| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Daħħal hawn l-isem tal-entità ġuridika rreġistrata | | | | | | | |
| Numru tad-dokument:<br>P18 | | | | | Titlu tad-dokument:<br>**Politika tal-Kontrolli Kriptografiċi** | | | | | | | |
| 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 8 | - |
| ISO/IEC 27002:2022 | Kontrolli 8.24, 8.25, 8 | - |
| NIST SP 800-53 Rev. 5 | SC-12 sa SC-17, SC-28, SC-28(1), SC-12(3) | - |
| GDPR tal-UE | Artikolu 32, Artikoli 33–34, Premessa 83 | - |
| Direttiva NIS2 tal-UE | Artikolu 21(2)(d) | - |
| DORA tal-UE | Artikoli 6(2)(d), 11(1)(c) | - |
| COBIT 2019 | DSS05.01, DSS06.06, MEA03 | - |

**1. Għan**

1.1 Din il-politika tiddefinixxi rekwiżiti obbligatorji għall-użu sigur u konformi tal-kontrolli kriptografiċi fl-organizzazzjoni kollha sabiex tiġi żgurata l-Kunfidenzjalità, l-Integrità, id-Disponibbiltà (CIA) u l-awtentiċità ta' informazzjoni sensittiva u regolata.

1.2 L-użu tal-kontrolli kriptografiċi jsaħħaħ il-fiduċja fl-operazzjonijiet tas-sigurtà tad-data, jappoġġa komunikazzjonijiet siguri, isaħħaħ il-kontroll tal-aċċess u jippermetti l-konformità regolatorja permezz ta' prattiki effettivi ta' ċifrar u ġestjoni taċ-ċwievet.

1.3 Din il-politika hija allinjata mal-ISO/IEC 27001:2022, Klawżola 8.1, u mal-Anness A, Kontroll 8.24, u tappoġġa obbligi legali u operattivi skont l-Artikolu 32 tal-GDPR, l-Artikolu 6(2)(d) tad-DORA u l-Artikolu 21 tan-NIS2. Tappoġġa wkoll l-objettivi tal-COBIT 2019 għas-servizzi tas-sigurtà u l-protezzjoni tal-assi tad-data.

**2. Kamp ta' applikazzjoni**

2.1 Din il-politika tapplika għall-unitajiet organizzattivi kollha, għall-funzjonijiet tan-negozju kollha, għall-persunal kollu u għall-forniturі terzi ta' servizzi involuti fl-użu, fl-amministrazzjoni jew fl-implimentazzjoni ta' għodod u metodi kriptografiċi.

2.2 L-ambjenti koperti jinkludu sistemi ta' produzzjoni, żvilupp, staging, backup u rkupru minn diżastru fejn data sensittiva tiġi trażmessa, ipproċessata jew maħżuna.

**2.3 Il-kamp ta' applikazzjoni jinkludi l-komponenti u l-każijiet ta' użu kriptografiċi kollha, inklużi iżda mhux limitati għal:**

2.3.1 Ċifrar simmetriku u asimmetriku

2.3.2 Firem diġitali u ċertifikati

2.3.3 Algoritmi ta' hashing

2.3.4 Ġenerazzjoni, distribuzzjoni u qerda siguri taċ-ċwievet

2.3.5 Transport Layer Security (TLS), ċifrar sħiħ tad-diska (FDE), u ċifrar fil-livell tal-API

2.3.6 Elementi siguri bħal Hardware Security Modules (HSMs), Trusted Platform Modules (TPMs), u Key Management Systems (KMS)

**2.4 Din il-politika tirregola l-użu tal-kontrolli kriptografiċi fir-rigward ta':**

2.4.1 Data kklassifikata bħala Kunfidenzjali, Kunfidenzjali Ħafna jew Regolata

2.4.2 Awtentikazzjoni u verifika ta' identitajiet diġitali

2.4.3 Komunikazzjonijiet siguri ma' partijiet esterni

2.4.4 Kustodja taċ-ċwievet u mekkaniżmi ta’ kontroll doppju

**3. Objettivi**

3.1 Jiġi żgurat li t-teknoloġiji kriptografiċi jintgħażlu, jiġu approvati, implimentati u miżmuma skont ir-riskju tan-negozju, standards internazzjonali u obbligi regolatorji.

3.2 Tistabbilixxi struttura ta’ governanza standardizzata għall-ġestjoni tas-servizzi kriptografiċi, inkluża responsabbiltà ċara għall-implimentazzjoni, il-verifika u l-ġestjoni tal-eċċezzjonijiet.

3.3 Tipprevjeni l-użu mhux awtorizzat, il-konfigurazzjoni ħażina jew l-obsolexxenza ta’ algoritmi u kontrolli kriptografiċi permezz ta’ proċess formali ta’ approvazzjoni u rieżami.

3.4 Tiżgura li l-kontrolli kriptografiċi jkunu integrati fil-fażi tad-disinn tas-sistema u vverifikati regolarment biex jiġi evitat esponiment tad-data, kompromess taċ-ċwievet jew degradazzjoni tal-protokolli.

