					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P22					Titlu tad-dokument: **Politika tal-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**

1. Għan

1.1 L-għan ta' din il-politika huwa li tistabbilixxi rekwiżiti ċari u infurzabbli għall-ġenerazzjoni, il-protezzjoni, ir-rieżami u l-analiżi tal-logs li jaqbdu avvenimenti ewlenin tas-sistema u tas-sigurtà fl-ambjent tal-IT tal-organizzazzjoni.

1.2 L-illoggjar u l-monitoraġġ huma kritiċi għas-sejbien ta' anomaliji, għar-rispons għat-theddid, għall-investigazzjoni forensika, għad-dimostrazzjoni tal-konformità u għall-konformità legali. Din il-politika tiżgura li l-avvenimenti kollha ġġenerati mis-sistema jiġu rreġistrati, miżmuma u kkorellati kif xieraq, b'eżattezza tal-ħin sinkronizzata.

1.3 Din il-politika hija essenzjali biex tappoġġa l-Klawżola 8.1 tal-ISO/IEC 27001 u l-Kontrolli tal-Anness A 8.15 (Illoggjar), 8.16 (Monitoraġġ) u 8.17 (Sinkronizzazzjoni tal-Arloġġ), u hija mmappjata direttament mal-obbligi regolatorji taħt il-GDPR, in-NIS2, id-DORA u l-COBIT 2019.

2. Kamp ta' applikazzjoni

2.1 Din il-politika tapplika għas-sistemi, is-servizzi u l-ambjenti kollha li jaħżnu, jipproċessaw jew jittrasmettu data koperta mis-Sistema ta' Ġestjoni tas-Sigurtà tal-Informazzjoni (ISMS), inklużi:

2.1.1 infrastruttura fuq il-post, servizzi cloud (eż. IaaS, PaaS, SaaS), u ambjenti ibridi

2.1.2 sistemi operattivi, bażijiet tad-data, applikazzjonijiet u apparat tan-network

2.1.3 sistemi ta' sigurtà bħas-SIEMs, firewalls, pjattaformi ta' skoperta u rispons tal-endpoint (EDR), konċentraturi tal-VPN, u fornituri tal-identità

2.2 Il-partijiet interessati li ġejjin jaqgħu fil-kamp ta' applikazzjoni:

2.2.1 utenti interni bi privileġġi tas-sistema jew privileġġi amministrattivi

2.2.2 persunal tal-infrastruttura u tal-operazzjonijiet tal-IT

2.2.3 iċ-Ċentru tal-Operazzjonijiet tas-Sigurtà (SOC) u timijiet tas-sejbien tat-theddid

2.2.4 żviluppaturi tas-software u sidien tal-applikazzjonijiet

2.2.5 fornituri ta' servizzi ta' partijiet terzi li jimmaniġġjaw sistemi li jiġġeneraw logs

3. Objettivi

3.1 Tiżgura li s-sistemi kritiċi kollha jiġġeneraw logs ta' avvenimenti tas-sigurtà u reġistri tal-attività tas-sistema li jinżammu skont rekwiżiti regolatorji, legali u kuntrattwali.

3.2 Tiddefinixxi t-tipi minimi ta' avvenimenti u l-kontenut tal-logs meħtieġa biex jiġu skoperti attivitajiet mhux awtorizzati, jiġu rintraċċati l-azzjonijiet tal-utenti u jiġu appoġġjati investigazzjonijiet forensiċi.

3.3 Teħtieġ kontrolli ta' protezzjoni biex jiġi evitat it-tbagħbis tal-logs, it-tħassir mhux awtorizzat jew aċċess mhux ikkontrollat għad-data tal-logs.

3.4 Tistabbilixxi sistemi ċentralizzati ta' illoggjar u twissijiet (eż. SIEM) biex jiġbru, jikkorellaw u jeskalaw attività suspettuża kważi f'ħin reali.

3.5 Tiżgura s-sinkronizzazzjoni tal-arloġġi tas-sistemi sabiex tippermetti korrelazzjoni preċiża bejn sistemi differenti u analiżi tal-inċidenti.

3.6 Tippermetti titjib kontinwu u konformità billi tintegra l-monitoraġġ tal-logs mal-proċessi tal-awditjar, tal-ġestjoni tar-riskju u tal-ġestjoni tal-inċidenti.

