					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P12S					Titlu tad-dokument: **Politika tal-Ġestjoni tal-Assi**							
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**

Allinjament ma’ standards u regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżola 8	Rekwiżiti għall-ġestjoni tal-assi
ISO/IEC 27002:2022	Kontroll 5	Kontrolli għall-ġestjoni tal-assi
NIST SP 800-53 Rev.5	CM-8	Inventarju tal-komponenti tas-sistemi
Direttiva NIS2 tal-UE	Artikolu 21(2)(a)	Traċċar tal-assi għall-protezzjoni tas-sistemi tan-network u tal-informazzjoni
DORA tal-UE	Artikolu 5(8)	Rekwiżiti għall-inventarju tal-assi tal-ICT
COBIT 2019	BAI	Ġestjoni tal-assi tal-IT tul iċ-ċiklu tal-ħajja
GDPR tal-UE	Artikolu 30	Inventarju tal-attivitajiet tal-ipproċessar tad-data

1. Għan

1.1 Din il-politika tistabbilixxi kif l-organizzazzjoni tidentifika, issegwi, tipproteġi u tirtira l-assi tal-informazzjoni tagħha, inklużi kemm il-komponenti fiżiċi kif ukoll dawk diġitali.

1.2 L-għan huwa li jitnaqqsu r-riskji operattivi u tas-sigurtà billi tinżamm viżibbiltà, responsabbiltà u ġestjoni sigura tal-assi kollha tan-negozju tul iċ-ċiklu tal-ħajja tagħhom.

1.3 Inventarju affidabbli tal-assi jappoġġa l-konformità regolatorja, ir-rispons għall-inċidenti, l-ippjanar tal-kontinwità u l-ġestjoni tar-riskju.

1.4 Din il-politika tappoġġa wkoll iċ-ċertifikazzjoni skont ISO/IEC 27001 u turi allinjament ma’ obbligi legali, finanzjarji u taċ-ċibersigurtà taħt oqfsa bħall-GDPR, in-NIS2 u d-DORA.

1.5 Għall-intrapriżi żgħar u ta’ daqs medju (SMEs), approċċ sempliċi iżda sistematiku għall-ġestjoni tal-assi huwa essenzjali biex jiġu evitati apparati mhux ġestiti, tnixxijiet ta’ data jew nuqqasijiet fl-awditjar, b’mod partikolari meta l-organizzazzjoni topera b’riżorsi tekniċi limitati.

2. Kamp ta’ applikazzjoni

2.1 Din il-politika tapplika għall-assi kollha li huma proprjetà tal-organizzazzjoni, mikrija minnha jew inkella ġestiti minnha, inklużi dawk użati fi:

2.1.1 xogħol ibbażat fl-uffiċċju

2.1.2 arranġamenti ta’ xogħol remoti jew ibridi

2.1.3 operazzjonijiet fuq il-post jew mobbli

2.1.4 ambjenti cloud u esternalizzati

2.2 It-tipi ta’ assi koperti jinkludu, iżda mhumiex limitati għal:

2.2.1 Hardware: laptops, desktops, monitors, phones, tablets, USB drives, routers, printers, backup media

2.2.2 Softwer: applikazzjonijiet installati, għodod SaaS, sistemi operattivi, għodod antivirus, liċenzji

2.2.3 Assi tad-data: repożitorji ta’ data tan-negozju, spreadsheets, reġistri tal-klijenti, kodiċi tas-sors

2.2.4 Kredenzjali u servizzi diġitali: ismijiet ta’ dominju, ċertifikati diġitali, ċwievet tal-API, kontijiet tal-imejl, kredenzjali tal-login tal-cloud

2.2.5 Apparati ta’ aċċess: ċwievet, smartcards, fobs tal-aċċess, tokens bijometriċi

2.3 L-impjegati kollha, il-kuntratturi u l-fornituri terzi li jimmaniġġjaw assi tal-organizzazzjoni jaqgħu fil-kamp ta’ applikazzjoni ta’ din il-politika.

2.4 Il-politika tirregola kemm assi għal żmien qasir (eż. laptops allokati għal proġett speċifiku) kif ukoll assi għal żmien twil, kif ukoll assi kondiviżi użati minn aktar minn membru wieħed tal-persunal.

3. Objettivi

3.1 Jiġi stabbilit u miżmum inventarju sħiħ u preċiż tal-assi rilevanti kollha, aġġornat b’mod kontinwu.

3.2 Jiġi żgurat li kull assi jkollu sid maħtur responsabbli għall-użu, il-ħażna u r-ritorn tiegħu.

3.3 L-assi jiġu kklassifikati skont is-sensittività, l-impatt fuq in-negozju jew ir-rilevanza regolatorja tagħhom, sabiex ikunu jistgħu jiġu applikati livelli ta’ protezzjoni differenzjati.

3.4 Jiġu ddefiniti proċeduri ċari għall-ħruġ tal-assi, l-assenjazzjoni mill-ġdid, il-manutenzjoni, ir-rappurtar tat-telf u l-irtirar.

3.5 Jiġi żgurat li l-assi jiġu ġestiti b’mod sigur tul iċ-ċiklu tal-ħajja tagħhom u li l-informazzjoni maħżuna fihom tkun jew protetta jew imħassra b’mod sigur meta jsir ir-rimi.

3.6 Tittnaqqas il-probabbiltà ta’ inċidenti tas-sigurtà kkawżati minn riżorsi tal-organizzazzjoni mhux traċċati, mhux irritornati jew użati ħażin.

3.7 Tiġi appoġġata l-konformità mal-liġijiet rilevanti (eż. il-prinċipju ta’ responsabbiltà tal-GDPR) u mal-istandards taċ-ċertifikazzjoni taċ-ċibersigurtà.

