja l-Politika tas-Sigurtà tal-Informazzjoni u l-qafas tal-ISMS.

4.1.2 Tiżgura l-allinjament bejn l-objettivi tas-sigurtà u l-istrateġija tan-negozju.

4.1.3 Tagħti eżempju u tippromwovi kultura b'saħħitha tas-sigurtà tal-informazzjoni.

4.1.4 Tirrieżamina u tapprova bidliet ewlenin fil-kamp ta’ applikazzjoni tal-ISMS, fit-trattament tar-riskju u fl-istruttura ta’ governanza.

**4.2 Direttur tas-Sigurtà tal-Informazzjoni (CISO) / Maniġer tal-ISMS**

4.2.1 Huwa responsabbli għall-ISMS u jiżgura li din il-politika tibqa’ konformi mal-ISO/IEC 27001.

4.2.2 Imexxi l-evalwazzjoni tar-riskju, l-implimentazzjoni tal-kontrolli u l-proċessi ta’ titjib kontinwu.

4.2.3 Jiżgura l-koordinazzjoni bejn funzjonijiet differenti tal-isforzi tas-sigurtà u jissorvelja l-politiki subordinati.

4.2.4 Jirrapporta lit-tmexxija eżekuttiva dwar l-istatus tal-ISMS, l-inċidenti, ir-riżultati tal-awditjar u l-metriċi.

4.2.5 Jiżgura li r-rieżamijiet u l-aġġornamenti tal-politika jitwettqu skont it-Taqsima 9 ta’ dan id-dokument.

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

**9. Rekwiżiti ta’ rieżami u aġġornament**

**9.1 Frekwenza tar-rieżami**

**9.1.1 Din il-politika għandha tiġi rieżaminata mill-inqas darba fis-sena jew meta jseħħ xi wieħed mill-fatturi li ġejjin:**

9.1.1.1 Bidliet sinifikanti fl-obbligi legali, regolatorji jew kuntrattwali

9.1.1.2 Bidliet materjali fil-profil tar-riskju tal-organizzazzjoni

9.1.1.3 Riżultati minn awditi interni jew esterni

9.1.1.4 Inċidenti ewlenin jew fallimenti tal-kontrolli

**9.2 Awtorità u proċess tar-rieżami**

9.2.1 Is-CISO jew il-Maniġer tal-ISMS maħtur għandu jmexxi l-proċess ta’ rieżami.

**9.2.2 L-inputs għar-rieżami għandhom jinkludu:**

9.2.2.1 Riżultati tal-awditjar intern

9.2.2.2 Xejriet tal-evalwazzjoni tar-riskju

9.2.2.3 Bidliet fil-proċessi tan-negozju u fit-teknoloġija

9.2.2.4 Prestazzjoni kontra KPIs u limiti tar-riskju

**9.2.3 L-aġġornamenti kollha għandhom:**

9.2.3.1 Ikunu soġġetti għal kontroll tal-verżjonijiet u dokumentati

9.2.3.2 Ikunu approvati mill-Ġestjoni Eżekuttiva

9.2.3.3 Jitqassmu lill-partijiet kollha affettwati permezz ta’ kanali uffiċjali ta’ komunikazzjoni

9.2.3.4 Jattivaw l-aġġornamenti meħtieġa għad-dokumentazzjoni subordinata u għat-taħriġ

**10. Politiki relatati u rabtiet**

**10.1 Din il-politika bażika hija marbuta direttament mal-politiki u l-oqfsa organizzattivi tas-sigurtà li ġejjin:**

10.1.1 P2 – Politika dwar ir-Rwoli u r-Responsabbiltajiet ta’ Governanza: Tiddefinixxi l-istruttura ta’ governanza u l-ġerarkija tal-awtorità msemmija f’dan id-dokument.

10.1.2 P3 – Politika dwar l-Użu Aċċettabbli: Tiżgura l-konformità fl-imġiba u l-immaniġġjar aċċettabbli tal-assi tal-informazzjoni.

10.1.3 P4 – Politika tal-Kontroll tal-Aċċess: Toperazzjonalizza l-kontrolli relatati mal-aċċess li joħorġu minn din il-politika ġenerali.

10.1.4 P6 – Politika tal-Ġestjoni tar-Riskju: Tipprovdi l-kuntest ibbażat fuq ir-riskju għall-għażla tal-kontrolli u l-aċċettazzjoni tar-riskji residwi.

10.1.5 P33 – Politika tal-Monitoraġġ, l-Awditjar u l-Konformità: Tiddettalja kif il-mekkaniżmi interni ta' assigurazzjoni jivverifikaw l-applikazzjoni tal-politika.

10.2 Dawn l-interdipendenzi jiżguraw allinjament komprensiv u traċċabbiltà fl-ISMS kollu u jappoġġjaw governanza unifikata tar-riskju u tal-konformità.