3.5 Tapplika l-ġestjoni taċ-ċiklu tal-ħajja taċ-ċwievet kriptografiċi kollha, inklużi l-ġenerazzjoni, il-ħażna, l-użu, ir-rotazzjoni, ir-revoka u l-qerda sigura.

3.6 Tiżgura l-konformità ma’ regolamenti internazzjonali u reġjonali li jobbligaw iċ-ċifrar u l-immaniġġjar sigur tad-data, inklużi l-GDPR, id-DORA, in-NIS2 u l-COBIT 2019.

**4. Rwoli u responsabbiltajiet**

**4.1 Maniġer tas-Sigurtà tal-Informazzjoni / Uffiċjal Ewlieni tas-Sigurtà tal-Informazzjoni**

4.1.1 Huwa s-sid ta’ din il-politika u jiżgura l-allinjament tagħha mal-ISMS u mal-Anness A tal-ISO/IEC 27001, Kontroll 8.24.

4.1.2 Japprova l-użu ta’ algoritmi u kontrolli kriptografiċi u jiżgura l-konformità fl-organizzazzjoni kollha.

**4.2 Responsabbli għall-Operazzjonijiet Kriptografiċi / Perit tas-Sigurtà**

4.2.1 Jiġġestixxi l-operazzjonijiet ta’ kuljum u l-amministrazzjoni tas-sistemi kriptografiċi.

4.2.2 Iżomm il-Lista tal-Metodi Kriptografiċi Approvati (ACML) u r-Reġistru tal-Ġestjoni taċ-Ċwievet.

4.2.3 Iwettaq Rieżamijiet tad-Disinn Kriptografiku (CDRs) u jevalwa teknoloġiji kriptografiċi ġodda.

[ ... 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 riveduta kull sena mill-Maniġer tas-Sigurtà tal-Informazzjoni u mir-Responsabbli għall-Operazzjonijiet Kriptografiċi.

**9.2 L-attivaturi tar-rieżami jinkludu:**

9.2.1 Skoperta ta’ vulnerabbiltajiet kriptografiċi (eż. algorithm downgrade, attakki kwantiċi)

9.2.2 Bidliet regolatorji li jeħtieġu standards aġġornati taċ-ċifrar

9.2.3 Sejbiet operattivi jew tal-awditjar li jiżvelaw lakuni fil-politika

9.2.4 Aġġornamenti ta’ għodod kriptografiċi jew bidliet fl-arkitettura

**9.3 L-aġġornamenti għandhom ikunu taħt kontroll tal-verżjoni fir-Reġistru tal-Kontroll tad-Dokumenti tal-ISMS u kkomunikati lil:**

9.3.1 L-amministraturi kollha b’rwoli ta’ aċċess kriptografiku

9.3.2 Timijiet tal-iżvilupp u responsabbli DevSecOps

9.3.3 Fornituri terzi taħt obbligi kuntrattwali ta’ ċifrar

9.4 It-tim tal-ISMS għandu jiżgura li verżjonijiet sostitwiti jiġu arkivjati u ma jibqgħux jiġu riferuti fil-proċeduri operattivi.

**10. Politiki relatati u rabtiet**

10.1 P1 - Politika tas-Sigurtà tal-Informazzjoni. Tipprovdi l-governanza bażika għall-miżuri kollha tas-sigurtà, inkluża l-applikazzjoni tal-kontrolli kriptografiċi, il-protezzjoni tal-assi u komunikazzjonijiet siguri.

10.2 P4 - Politika dwar il-Kontroll tal-Aċċess. Tiżgura li l-aċċess loġiku għal materjal kriptografiku u għal sistemi ta' ġestjoni taċ-ċifrar ikun limitat b'mod strett skont il-prinċipju tal-inqas privileġġ u s-separazzjoni tad-dmirijiet.

10.3 P6 - Politika tal-Ġestjoni tar-Riskju. Tappoġġa l-evalwazzjoni tar-riskji tal-kontrolli kriptografiċi u tiddokumenta l-istrateġija tat-trattament tar-riskju għal eċċezzjonijiet, obsolexxenza ta' algoritmi jew xenarji ta' kompromess taċ-ċwievet.

10.4 P12 - Politika tal-Ġestjoni tal-Assi. Tobbliga l-klassifikazzjoni ta' data sensittiva u assi tal-hardware, li tiddetermina direttament ir-rekwiżiti kriptografiċi u l-obbligi tal-kustodja taċ-ċwievet.

10.5 P13 - Politika tal-Klassifikazzjoni u t-Tikkettar tad-Data. Tiddefinixxi l-livelli ta' klassifikazzjoni (eż. Kunfidenzjali, Regolata) li jattivaw rekwiżiti speċifiċi ta' ċifrar għal data fi tranżitu u data maħżuna.

10.6 P14 - Politika taż-Żamma u r-Rimi tad-Data. Tispeċifika proċeduri għar-rimi sigur ta' mezzi ta' ħażna iċċifrati u ta' materjal kriptografiku taċ-ċwievet fit-tmiem tal-ħajja.

