					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P22S					Naslov dokumenta: **Politika beleženja in spremljanja**							
Različica: 1.0		Datum začetka veljavnosti: 01.01.2025			Lastnik dokumenta:							
X	Politika		Standard		Postopek		Obrazec		Register		Drugo	

Zgodovina revizij				
Številka revizije	**Datum revizije**	**Spremembe**	**Pregledal**	**Lastnik procesa**

Odobritve			
Ime	**Delovno mesto**	**Datum**	**Podpis**

Usklajenost s standardi in predpisi

Standard/predpis	Klavzula/člen	Komentar
ISO/IEC 27001:2022	Klavzula 8	Operativne kontrole, vključno z beleženjem
ISO/IEC 27002:2022	Kontrole 8.15, 8.16, 8.17	Revizijsko beleženje dogodkov, zaščita dnevnikov in spremljanje
NIST SP 800-53 Rev.5	AU-2 do AU-12, SI-4	Vsebina in pregled revizijskih dnevnikov, hramba, zaznavanje anomalij, opozarjanje
Uredba EU GDPR	Členi 5(1)(f), 32, 33	Zaupnost in celovitost podatkov, tehnični ukrepi ter obvestila o kršitvah
Direktiva EU NIS2	Členi 21(2)(d), 23	Mehanizmi beleženja za zaznavanje anomalij in poročanje o incidentih v 24 urah
Uredba EU DORA	Člena 10, 15	Operativna odpornost, spremljanje in beleženje pri ponudnikih storitev
COBIT 2019	DSS01.03, DSS05.02	Sledljivost dejavnosti in zaščita z beleženjem in spremljanjem

1. Namen

1.1 Ta politika določa obvezne kontrole beleženja in spremljanja za zagotavljanje varnosti, odgovornosti in operativne celovitosti informacijskih sistemov organizacije.

1.2 Določa vrste dogodkov, ki jih je treba beležiti, način hrambe dnevnikov, način njihovega pregleda ter odgovornosti zaposlenih in ponudnikov storitev.

1.3 Beleženje in spremljanje podpirata zaznavanje groženj, skladnost z regulatornimi zahtevami, odzivanje na incidente in forenzično analizo.

1.4 Ta politika organizaciji omogoča izpolnjevanje zahtev glede operativnih kontrol po standardu ISO/IEC 27001 ter podpira stalno pripravljenost na revizijo, zaupanje strank in skladnost z GDPR, NIS2 in DORA.

2. Področje uporabe

2.1 Ta politika velja za vse sisteme in uporabnike v organizaciji, vključno z:

2.1.1 delovnimi postajami, prenosniki, strežniki, požarnimi zidovi, stikali, usmerjevalniki in brezžičnimi dostopovnimi točkami,

2.1.2 storitvami v oblaku, ki se uporabljajo za poslovanje (npr. e-pošta, hramba datotek, varnostno kopiranje, orodja za sodelovanje),

2.1.3 funkcijami beleženja v protivirusni programski opremi, aplikacijah, operacijskih sistemih in omrežni opremi,

2.1.4 vsemi zaposlenimi, pogodbenimi izvajalci in ponudniki upravljanih storitev (MSP), ki uporabljajo ali upravljajo sisteme,

2.1.5 vsemi lokacijami, kjer se uporabljajo informacijski sistemi podjetja, vključno z okolji za delo na daljavo, hibridnimi oblikami dela ali uporabo lastnih naprav.

2.2 Politika velja tudi za dnevnike, ki jih ustvarjajo storitve tretjih oseb, kadar ima organizacija skrbniški dostop ali pogodbene pravice do revizije.

3. Cilji

3.1 Zagotoviti beleženje sistemskih dejavnosti, vključno z avtentikacijo, spremembami konfiguracije, dostopom do občutljivih podatkov in varnostnimi opozorili.

3.2 Vzdrževati varne in točne dnevnike za zaznavanje kršitev politike, sistemskih napak ali nepooblaščenih dejanj.

3.3 Omogočiti hiter pregled dnevnikov med incidenti, preiskavami in revizijami.

3.4 Podpreti časovno usklajevanje za zagotavljanje celovitosti in korelacije podatkov v dnevnikih.

3.5 Zaščititi dnevnike pred posegi, izgubo ali prezgodnjim izbrisom.

3.6 Izpolniti pravne in regulatorne obveznosti glede odgovornosti za delovanje sistemov, sledljivosti in odzivanja na kršitve.

4. Vloge in odgovornosti

4.1 Generalni direktor (GM)

4.1.1 odobri to politiko in zagotovi njeno izvajanje v vseh poslovnih sistemih,

4.1.2 pregleduje opozorila z visoko stopnjo resnosti in resne ugotovitve presoje, o katerih poročajo IT ali funkcije zasebnosti,

4.1.3 potrdi izjeme, kadar beleženja ali hrambe ni mogoče tehnično uveljaviti.

4.2 Ponudnik IT-podpore / interna funkcija IT

4.2.1 uvede in konfigurira beleženje za operacijske sisteme, omrežne naprave, protivirusna orodja in ključne aplikacije,

4.2.2 zagotovi, da se dnevniki hranijo, varnostno kopirajo in zaščitijo pred spremembami,

4.2.3 pregleduje dnevnike v skladu z določenim razporedom ter preiskuje sumljive ali nepooblaščene dejavnosti,

4.2.4 vzdržuje sisteme opozarjanja, ki zaznavajo neobičajno vedenje ali kazalnike vdora.

