					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P25S					Naslov dokumenta: **Politika zahtev za varnost aplikacij**							
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 varnostjo aplikacij
ISO/IEC 27002:2022	Kontroli 8.25–8.26	Varna zasnova, razvoj, testiranje in pregled izvorne kode
NIST SP 800-53 Rev.5	SA-11, SI-10	Testiranje razvijalcev in aplikacij, analiza kode, preprečevanje pomanjkljivosti
Uredba EU GDPR	Člen 25	Varstvo podatkov že pri načrtovanju in privzeto varstvo zasebnosti
Direktiva EU NIS2	Člen 21(2)(a), (e)	Tehnični ukrepi za zaščito aplikacij in zaznavanje tveganj
Uredba EU DORA	Člena 9(2)(c), 10(2)(c)	Varnost aplikacij za digitalno operativno odpornost
COBIT 2019	BAI03	Upravljanje varne izdelave ali pridobitve programske opreme

1. Namen

1.1 Ta politika določa najmanjše obvezne kontrole varnosti aplikacij, ki se zahtevajo za vso programsko opremo in sistemske rešitve, ki jih uporablja organizacija, ne glede na to, ali so razvite interno ali pridobljene od zunanjih dobaviteljev.

1.2 Zagotavlja, da so aplikacije zasnovane, uvedene in vzdrževane tako, da varujejo podatke strank, zaposlenih in poslovne podatke pred nepooblaščenim dostopom, neustrezno uporabo, spremembo ali uničenjem.

1.3 Ta politika podpira prizadevanja organizacije za pridobitev in ohranjanje certifikacije ISO/IEC 27001, izpolnjevanje obveznosti po GDPR in NIS2 ter zmanjševanje operativnih tveganj, povezanih z neustreznimi uvedbami programske opreme.

1.4 Prispeva k vzpostavitvi doslednega pristopa k varnosti aplikacij, primernega za revizijo, za mala in srednja podjetja z določitvijo enotnega kontrolnega seznama varnostnih funkcionalnosti in praks, prilagojenega okoljem z omejenimi internimi tehničnimi viri.

2. Področje uporabe

2.1 Ta politika velja za vse aplikacije, sisteme, orodja in platforme, ki:

2.1.1 so razviti interno, prilagojeni ali skriptirani za interno uporabo,

2.1.2 so nabavljeni kot komercialna programska oprema, SaaS ali storitve v oblaku,

2.1.3 obdelujejo, hranijo ali prenašajo osebne podatke, poslovne evidence ali občutljive operativne informacije,

2.1.4 so dostopni zaposlenim, pogodbenim izvajalcem, strankam ali partnerjem prek notranjih omrežij, interneta ali mobilnih platform.

2.2 Politika zajema:

2.2.1 razvijalce (interne ali pogodbene),

2.2.2 dobavitelje programske opreme in ponudnike storitev v oblaku,

2.2.3 osebje za podporo IT ali skrbnike, odgovorne za uvajanje in podporo,

2.2.4 lastnike aplikacij in poslovne uporabnike, vključene v odobritev in nadzor sistemov.

3. Cilji

3.1 Zagotoviti, da imajo vse aplikacije, ki jih uporablja organizacija, vgrajene in preverljive varnostne kontrole, ki zmanjšujejo pogoste ranljivosti programske opreme.

3.2 Varovati zaupnost, celovitost in razpoložljivost (CIA) podatkov, ki jih obdelujejo aplikacije, ne glede na to, kje gostujejo.

3.3 Zahtevati formalno testiranje, pregled in preverjanje varnosti aplikacij, preden je katera koli nova aplikacija ali večja posodobitev odobrena za produkcijsko uporabo.

3.4 Omogočiti dosledno in varno upravljanje uporabniških poverilnic, podatkov sej in pravic dostopa v vseh poslovno kritičnih sistemih.

3.5 Zahtevati varno revizijsko beleženje, revizijske zmogljivosti in funkcionalnosti spremljanja v vseh aplikacijah za podporo zaznavanju sumljivih dejavnosti in odzivanju nanje.

3.6 Zmanjšati pravna in skladnostna tveganja z zagotavljanjem, da aplikacije izpolnjujejo veljavne regulativne varnostne zahteve.

4. Vloge in odgovornosti

4.1 Generalni direktor

4.1.1 Nosi splošno odgovornost za varnost aplikacij v celotni organizaciji.

4.1.2 Odobri to politiko in zagotovi, da so vse nabave ali razvojni projekti skladni z njo.

4.1.3 Zagotovi, da so dobavitelji in ponudniki storitev pogodbeno zavezani zahtevam glede varnosti aplikacij.

4.1.4 Pregleda in odobri izjeme glede tveganj, kadar popolne skladnosti zaradi poslovnih omejitev ni mogoče doseči.

4.2 Lastnik aplikacije (če je imenovan)

4.2.1 Med izbiro sistema ali začetkom projekta opredeli specifične varnostne zahteve aplikacije.

4.2.2 Preveri, da so vključene ključne funkcionalnosti, kot so zaščita prijave, šifriranje in dnevniki dejavnosti.

4.2.3 Sodeluje pri pregledih pred uvedbo in potrdi, da varnostne kontrole izpolnjujejo poslovne potrebe.

[... 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 To politiko mora Generalni direktor pregledati najmanj enkrat v vsakem koledarskem letu, da:

9.1.1 odraža spremembe regulativnih zahtev (npr. GDPR, NIS2, DORA),

9.1.2 vključi nove ali nastajajoče grožnje in tehnike napadov,

9.1.3 posodobi besedilo in zahteve glede na spremembe platform, dobaviteljev ali razvojnih metod.