4. Rwoli u responsabbiltajiet

4.1 Uffiċjal Kap tas-Sigurtà tal-Informazzjoni (CISO)

4.1.1 Huwa s-sid ta' din il-politika u jiżgura li tkun allinjata mal-pożizzjoni tar-riskju tal-organizzazzjoni, mar-rekwiżiti tal-awditjar u mal-obbligi tal-ISMS.

4.1.2 Japprova l-kamp ta' applikazzjoni tal-illoggjar għal sistemi regolati jew ta' riskju għoli u jeżerċita sorveljanza fuq ir-rappurtar tal-konformità.

4.2 Maniġer taċ-Ċentru tal-Operazzjonijiet tas-Sigurtà (SOC)

4.2.1 Iħaddem u jżomm pjattaformi ċentralizzati ta' ġestjoni tal-logs (eż. SIEM).

4.2.2 Jiddefinixxi r-regoli tal-aggregazzjoni tal-logs, il-livelli tat-twissijiet u l-mogħdijiet ta' eskalazzjoni għat-trijaġġ tal-inċidenti.

4.2.3 Jirrevedi r-rapporti ta' kuljum u jiżgura li l-anomaliji jiġu analizzati, dokumentati u eskalati kif meħtieġ.

[... 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 kull sena, jew qabel, bi tweġiba għal:

9.1.1 bidliet kbar fl-arkitettura tas-sistema jew fl-infrastruttura tal-illoggjar (eż. migrazzjoni tas-SIEM)

9.1.2 reviżjonijiet fir-rekwiżiti regolatorji tal-illoggjar (eż. obbligi ta' illoggjar taħt in-NIS2 u d-DORA)

9.1.3 sejbiet minn awditi jew analiżijiet wara inċident

9.1.4 theddid emerġenti li jeħtieġ monitoraġġ imsaħħaħ (eż. theddid intern, kompromess fil-katina tal-provvista)

9.2 Il-proċess tar-rieżami għandu jkun immexxi mill-Maniġer taċ-Ċentru tal-Operazzjonijiet tas-Sigurtà (SOC) f'koordinazzjoni mas-CISO, il-Ġestjoni tar-Riskju, il-Konformità u t-timijiet tal-Infrastruttura tal-IT.

9.3 Il-bidliet approvati għandhom ikunu taħt kontroll tal-verżjoni fir-Reġistru tal-Kontroll tad-Dokumenti tal-ISMS u kkomunikati lil:

9.3.1 il-partijiet interessati kollha b'responsabbiltà għall-manutenzjoni tas-sistemi tal-illoggjar

9.3.2 sidien tal-applikazzjonijiet u tas-sistemi

9.3.3 fornituri terzi b'dmirijiet ta' telemetrija jew ta' integrazzjoni mas-SIEM

9.4 Il-verżjonijiet kollha sostitwiti għandhom jiġu arkivjati b'mod sigur, b'aċċess ristrett għal kustodji awtorizzati tal-ISMS għal finijiet ta' awditjar u legali.

10. Politiki relatati u rabtiet

10.1 P1 – Politika tas-Sigurtà tal-Informazzjoni. Tistabbilixxi l-impenn fundamentali biex jiġu protetti s-sistemi u d-data, li taħtu l-illoggjar u l-monitoraġġ jiffunzjonaw bħala kontrolli detettivi kritiċi u fatturi abilitanti tar-rispons.

10.2 P4 – Politika dwar il-Kontroll tal-Aċċess. Tiżgura li l-aċċess privileġġjat, il-logins tal-utenti u l-avvenimenti ta' awtorizzazzjoni jinqabdu fil-logs u jkunu soġġetti għal monitoraġġ għal abbuż jew imġiba anomala.

10.3 P5 – Politika tal-Ġestjoni tat-Tibdil. Teħtieġ l-illoggjar tal-bidliet fis-sistema, it-tqegħid fis-servizz tal-patches u l-aġġornamenti tal-konfigurazzjoni li jistgħu jintroduċu riskju jew modifiki mhux awtorizzati.

10.4 P21 – Politika tas-Sigurtà tan-Network. Teħtieġ illoggjar fil-livell tan-network (eż. logs tal-firewall, twissijiet IDS/IPS, attività tal-VPN) u integrazzjoni mas-SIEM għal viżibbiltà tal-anomaliji fit-traffiku u protezzjoni tal-perimetru.