4. Rwoli u responsabbiltajiet

4.1 Maniġer Ġenerali (GM)

4.1.1 Huwa s-sid ta’ din il-politika u responsabbli biex jiżgura li l-prattiki tal-ġestjoni tal-assi jiġu implimentati u osservati fl-organizzazzjoni kollha.

4.1.2 Jirrieżamina u japprova aġġornamenti għall-inventarju tal-assi u jawtorizza d-dekummissjonar jew it-trasferiment tal-assi fejn meħtieġ.

4.1.3 Għandu jiġi nnotifikat dwar kull telf, serq jew użu ħażin sinifikanti ta’ assi.

4.2 Responsabbli tal-IT jew kustodju tal-assi maħtur

4.2.1 Iżomm l-inventarju tal-assi (eż. fi spreadsheet, sistema ta’ ticketing jew task tracker sempliċi għall-assi).

4.2.2 Jassenja s-sjieda tal-assi u jsegwi bidliet fl-istatus (eż. ġdid, qed jintuża, taħt tiswija, irtirat).

4.2.3 Jivverifika li l-assi kollha maħruġa huma dokumentati u marbuta ma’ individwu jew unità tan-negozju.

4.2.4 Jiżgura li t-tikketti tal-klassifikazzjoni jiġu applikati u osservati (eż. Intern, Kunfidenzjali).

4.2.5 Jikkoordina l-irkupru, is-sanitarizzazzjoni u d-diżattivazzjoni tal-assi matul il-proċedura ta’ tluq jew l-irtirar.

4.2.6 Jirrapporta kull diskrepanza fl-assi li ma tkunx ġiet solvuta lill-GM.

[... 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 rieżaminata mill-inqas darba fis-sena u kull meta:

9.1.1 Jiddaħħlu tipi ġodda ta’ teknoloġija jew assi

9.1.2 Jinbidlu l-proċeduri tat-traċċar tal-assi (eż. bl-adozzjoni ta’ għodod jew pjattaformi ġodda)

9.1.3 Obbligi regolatorji ġodda jaffettwaw it-traċċabbiltà jew ir-rimi tal-assi

9.1.4 Inċident jew awditu jidentifika lakuna fil-prattiki attwali tal-ġestjoni tal-assi

9.2 Ir-rieżamijiet għandhom jinvolvu lill-GM u lir-Responsabbli tal-IT u jinkludu aġġornamenti għall-proċeduri tal-ġestjoni tal-assi, mudelli tal-inventarju u gwida dwar il-klassifikazzjoni.

9.3 L-aġġornamenti kollha għandhom ikunu dokumentati u kkomunikati lill-persunal affettwat. Għandu jinżamm reġistru tal-bidliet taħt kontroll tal-verżjoni.

10. Politiki relatati u rabtiet

10.1 P2S – Politika dwar ir-Rwoli u r-Responsabbiltajiet tal-Governanza: Tassenja r-responsabbiltà għas-sjieda tal-politika u għall-operazzjonijiet tal-IT.

10.2 P4S – Politika dwar il-Kontroll tal-Aċċess: Torbot l-użu tal-assi (eż. laptops, apparati mobbli) mad-drittijiet tal-aċċess tal-utenti u mas-sistemi ta' ġestjoni tal-identità.

10.3 P7S – Politika ta' induzzjoni u terminazzjoni: Tiżgura li l-ħruġ u l-irkupru tal-assi jkunu integrati fil-proċessi taċ-ċiklu tal-ħajja tal-persunal.

10.4 P13S – Politika dwar il-Klassifikazzjoni u t-Tikkettar tad-Data: Tipprovdi regoli biex jiġi ddeterminat jekk assi għandux jiġi kklassifikat bħala Intern jew Kunfidenzjali.

10.5 P30S – Politika dwar ir-Rispons għall-Inċidenti: Tiggwida l-proċeduri ta' rispons jekk avveniment relatat ma' assi jwassal għal ksur tas-sigurtà jew tal-privatezza.

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001

11.1.1 Klawżola 8.1: Teħtieġ kontrolli operattivi biex jiġu ġestiti l-assi u protetti tul l-użu tagħhom.

11.2 ISO/IEC 27002

11.2.1 Kontroll 5.9: Jiddettalja kif l-assi għandhom jiġu identifikati, assenjati lil sid, ikklassifikati u ġestiti b'mod sigur.

11.3 NIST SP 800-53 Rev

11.3.1 CM-8: Jeħtieġ li l-organizzazzjonijiet jiżviluppaw u jżommu inventarju tal-komponenti tas-sistemi, inklużi hardware, softwer u assi virtwali.

11.4 GDPR tal-UE

11.4.1 Artikolu 30: Jeħtieġ dokumentazzjoni tal-attivitajiet tal-ipproċessar tad-data, li tiddependi fuq għarfien ta' fejn tinħażen id-data u fuq liema assi.

11.5 Direttiva NIS2 tal-UE

11.5.1 Artikolu 21(2)(a): Titlob miżuri tekniċi u organizzattivi, inkluż traċċar tal-assi, biex jipproteġu s-sistemi tan-network u tal-informazzjoni.

11.6 DORA tal-UE

11.6.1 Artikolu 5(8): L-entitajiet finanzjarji għandhom iżommu inventarji dettaljati tal-assi tal-ICT bħala parti mill-ġestjoni tar-riskju tal-ICT.

11.7 COBIT 2019

11.7.1 BAI09: Jispeċifika li l-assi tal-IT għandhom jiġu ġestiti tul iċ-ċiklu tal-ħajja tagħhom, mill-akkwist sal-irtirar, b'sjieda u kontrolli ċari.