					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P22S					Titlu tad-dokument: **Politika dwar l-Illoggjar u l-Monitoraġġ**							
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**

Allinjata ma’ standards u regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżola 8	Kontrolli operattivi, inkluż l-illoggjar
ISO/IEC 27002:2022	Kontrolli 8.15, 8.16, 8.17	Reġistrazzjoni tal-avvenimenti, protezzjoni tal-logs u monitoraġġ
NIST SP 800-53 Rev.5	AU-2 sa AU-12, SI-4	Kontenut u rieżami tal-logs tal-awditjar, żamma, skoperta ta’ anomaliji u twissijiet
GDPR tal-UE	Artikoli 5(1)(f), 32, 33	Kunfidenzjalità u integrità tad-data, miżuri tekniċi u notifika ta’ ksur
Direttiva NIS2 tal-UE	Artikoli 21(2)(d), 23	Mekkaniżmi ta’ logging għall-iskoperta ta’ anomaliji u rappurtar ta’ inċidenti fi żmien 24 siegħa
DORA tal-UE	Artikoli 10, 15	Reżiljenza operattiva u monitoraġġ/illoggjar tal-fornituri tas-servizzi
COBIT 2019	DSS01.03, DSS05.02	Traċċabbiltà tal-attività u protezzjoni permezz tal-illoggjar u l-monitoraġġ

1. Għan

1.1 Din il-politika tistabbilixxi kontrolli obbligatorji għall-illoggjar u l-monitoraġġ biex tiġi żgurata s-sigurtà, ir-responsabbiltà u l-integrità operattiva tas-sistemi tal-IT tal-organizzazzjoni.

1.2 Hija tiddefinixxi t-tipi ta’ avvenimenti li għandhom jiġu rreġistrati fil-logs, kif il-logs jinħażnu, kif jiġu rieżaminati, u r-responsabbiltajiet tal-persunal u tal-forniturі tas-servizzi.

1.3 L-illoggjar u l-monitoraġġ jappoġġjaw l-iskoperta tat-theddid, il-konformità regolatorja, ir-rispons għall-inċidenti u l-analiżi forensika.

1.4 Din il-politika tippermetti lill-organizzazzjoni tissodisfa r-rekwiżiti ta’ kontroll operattiv tal-ISO/IEC 27001 u tappoġġja l-kapaċità li turi konformità kontinwa, il-fiduċja tal-klijenti u l-konformità mal-GDPR, man-NIS2 u mad-DORA.

2. Kamp ta’ applikazzjoni

2.1 Din il-politika tapplika għas-sistemi u l-utenti kollha fi ħdan l-organizzazzjoni, inklużi:

2.1.1 Stazzjonijiet tax-xogħol, laptops, servers, firewalls, switches, routers u punti ta’ aċċess mingħajr fili

2.1.2 Servizzi cloud użati għall-operazzjonijiet tan-negozju (eż. imejl, ħażna ta’ fajls, backups, għodod ta’ kollaborazzjoni)

2.1.3 Funzjonijiet ta’ logging fuq softwer antivirus, applikazzjonijiet, sistemi operattivi u tagħmir tan-network

2.1.4 L-impjegati kollha, il-kuntratturi u l-forniturі ta’ servizzi ġestiti (MSPs) li jużaw jew jamministraw is-sistemi

2.1.5 Kull post fejn jintużaw is-sistemi tal-IT tal-kumpanija, inklużi ambjenti remoti, ibridi jew BYOD

2.2 Il-politika tapplika wkoll għal logs iġġenerati minn servizzi ta’ partijiet terzi fejn l-organizzazzjoni għandha aċċess amministrattiv jew drittijiet kuntrattwali ta’ awditjar.