9.2 Vmesni pregledi se morajo izvesti tudi, kadar:

9.2.1 se uvedejo nove aplikacije,

9.2.2 obstoječe aplikacije doživijo pomembne posodobitve ali integracijo,

9.2.3 pride do incidenta ali kršitve, povezane z aplikacijo,

9.2.4 so nova tveganja ugotovljena na podlagi zunanjih obvestil ali panožnih opozoril.

9.3 Vse posodobitve te politike morajo biti:

9.3.1 odobrene s strani Generalnega direktorja,

9.3.2 dokumentirane z evidenco različic in razlogom za spremembo,

9.3.3 sporočene vsem zaposlenim, razvijalcem in dobaviteljem, ki sodelujejo pri upravljanju aplikacij,

9.3.4 varno shranjene za potrebe revizije in sklicevanja na skladnost.

10. Povezane politike in povezave

10.1 To politiko neposredno podpirajo in prispevajo k njenemu izvajanju naslednje varnostne politike, usklajene za SME:

10.1.1 P2S – Politika vlog in odgovornosti upravljanja: določa odgovornosti za odobritev aplikacij, izvajanje politike in upravljanje dobaviteljev.

10.1.2 P4S – Politika nadzora dostopa: zagotavlja, da je dostop do aplikacij usklajen z načelom najmanjših privilegijev in načeli upravljanja sej.

10.1.3 P8S – Politika ozaveščanja in usposabljanja za informacijsko varnost: zagotavlja, da so uporabniki in razvijalci usposobljeni za prepoznavanje in prijavljanje groženj, povezanih z aplikacijami.

10.1.4 P17S – Politika varstva podatkov in zasebnosti: določa zaščitne ukrepe zasebnosti podatkov, ki jih mora uveljavljati vsaka aplikacija, ki obdeluje osebne podatke.

10.1.5 P14S – Politika hrambe podatkov in odstranjevanja: ureja, kako morajo biti dnevniki, varnostne kopije in občutljivi podatki, ki jih ustvari aplikacija, hranjeni, arhivirani in varno uničeni.

10.1.6 P30S – Politika odzivanja na incidente: določa korake za prepoznavanje, prijavo in zajezitev varnostnih dogodkov, povezanih z aplikacijami.

10.2 Te politike skupaj zagotavljajo, da je varnost aplikacij v celoti vključena v sistem upravljanja informacijske varnosti (ISMS) organizacije in da je organizacija pripravljena na revizijo.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001

11.1.1 Klavzula 8 – zahteva, da organizacije vzpostavijo operativne kontrole za obravnavo tveganj informacijske varnosti, vključno s tveganji, povezanimi z aplikacijami in programskimi sistemi.

11.2 ISO/IEC 27002

11.2.1 Kontrola 8.25 – priporoča izvajanje praks varne zasnove, razvoja in pregleda izvorne kode za vse aplikacije, vključno s tistimi, ki jih zagotavljajo dobavitelji.

11.2.2 Kontrola 8.26 – priporoča formalno testiranje kontrol za varnost aplikacij, zlasti na področjih nadzora dostopa, preverjanja vnosa in upravljanja sej.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – določa zahteve za testiranje razvijalcev, analizo kode in dinamično skeniranje aplikacij pred uvedbo.

11.3.2 SI-10 – obravnava zaznavanje in preprečevanje pogostih napak programske opreme ter poudarja ozaveščenost razvijalcev in tehnične zaščitne ukrepe.

11.4 Uredba EU GDPR (2016/679)

11.4.1 Člen 25 – »varstvo podatkov že pri načrtovanju in privzeto varstvo zasebnosti« zahteva, da se zasebnost in varnost vključita v osnovno zasnovo aplikacij, ki obdelujejo osebne podatke.

11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Člen 21(2)(a) in (e) – zahteva, da bistveni in pomembni subjekti uvedejo tehnične ukrepe za zaščito aplikacij in zaznavanje tveganj, povezanih s programsko opremo.

11.6 Uredba EU DORA (2022/2554)

11.6.1 Člena 9(2)(c), 10(2)(c) – zahtevata, da mala in srednja podjetja v finančnem sektorju vgradijo kontrole varnosti na ravni aplikacij in izvajajo redne presoje za ohranjanje digitalne operativne odpornosti.

11.7 COBIT 2019

11.7.1 BAI03 – »Upravljanje identifikacije rešitev in izdelave« usmerja razvoj ali pridobitev varne programske opreme, usklajene s tveganji, skladnostjo in poslovnimi zahtevami, tudi v okoljih malih in srednjih podjetij z omejenimi viri.