## 11. Standards u oqfsa ta' referenza

11.1 Din il-Politika tas-Sigurtà tal-Informazzjoni hija formalment allinjata mal-istandards u l-oqfsa li ġejjin biex tiżgura konformità sħiħa, tħejjija għall-awditjar u difensibbiltà regolatorja:

### 11.2 ISO/IEC 27001

11.2.1 Klawżola 5.1 – Tmexxija u Impenn: Din il-politika turi l-impenn tal-ogħla ġestjoni għas-sigurtà tal-informazzjoni u tiddefinixxi r-responsabbiltajiet u l-allokazzjoni tar-riżorsi għall-ISMS.

11.2.2 Klawżola 5.2 – Politika tas-Sigurtà tal-Informazzjoni: Dan id-dokument iservi bħala l-politika formali tas-sigurtà tal-organizzazzjoni, allinjata mal-objettivi ta' sigurtà ddikjarati, mal-istrateġija tan-negozju u mal-konformità mal-ISO/IEC 27001.

11.2.3 Klawżola 6.1 – Azzjonijiet biex jiġu indirizzati r-riskji u l-opportunitajiet: L-approċċ ibbażat fuq ir-riskju rifless f'din il-politika jiżgura li r-riżorsi tas-sigurtà jiġu applikati b'mod proporzjonat għat-theddid.

11.2.4 Klawżola 9.2 – Awditjar Intern u Klawżola 10 – Titjib: Din il-politika hija integrata fiċ-ċiklu tal-ħajja tat-titjib kontinwu tal-organizzazzjoni u hija soġġetta għal verifika permezz tal-awditjar intern.

11.2.5 ISO/IEC 27002:2022 – Kontroll 5.1: Jispeċifika gwida għall-istabbiliment u ż-żamma ta' politiki tas-sigurtà. Din il-politika tirrifletti r-rakkomandazzjonijiet tal-ISO/IEC 27002 għal dokumentazzjoni ġerarkika, ċikli ta' rieżami u applikabbiltà.

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

11.3.1 PL-1 (Politika u Proċeduri għall-Ippjanar tas-Sigurtà): Din il-politika tissodisfa r-rekwiżit li tiġi żviluppata, ikkomunikata u rieżaminata politika formali tas-sigurtà tal-informazzjoni għall-organizzazzjoni kollha.

11.3.2 PM-1 sa PM-5: Tindirizza l-governanza fil-livell tal-programm, inklużi rwoli tas-sigurtà tal-informazzjoni, allokazzjoni tar-riżorsi, strateġija tar-riskju u integrazzjoni tal-ippjanar tas-sigurtà fl-operazzjonijiet tal-intrapriża.

### 11.4 GDPR tal-UE (2016/679)

11.4.1 Artikolu 5(2): Jinforza l-prinċipju ta' responsabbiltà. Din il-politika tiddefinixxi l-partijiet responsabbli u azzjonijiet ta' applikazzjoni traċċabbli.

11.4.2 Artikolu 24: Jeħtieġ l-implimentazzjoni ta' miżuri tekniċi u organizzattivi, inklużi politiki allinjati mar-riskju.

11.4.3 Artikolu 32: Jappoġġja l-implimentazzjoni ta' miżuri xierqa biex tiġi żgurata s-sigurtà tad-data personali tul iċ-ċiklu tal-ħajja tagħha.

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

11.5.1 Artikolu 21(2)(a): Jobbliga lill-entitajiet jimplimentaw politika tas-sigurtà dokumentata li tindirizza l-ġestjoni tar-riskju u l-governanza. Din il-politika tissodisfa dak ir-rekwiżit u tappoġġja tħejjija usa' għaċ-ċibersigurtà u l-protezzjoni tal-infrastruttura kritika.

### 11.6 DORA tal-UE (2022/2554)

11.6.1 Artikolu 5(2): Jeħtieġ qafas dokumentat ta' kontroll intern għall-ġestjoni tar-riskju tal-ICT. Din il-politika tappoġġja l-konformità tas-settur finanzjarju billi tassenja rwoli, kontrolli u funzjonijiet ta' sorveljanza allinjati mal-aspettattivi ta' governanza tad-DORA.

**11.7 COBIT 2019**

11.7.1 EDM01 – Stabbiliment tal-Qafas ta' Governanza: Din il-politika tappoġġja l-governanza tal-intrapriża billi tiddefinixxi r-rwoli tal-ISMS, l-impenji tat-tmexxija u l-objettivi strateġiċi.

11.7.2 APO01 – Qafas ta' Ġestjoni: Jappoġġja l-istabbiliment u t-tħaddim ta' ISMS strutturat.

11.7.3 APO12 – Ġestjoni tar-Riskju: Jipprovdi l-pedament għall-governanza tar-riskju tas-sigurtà tal-informazzjoni.

11.7.4 MEA01/MEA03 – Monitoraġġ, Evalwazzjoni u Valutazzjoni: Isaħħaħ l-evalwazzjoni kontinwa tal-prestazzjoni u l-monitoraġġ tal-kontroll intern permezz tal-applikazzjoni tal-konformità mal-politika.