					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P25S					Naziv dokumenta: **Politika sigurnosnih zahtjeva za aplikacije**							
Verzija: 1.0		Datum stupanja na snagu: 01.01.2025			Vlasnik dokumenta:							
X	Politika		Standard		Postupak		Obrazac		Registar		Drugo	

Povijest revizija				
Broj revizije	**Datum revizije**	**Promjene**	**Pregledao/la**	**Vlasnik procesa**

Odobrenja			
Ime	**Radno mjesto**	**Datum**	**Potpis**

Usklađeno sa standardima i propisima

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točka 8	Operativne kontrole, uključujući sigurnost aplikacija
ISO/IEC 27002:2022	Kontrole 8.25–8.26	Siguran dizajn, razvoj, testiranje i pregled koda
NIST SP 800-53 Rev.5	SA-11, SI-10	Testiranje aplikacija od strane razvojnih inženjera, analiza koda, sprječavanje nedostataka
GDPR EU	Članak 25	zaštita privatnosti u fazi projektiranja / zaštita privatnosti prema zadanim postavkama
Direktiva EU NIS2	Članak 21(2)(a), (e)	Tehničke mjere za zaštitu aplikacija i otkrivanje rizika
Uredba EU DORA	Članci 9(2)(c), 10(2)(c)	Sigurnost aplikacija za digitalnu operativnu otpornost
COBIT 2019	BAI03	Upravljanje sigurnom izgradnjom/nabavom softvera

1. Svrha

1.1 Ova politika definira minimalne obvezne kontrole sigurnosti aplikacija koje se zahtijevaju za sva softverska i sustavna rješenja koja organizacija koristi, neovisno o tome jesu li razvijena interno ili nabavljena od vanjskih dobavljača.

1.2 Ova politika osigurava da su aplikacije projektirane, implementirane i održavane tako da štite podatke klijenata, zaposlenika i poslovne podatke od neovlaštenog pristupa, zlouporabe, izmjene ili uništenja.

1.3 Ova politika podupire aktivnosti organizacije usmjerene na postizanje i održavanje certifikacije ISO/IEC 27001, ispunjavanje obveza prema GDPR-u i NIS2 te smanjenje operativnih rizika povezanih s nesigurnim uvođenjem softvera.

1.4 Ova politika pomaže uspostaviti dosljedan i revizijski provjerljiv pristup sigurnosti aplikacija za SME organizacije utvrđivanjem jedinstvenog kontrolnog popisa sigurnosnih funkcionalnosti i praksi, prilagođenog okruženjima s ograničenim internim tehničkim resursima.

2. Opseg

2.1 Ova politika primjenjuje se na sve aplikacije, sustave, alate i platforme koje:

2.1.1 se razvijaju interno, prilagođavaju ili skriptiraju za internu uporabu

2.1.2 se nabavljaju kao komercijalni softver, SaaS ili usluge u oblaku

2.1.3 obrađuju, pohranjuju ili prenose osobne podatke, poslovne zapise ili osjetljive operativne informacije

2.1.4 im pristupaju zaposlenici, ugovorni izvođači, klijenti ili partneri putem internih mreža, interneta ili mobilnih platformi

2.2 Ova politika obuhvaća:

2.2.1 razvojne inženjere (interne ili ugovorene)

2.2.2 dobavljače softvera i pružatelje usluga u oblaku

2.2.3 IT i tehničko-operativno osoblje odnosno administratore odgovorne za uvođenje i podršku

2.2.4 vlasnike aplikacija i poslovne korisnike uključene u odobravanje sustava i nadzor

3. Ciljevi

3.1 Osigurati da sve aplikacije koje organizacija koristi imaju ugrađene i provjerljive sigurnosne kontrole koje ublažavaju uobičajene ranjivosti softvera.

3.2 Zaštititi povjerljivost, cjelovitost i dostupnost podataka koje obrađuju aplikacije, neovisno o tome gdje su hostirane.

3.3 Zahtijevati formalno testiranje, pregled i provjeru sigurnosti aplikacija prije nego što se bilo koja nova aplikacija ili značajno ažuriranje odobri za pristup produkcijskom okruženju.

3.4 Omogućiti dosljedno i sigurno upravljanje korisničkim vjerodajnicama, podacima o sesiji i pravima pristupa u svim poslovno kritičnim sustavima.

3.5 Zahtijevati sigurno bilježenje događaja, mogućnosti revizije i funkcionalnosti praćenja u svim aplikacijama radi podrške otkrivanju sumnjivih aktivnosti i odgovoru na njih.

3.6 Smanjiti pravne rizike i rizike usklađenosti osiguravanjem da aplikacije ispunjavaju primjenjive regulatorne sigurnosne zahtjeve.

4. Uloge i odgovornosti

4.1 glavni direktor (GM)

4.1.1 Snosi ukupnu odgovornost za sigurnost aplikacija u cijeloj organizaciji.

4.1.2 Odobrava ovu politiku i osigurava da su sve nabave ili razvojni projekti usklađeni s njom.

4.1.3 Osigurava da su dobavljači i pružatelji usluga ugovorno obvezani na zahtjeve sigurnosti aplikacija.

4.1.4 Pregledava i odobrava iznimke povezane s rizikom kada se puna usklađenost ne može postići zbog poslovnih ograničenja.

4.2 vlasnik aplikacije (ako je imenovan)

4.2.1 Utvrđuje sigurnosne potrebe specifične za aplikaciju tijekom odabira sustava ili pokretanja projekta.

4.2.2 Provjerava da su uključene ključne funkcionalnosti kao što su zaštita prijave, šifriranje i revizijsko bilježenje aktivnosti.