10.5 P23 – Politika dwar is-Sinkronizzazzjoni tal-Ħin. Teħtieġ konsistenza tal-arloġġi bejn is-sistemi, li hija essenzjali għal illoggjar affidabbli u korrelazzjoni ta' avvenimenti tas-sigurtà f'ambjenti differenti.

10.6 P30 – Politika dwar ir-Rispons għall-Inċidenti. Tiddependi fuq id-data tal-logs u l-mekkaniżmi tat-twissijiet biex tidentifika, tinvestiga u tirrispondi għal inċidenti ta' sigurtà, filwaqt li tippreserva wkoll artifacts forensiċi għar-rieżami wara l-inċident.

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001

11.1.1 Klawżola 8.1 – Ippjanar u Kontroll Operattiv: Teħtieġ kontrolli għall-monitoraġġ tal-operazzjonijiet u salvagwardji kontra aċċess mhux awtorizzat u użu ħażin tas-sistema.

11.2 ISO/IEC 27002:2022 – Kontrolli 8.15, 8.16, 8.17

11.2.1 Tiddefinixxi rekwiżiti dettaljati tal-illoggjar, inkluż liema avvenimenti għandhom jiġu rreġistrati, kif għandhom jiġu protetti u analizzati l-logs, u kif għandha tiġi żgurata l-affidabbiltà tat-timestamps bejn is-sistemi.

11.3 NIST SP 800-53 Rev.5

11.3.1 AU-2 sa AU-12: Ikopri l-għażla tal-avvenimenti, l-illoggjar, il-protezzjoni, ir-rieżami tal-awditjar, ir-rispons għal fallimenti tal-awditjar, u ż-żamma tar-reġistri tal-awditjar.

11.3.2 SI-4 – Monitoraġġ tas-Sistema: Jeħtieġ monitoraġġ attiv tas-sistema bi twissijiet ibbażati fuq attività anomala.

11.3.3 SC-45 – Sinkronizzazzjoni tal-Ħin tas-Sistema: Isaħħaħ l-eżattezza tal-ħin għat-traċċabbiltà tal-avvenimenti u l-korrelazzjoni tal-inċidenti.

11.4 GDPR tal-UE (2016/679)

11.4.1 Artikolu 32 – Sigurtà tal-Ipproċessar: Jeħtieġ kontrolli tekniċi bħall-illoggjar u l-monitoraġġ biex jiġu żgurati s-sigurtà u r-responsabbiltà, b'mod partikolari fir-rigward tal-aċċess għad-data personali.

11.5 Direttiva NIS2 tal-UE (2022/2555)

11.5.1 Artikolu 21(2)(e): Jobbliga sistemi ta' illoggjar u monitoraġġ tal-avvenimenti għas-sejbien rapidu u r-rispons għal inċidenti ta' sigurtà.

11.6 DORA tal-UE (2022/2554)

11.6.1 Artikolu 9 – Ġestjoni tar-Riskju tal-ICT: Jeħtieġ mekkaniżmi biex tinstab attività anomala, jiġu rreġistrati inċidenti, u tinżamm data forensika.

11.6.2 Artikolu 11 – Ittestjar tal-Pjanijiet ta' Kontinwità tan-Negozju tal-ICT: Jenfasizza l-kontinwità tal-monitoraġġ u l-verifika tad-disponibbiltà tal-logs waqt tfixkil operattiv.

11.7 COBIT 2019

11.7.1 DSS01.05 – Ġestjoni tal-Logs tas-Sigurtà: Jeħtieġ implimentazzjoni ta' kapaċitajiet tal-illoggjar għall-infrastruttura kritika kollha.

11.7.2 DSS05.04 – Monitoraġġ ta' Avvenimenti tas-Sigurtà: Jobbliga monitoraġġ u analiżi tal-logs f'ħin reali biex jinstabu u jiġu indirizzati avvenimenti.

11.7.3 MEA03 – Monitoraġġ, Evalwazzjoni u Valutazzjoni tal-Konformità: Jeħtieġ rieżami regolari tal-prattiki tal-illoggjar u allinjament mal-objettivi tal-kontrolli.