10.7 P30 - Politika dwar ir-Rispons għall-Inċidenti. Tiddeskrivi l-istrateġija tal-organizzazzjoni għar-rispons għal kompromess taċ-ċwievet, użu ħażin taċ-ċertifikati jew vulnerabbiltajiet algoritmiċi suspettati, inklużi revoka rapida u rappurtar ta' ksur.

## 11. Standards u oqfsa ta' referenza

### 11.1 ISO/IEC 27001

11.1.1 Klawżola 8.1 - Ippjanar u Kontroll Operattiv: Tapplika kontrolli tekniċi tas-sigurtà, inklużi miżuri kriptografiċi, bħala parti mis-salvagwardji operattivi.

### 11.2 ISO/IEC 27002:2022

11.2.1 Kontrolli 8.24, 8.25, 8: Tipprovdi gwida għall-implimentazzjoni dwar l-objettivi tal-kontrolli kriptografiċi, l-għażla tal-algoritmi, l-applikazzjoni tal-protokolli u l-ġestjoni taċ-ċiklu tal-ħajja taċ-ċertifikati.

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

11.3.1 SC-12 - Stabbiliment taċ-Ċwievet Kriptografiċi: Jiżgura ġenerazzjoni u skambju siguri taċ-ċwievet taċ-ċifrar. Il-P18 tiddefinixxi kif għandhom jiġu ġġenerati u skambjati ċ-ċwievet simmetriċi/asimmetriċi bl-użu ta' algoritmi u protokolli approvati.

11.3.2 SC-13 - Protezzjoni Kriptografika: Tobbliga l-użu tal-kontrolli kriptografiċi biex tipproteġi l-kunfidenzjalità u l-integrità tal-informazzjoni. Il-P18 tapplika ċ-ċifrar għal data maħżuna u data fi tranżitu skont il-klassifikazzjoni tad-data, bi standards tal-algoritmi allinjati man-NIST FIPS 140-3.

11.3.3 SC-17 - Ċertifikati tal-Public Key Infrastructure (PKI): Teħtieġ l-implimentazzjoni ta' PKI biex tappoġġa l-awtentikazzjoni u l-firem diġitali. Il-P18 tiddeskrivi l-użu tal-PKI biex jiġu ssigurati komunikazzjonijiet, identitajiet tas-sistema u aċċess amministrattiv.

11.3.4 SC-28, SC-28(1) - Protezzjoni tal-Informazzjoni Meta Maħżuna u fi Tranżitu: Teħtieġ ċifrar tad-data meta tkun maħżuna jew trażmessa fuq netwerks mhux fdati. Il-P18 tispeċifika l-applikazzjoni ta' TLS, VPN tunnels, ċifrar sħiħ tad-diska u metodi siguri ta' ħażna għal data sensittiva.

11.3.5 SC-12(3) - Ġenerazzjoni ta' Ċwievet Simmetriċi għal Ħażna u Distribuzzjoni Siguri: Tiffoka fuq il-ġenerazzjoni u l-immaniġġjar siguri ta' ċwievet simmetriċi. Il-P18 tobbliga l-użu ta' ġeneraturi b'saħħithom ta' numri każwali, politiki ta' rotazzjoni taċ-ċwievet u vaults siguri taċ-ċwievet għal operazzjonijiet kriptografiċi.

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

11.4.1 Artikolu 32 - Sigurtà tal-Ipproċessar: Jirrakkomanda b'mod espliċitu ċ-ċifrar bħala miżura għat-tnaqqis tar-riskju għal data personali.

11.4.2 Premessa 83: Tenfasizza ċ-ċifrar bħala kontroll biex jiġi evitat aċċess mhux awtorizzat għad-data.

11.4.3 Artikoli 33 u 34: Iċ-ċifrar jista' jeżenta lill-organizzazzjonijiet minn notifiki obbligatorji ta' ksur jekk ikun effettiv.

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

11.5.1 Artikolu 21(2)(d): Jeħtieġ miżuri tekniċi u organizzattivi, inklużi protezzjonijiet kriptografiċi, biex tinżamm id-disponibbiltà u l-integrità tas-servizz.

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

11.6.1 Artikolu 6(2)(d): L-istituzzjonijiet finanzjarji għandhom jiżguraw id-data, inkluż permezz ta' ċifrar b'saħħtu ta' informazzjoni kritika.

11.6.2 Artikolu 11(1)(c): Jobbliga kontrolli siguri tal-ipproċessar tad-data għal forniturі terzi ta' servizzi tal-ICT.

**11.7 COBIT 2019**

11.7.1 DSS05.01 - Ipproteġi l-Assi tal-Informazzjoni: Jeħtieġ l-użu taċ-ċifrar u tal-ġestjoni taċ-ċwievet biex tiġi salvagwardjata d-data kontra aċċess mhux awtorizzat.

11.7.2 DSS06.06 - Ittestjar tas-Sigurtà Ġestit: Jirrakkomanda verifika tal-konformità kriptografika bħala parti mill-evalwazzjonijiet tal-vulnerabbiltà.

11.7.3 MEA03 - Immonitorja, Evalwa u Ivvaluta l-Konformità: Jobbliga assigurazzjoni kontinwa tal-effettività tal-kontrolli kriptografiċi.