4.2.3 Sudjeluje u pregledima prije uvođenja i potvrđuje da sigurnosne kontrole zadovoljavaju poslovne potrebe.

[... Odjeljci 4.3–8 nisu uključeni u ovaj pregled. Kupite cijeli dokument za pristup potpunom sadržaju. ...]

9. Zahtjevi za pregled i ažuriranje

9.1 Ovu politiku glavni direktor mora pregledati najmanje jednom u svakoj kalendarskoj godini kako bi se:

9.1.1 odrazile promjene regulatornih zahtjeva (npr. GDPR, NIS2, DORA)

9.1.2 uvrstile nove ili nastajuće prijetnje i tehnike napada

9.1.3 ažurirali jezik i zahtjevi radi usklađenja s promjenama platformi, dobavljača ili metoda razvoja

9.2 Izvanredni pregledi moraju se provesti i kada:

9.2.1 se uvode nove aplikacije

9.2.2 postojeće aplikacije prolaze značajna ažuriranja ili integraciju

9.2.3 nastane incident ili povreda povezana s aplikacijom

9.2.4 se utvrde novi rizici na temelju vanjskih obavijesti ili upozorenja iz industrije

9.3 Sva ažuriranja ove politike moraju biti:

9.3.1 odobrena od strane glavnog direktora

9.3.2 dokumentirana uz povijest verzija i razlog promjene

9.3.3 priopćena svim zaposlenicima, razvojnim inženjerima i dobavljačima uključenima u upravljanje aplikacijama

9.3.4 sigurno pohranjena za potrebe revizije i usklađenosti

10. Povezane politike i poveznice

10.1 Ovu politiku izravno podupiru i ona doprinosi primjeni sljedećih sigurnosnih politika usklađenih za SME:

10.1.1 P2S – Politika uloga i odgovornosti u upravljanju: dodjeljuje odgovornost za odobravanje aplikacija, provedbu politike i upravljanje dobavljačima.

10.1.2 P4S – Politika kontrole pristupa: osigurava da je pristup aplikacijama usklađen s načelom najmanjih privilegija i načelima upravljanja sesijama.

10.1.3 P8S – Politika podizanja svijesti i osposobljavanja o informacijskoj sigurnosti: osigurava da su korisnici i razvojni inženjeri osposobljeni za prepoznavanje i prijavljivanje prijetnji povezanih s aplikacijama.

10.1.4 P17S – Politika zaštite podataka i privatnosti: utvrđuje zaštitne mjere privatnosti podataka koje mora primjenjivati svaka aplikacija koja obrađuje osobne podatke.

10.1.5 P14S – Politika zadržavanja i zbrinjavanja podataka: uređuje kako se dnevnički zapisi, sigurnosne kopije i osjetljivi podaci koje generiraju aplikacije moraju zadržavati, arhivirati i sigurno uništavati.

10.1.6 P30S – Politika odgovora na incidente: utvrđuje korake za prepoznavanje, prijavljivanje i ograničavanje sigurnosnih događaja povezanih s aplikacijama.

10.2 Zajedno, ove politike osiguravaju da je sigurnost aplikacija u potpunosti integrirana u sustav upravljanja informacijskom sigurnošću (ISMS) organizacije i spremna za reviziju.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001

11.1.1 Točka 8.1 – Zahtijeva da organizacije uspostave operativne kontrole za upravljanje rizicima informacijske sigurnosti, uključujući rizike povezane s aplikacijama i softverskim sustavima.

11.2 ISO/IEC 27002

11.2.1 Kontrola 8.25 – Preporučuje primjenu praksi sigurnog dizajna, razvoja i pregleda koda u svim aplikacijama, uključujući one koje isporučuju dobavljači.

11.2.2 Kontrola 8.26 – Preporučuje formalno testiranje kontrola sigurnosti aplikacija, osobito u područjima koja uključuju kontrolu pristupa, provjeru unosa i upravljanje sesijama.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Utvrđuje zahtjeve za testiranje od strane razvojnih inženjera, analizu koda i dinamičko skeniranje aplikacija prije uvođenja.

11.3.2 SI-10 – Obuhvaća otkrivanje i sprječavanje uobičajenih nedostataka softvera, uz naglasak na osviještenost razvojnih inženjera i tehničke zaštitne mjere.

11.4 GDPR EU (2016/679)

11.4.1 Članak 25 – „Zaštita podataka u fazi projektiranja i prema zadanim postavkama” nalaže ugrađivanje privatnosti i sigurnosti u temeljni dizajn aplikacija koje obrađuju osobne podatke.

11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Članak 21(2)(a) i (e) – Zahtijeva da ključni i važni subjekti provode tehničke mjere za zaštitu aplikacija i otkrivanje rizika povezanih sa softverom.

11.6 Uredba EU DORA (2022/2554)

11.6.1 Članak 9(2)(c), 10(2)(c) – Zahtijeva da SME subjekti u financijskom sektoru ugrađuju sigurnosne kontrole na razini aplikacija i provode redovite procjene radi održavanja digitalne operativne otpornosti.

11.7 COBIT 2019

11.7.1 BAI03 – „Manage Solutions Identification and Build" daje smjernice za razvoj ili nabavu sigurnog softvera usklađenog s rizicima, usklađenošću i poslovnim zahtjevima, uključujući SME okruženja s ograničenim resursima.