3. Objettivi

3.1 Tiżgura l-illoggjar tal-attività tas-sistema, inklużi l-awtentikazzjoni, il-bidliet fil-konfigurazzjoni, l-aċċess għal data sensittiva u t-twissijiet tas-sigurtà

3.2 Tiżgura ż-żamma ta' logs siguri u preċiżi biex jinstabu ksur tal-politika, żbalji tas-sistema jew azzjonijiet mhux awtorizzati

3.3 Tippermetti rieżami rapidu tal-logs matul inċidenti, investigazzjonijiet u awditi

3.4 Tappoġġja s-sinkronizzazzjoni tal-ħin biex tiġi żgurata l-integrità u l-korrelazzjoni tad-data fil-logs

3.5 Tipproteġi l-logs minn tbagħbis, telf jew tħassir prematur

3.6 Tissodisfa obbligi legali u regolatorji relatati mar-responsabbiltà tas-sistemi, it-traċċabbiltà u r-rispons għall-ksur

4. Rwoli u responsabbiltajiet

4.1 Maniġer Ġenerali (GM)

4.1.1 Japprova din il-politika u jiżgura l-implimentazzjoni tagħha fis-sistemi kollha tan-negozju

4.1.2 Jirrieżamina twissijiet ta' severità għolja u sejbiet serji tal-awditjar irrappurtati mill-funzjonijiet tal-IT jew tal-privatezza

4.1.3 Jagħti l-approvazzjoni finali għal eċċezzjonijiet fejn l-illoggjar jew iż-żamma ma jkunux jistgħu jiġu infurzati teknikament

4.2 Fornitur ta' Appoġġ tal-IT / Rwol Intern tal-IT

4.2.1 Jimplimenta u jikkonfigura l-illoggjar għal sistemi operattivi, apparati tan-network, għodod antivirus u applikazzjonijiet ewlenin

4.2.2 Jiżgura li l-logs jinżammu, jiġu backupjati u protetti kontra tibdil mhux awtorizzat

4.2.3 Jirrieżamina l-logs skont skeda stabbilita u jinvestiga attività suspettuża jew mhux awtorizzata

4.2.4 Iżomm sistemi ta' twissija li jidentifikaw imġiba anomala jew indikaturi ta' intrużjoni

[... 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-inqas darba fis-sena mill-Maniġer Ġenerali, bl-appoġġ tal-Fornitur ta' Appoġġ tal-IT u tal-Koordinatur tal-Privatezza.

9.2 Attivaturi tar-rieżami

9.2.1 Għandhom isiru rieżamijiet mhux skedati b'risposta għal:

9.2.1.1 Sejbiet relatati mal-logs minn awditi interni jew esterni

9.2.1.2 Inċidenti ta' sigurtà fejn il-logs kienu nieqsa, korrotti jew insuffiċjenti

9.2.1.3 Bidliet materjali fl-infrastruttura tal-IT (eż. migrazzjoni lejn pjattaformi ta' logging fil-cloud)

9.2.1.4 Aġġornamenti għall-obbligi legali jew regolatorji (eż. GDPR, NIS2, DORA)

9.3 Kontroll tal-verżjoni

9.3.1 Il-bidliet kollha f'din il-politika għandhom jiġu rreġistrati b'numru tal-verżjoni, data u sommarju tar-reviżjonijiet

9.3.2 Verżjonijiet preċedenti għandhom jiġu arkivjati u miżmuma għal mill-inqas 3 snin

9.3.3 Politiki aġġornati għandhom jiġu kkomunikati lill-partijiet ikkonċernati affettwati, b'mod partikolari lil dawk li għandhom aċċess fil-livell tas-sistema

10. Politiki relatati u rabtiet

10.1 Din il-politika tappoġġja direttament u hija appoġġjata mill-politiki li ġejjin tal-SME dwar is-sigurtà tal-informazzjoni:

10.1.1 P17S – Politika dwar il-Protezzjoni tad-Data u l-Privatezza: Tiżgura li d-data fil-logs li tinkludi informazzjoni personali tiġi ġestita b'integrità, b'salvagwardji taż-żamma u b'kontrolli tal-aċċess f'konformità mar-rekwiżiti tal-GDPR.

10.1.2 P21S – Politika dwar is-Sigurtà tan-Netwerk: Tipprovdi l-bażi għall-ġbir ta' logs relatati ma' firewalls, aċċess mingħajr fili, VPNs u monitoraġġ tas-segmentazzjoni.