[... Razdelki 4.3–8 niso vključeni v ta predogled. Kupite celoten dokument za dostop do celotne vsebine. ...]

9. Zahteve za pregled in posodobitev

9.1 Letni pregled

9.1.1 To politiko mora najmanj enkrat letno pregledati generalni direktor ob podpori ponudnika IT-podpore in koordinatorja za zasebnost.

9.2 Povodi za pregled

9.2.1 Izredni pregledi se morajo izvesti kot odziv na:

9.2.1.1 ugotovitve notranjih ali zunanjih revizij, povezane z dnevniki,

9.2.1.2 varnostne incidente, pri katerih so dnevniki manjkali, bili poškodovani ali nezadostni,

9.2.1.3 bistvene spremembe informacijske infrastrukture (npr. migracija na platforme za beleženje v oblaku),

9.2.1.4 posodobitve pravnih ali regulatornih obveznosti (npr. GDPR, NIS2, DORA).

9.3 Nadzor različic

9.3.1 Vse spremembe te politike morajo biti zabeležene s številko različice, datumom in povzetkom sprememb.

9.3.2 Prejšnje različice morajo biti arhivirane in hranjene najmanj 3 leta.

9.3.3 Posodobljene politike je treba sporočiti prizadetim deležnikom, zlasti tistim z dostopom na ravni sistema.

10. Povezane politike in povezave s kontrolami

10.1 Ta politika neposredno podpira naslednje politike SME s področja informacijske varnosti in je z njimi tudi podprta:

10.1.1 P17S – Politika varstva podatkov in zasebnosti: zagotavlja, da se podatki v dnevnikih, ki vsebujejo osebne podatke, upravljajo s celovitostjo, ustrezno hrambo in kontrolami dostopa v skladu z zahtevami GDPR.

10.1.2 P21S – Politika omrežne varnosti: zagotavlja podlago za zajem dnevnikov, povezanih s požarnimi zidovi, brezžičnim dostopom, VPN in spremljanjem segmentacije.

10.1.3 P24S – Politika varnega razvoja: zagotavlja, da so dnevniki aplikacij (npr. za poskuse prijave, napake in izjeme) vključeni v načrtovanje in delovanje programske opreme.

10.1.4 P30S – Politika odzivanja na incidente: temelji na točnih in popolnih podatkih iz dnevnikov za zaznavanje, analizo in odzivanje na dogodke informacijske varnosti.

10.1.5 P23S – Politika časovnega usklajevanja: zagotavlja dosledne in sledljive časovne žige v vseh sistemih, kar omogoča korelacijo dnevnikov med preiskavami.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001

11.1.1 Klavzula 8.1 – Zahteva uvedbo operativnih kontrol za zmanjševanje tveganj informacijske varnosti, vključno z beleženjem.

11.2 ISO/IEC 27002

11.2.1 Kontrola 8.15 – Zahteva revizijsko beleženje dogodkov za podporo zaznavanju anomalij in odgovornosti.

11.2.2 Kontrola 8.16 – Zahteva zaščito dnevnikov pred posegi in nepooblaščenim dostopom.

11.2.3 Kontrola 8.17 – Zahteva spremljanje sistemov zaradi neobičajnih dejavnosti in potrditev učinkovitosti kontrol spremljanja.

11.3 NIST SP 800-53 Rev.5

11.3.1 AU-2 do AU-12 – Obravnavajo vsebino revizijskih dnevnikov, pregled, hrambo in samodejno opozarjanje.

11.3.2 SI-4 – Zahteva zaznavanje sistemskih anomalij in poročanje o sumljivih dogodkih.

11.4 Uredba EU GDPR

11.4.1 Člen 5(1)(f) – Zahteva celovitost in zaupnost osebnih podatkov, kar vključuje tudi beleženje dostopa.

11.4.2 Člen 32 – Določa tehnične in organizacijske ukrepe za zagotavljanje varnosti, vključno z beleženjem in spremljanjem.

11.4.3 Člen 33 – Zahteva pravočasno obveščanje o kršitvah, podprto z dnevniki, ki omogočajo analizo temeljnega vzroka.

11.5 Direktiva EU NIS2

11.5.1 Člen 21(2)(d) – Zahteva mehanizme beleženja, ki zaznavajo anomalije in zagotavljajo podporo pri preiskavah incidentov.

11.5.2 Člen 23 – Zahteva poročanje o incidentih v 24 urah, kar je odvisno od točnih in pravočasnih podatkov v dnevnikih.

11.6 Uredba EU DORA

11.6.1 Člen 10 – Zahteva digitalno operativno odpornost, vključno s sledljivostjo incidentov, povezanih s sistemi IKT, prek beleženja.

11.6.2 Člen 15 – Nalaga spremljanje ponudnikov storitev, vključno s pravicami dostopa do dnevnikov in njihovim pregledom.

11.7 COBIT 2019

11.7.1 DSS01.03 – Zahteva sledljivost dejavnosti sistema z beleženjem in spremljanjem.

11.7.2 DSS05.02 – Obravnava beleženje kot ključno kontrolo pri zaščiti pred zlonamerno programsko opremo in drugimi nepooblaščenimi dejavnostmi.