10.1.3 P24S – Politika dwar l-Iżvilupp Sigur: Tiżgura li l-logs tal-applikazzjonijiet (eż. għal tentattivi ta' login, żbalji u eċċezzjonijiet) ikunu integrati fid-disinn u fl-operat tas-softwer.

10.1.4 P30S – Politika dwar ir-Rispons għall-Inċidenti: Tiddependi fuq data tal-logs preċiża u kompleta biex tiskopri, tanalizza u tirrispondi għal avvenimenti ta' sigurtà tal-informazzjoni.

10.1.5 P23S – Politika dwar is-Sinkronizzazzjoni tal-Ħin: Tiżgura timestamps konsistenti u traċċabbli fis-sistemi kollha, biex il-logs ikunu jistgħu jiġu korrelati waqt investigazzjonijiet.

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001

11.1.1 Klawżola 8.1 – Teħtieġ l-implimentazzjoni ta' kontrolli operattivi biex jittaffew ir-riskji tas-sigurtà tal-informazzjoni, inkluż l-illoggjar.

11.2 ISO/IEC 27002

11.2.1 Kontroll 8.15 – Jeħtieġ ir-reġistrazzjoni tal-avvenimenti biex tappoġġja l-iskoperta ta' anomaliji u r-responsabbiltà.

11.2.2 Kontroll 8.16 – Jeħtieġ il-protezzjoni tal-logs kontra tbagħbis u aċċess mhux awtorizzat.

11.2.3 Kontroll 8.17 – Jeħtieġ monitoraġġ tas-sistemi għal attività mhux tas-soltu u konferma tal-effettività tal-kontrolli tal-monitoraġġ.

11.3 NIST SP 800-53 Rev.5

11.3.1 AU-2 sa AU-12 – Ikopru l-kontenut tal-logs tal-awditjar, ir-rieżami, iż-żamma u t-twissijiet awtomatizzati.

11.3.2 SI-4 – Jeħtieġ l-iskoperta ta' anomaliji fis-sistema u r-rappurtar ta' avvenimenti suspettużi.

11.4 GDPR tal-UE

11.4.1 Artikolu 5(1)(f) – Jeħtieġ l-integrità u l-kunfidenzjalità tad-data personali, li tinkludi l-illoggjar tal-aċċess.

11.4.2 Artikolu 32 – Jobbliga miżuri tekniċi u organizzattivi biex tiġi żgurata s-sigurtà, inkluż l-illoggjar u l-monitoraġġ.

11.4.3 Artikolu 33 – Jeħtieġ notifika ta' ksur f'waqtha, appoġġjata minn logs li jippermettu analiżi tal-kawża ewlenija.

11.5 Direttiva NIS2 tal-UE

11.5.1 Artikolu 21(2)(d) – Jeħtieġ mekkaniżmi ta' logging li jiskopru anomaliji u jipprovdu appoġġ waqt investigazzjonijiet ta' inċidenti.

11.5.2 Artikolu 23 – Jobbliga rappurtar ta' inċidenti fi żmien 24 siegħa, li jiddependi fuq data tal-logs preċiża u f'waqtha.

11.6 DORA tal-UE

11.6.1 Artikolu 10 – Jeħtieġ reżiljenza operattiva diġitali, inkluża traċċabbiltà ta' inċidenti relatati mal-ICT permezz tal-illoggjar.

11.6.2 Artikolu 15 – Jobbliga monitoraġġ tal-fornituri tas-servizzi, inkluż aċċess għal logs u drittijiet ta' rieżami.

11.7 COBIT 2019

11.7.1 DSS01.03 – Jeħtieġ traċċabbiltà tal-attività tas-sistema permezz tal-illoggjar u l-monitoraġġ.

11.7.2 DSS05.02 – Jindirizza l-illoggjar bħala kontroll ewlieni fil-protezzjoni kontra l-malware u attività oħra mhux awtorizzata.