					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P25					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 regulativom

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točka 8	—
ISO/IEC 27002:2022	Kontrole 8.25–8.28	—
NIST SP 800-53 Rev.5	SA-11, SA-15, SI-10	—
GDPR EU	Članci 25, 32	—
Direktiva EU NIS2	Članci 21(2)(f), 23	—
Uredba EU DORA	Članci 9, 11	—
COBIT 2019	BAI03, BAI09, DSS05	—

1. Svrha

1.1 Ova politika definira obvezne sigurnosne zahtjeve na razini aplikacijskog sloja za softver koji organizacija razvija, nabavlja, integrira ili uvodi u uporabu. Njome se osigurava da su sve aplikacije projektirane, implementirane i održavane u skladu s načelima sigurnog razvoja, regulatornim obvezama i apetitom za rizik organizacije.

1.2 Ova politika propisuje uključivanje sigurnosti tijekom cijelog životnog ciklusa aplikacije, uključujući autentifikaciju korisnika, postupanje s podacima, zaštitu sučelja i sigurnu interakciju sa sučeljima za programiranje aplikacija i uslugama.

1.3 Primjenom ove politike organizacija nastoji spriječiti uvođenje softverskih ranjivosti, zaštititi osjetljive informacije te osigurati sljedivost i otpornost na iskorištavanje i zlouporabu.

2. Područje primjene

2.1 Ova politika primjenjuje se na sljedeće:

2.1.1 interno razvijene ili izvana nabavljene aplikacije, uključujući SaaS i namjenski razvijene alate

2.1.2 aplikacije koje podržavaju kritične poslovne operacije, korisnički pristup ili obradu reguliranih podataka

2.1.3 razvojne, DevOps, QA, produktne i sigurnosne timove

2.1.4 razvojne inženjere trećih strana, dobavljače softvera i integracijske partnere koji imaju pristup aplikacijama organizacije ili sučeljima za programiranje aplikacija

2.2 Ova politika primjenjuje se u svim okruženjima: razvojnom, testnom, pripremnom, produkcijskom i okruženju za oporavak od katastrofe, neovisno o tome jesu li sustavi smješteni u vlastitim prostorijama, u privatnim podatkovnim centrima ili u javnom oblaku.

3. Ciljevi

3.1 Definirati osnovne funkcionalne i nefunkcionalne sigurnosne zahtjeve koje moraju ispuniti sve aplikacije, neovisno o načinu razvoja ili tehnološkom sklopu.

3.2 Osigurati integraciju zaštitnih mehanizama na razini aplikacijskog sloja, uključujući provjeru ulaznih podataka, kodiranje izlaza, obradu pogrešaka i sigurnost sesija.

3.3 Zahtijevati sigurnu implementaciju mehanizama autentifikacije, autorizacije i kontrole pristupa usklađenih s politikama upravljanja identitetima i pristupom organizacije.

3.4 Propisati sigurnu interakciju sa sučeljima za programiranje aplikacija, web sučeljima i komponentama trećih strana primjenom odobrenih protokola i sigurnosnih kontrola.

3.5 Omogućiti rano otkrivanje i ublažavanje ranjivosti putem statičke i dinamičke analize, pregleda koda i modeliranja prijetnji.

3.6 Zaštititi osjetljive podatke u skladu s regulatornim zahtjevima primjenom enkripcije, klasifikacije i pravila zadržavanja podataka.

3.7 Osigurati kontinuiranu provjeru sigurnosnog profila aplikacija nakon puštanja u produkciju putem testiranja, praćenja i revizijske spremnosti.

4. Uloge i odgovornosti

4.1 Glavni direktor informacijske sigurnosti (CISO)

4.1.1 Vlasnik je ove politike i osigurava njezinu usklađenost sa strategijom informacijske sigurnosti i profilom rizika organizacije.

4.1.2 Odobrava sigurnosne zahtjeve za aplikacije i osigurava provedbu obveznih kontrola u funkcijama razvoja i nabave.

4.2 Voditelj sigurnosti aplikacija / voditelj DevSecOps-a

4.2.1 Definira osnovne sigurnosne kontrole i metodologije testiranja za aplikacijske komponente.

4.2.2 Nadzire sigurnu integraciju alata kao što su SAST, DAST, IAST i SCA u proces isporuke softvera.

4.2.3 Održava kontrolni popis sigurnosnih zahtjeva za aplikacije i kriterije provjere.

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

9. Zahtjevi za pregled i ažuriranje

9.1 Ova politika mora se pregledavati najmanje jednom godišnje ili češće kao odgovor na:

9.1.1 objave kritičnih ranjivosti koje utječu na uobičajene okvire ili ovisnosti

9.1.2 ažuriranja regulatornih obveza za sigurnost aplikacija (npr. NIS2, DORA)

9.1.3 veće promjene u praksama razvoja softvera, alatima ili arhitekturi oblaka organizacije

9.1.4 nalaze interne revizije ili vanjskih penetracijskih testiranja

9.2 Pregled vodi voditelj sigurnosti aplikacija, u koordinaciji s CISO-om, voditeljima DevOps inženjeringa, pravnih poslova, nabave i QA-a.

9.3 Sve izmjene moraju biti pod verzijskom kontrolom u registru upravljanja dokumentima ISMS-a i distribuirane svim pogođenim razvojnim i produktnim timovima.

9.4 Prethodne verzije stavljene izvan snage moraju se arhivirati najmanje tri godine radi sljedivosti, mogućnosti revizije i podrške istragama povreda.

10. Povezane politike i poveznice

10.1 P1 – Politika informacijske sigurnosti. Utvrđuje osnovu za zaštitu sustava i podataka, u okviru koje su kontrole na razini aplikacija obvezne radi sprječavanja neovlaštenog pristupa, curenja podataka i iskorištavanja.

10.2 P4 – Politika kontrole pristupa. Definira standarde upravljanja identitetima i sesijama koje sve aplikacije moraju provoditi, uključujući snažnu autentifikaciju, načelo najmanjih privilegija i zahtjeve za pregled pristupa.

10.3 P5 – Politika upravljanja promjenama. Uređuje prijenos aplikacijskog koda i konfiguracija u produkcijska okruženja te osigurava blokiranje neovlaštenih ili netestiranih promjena.

10.4 P17 – Politika zaštite podataka i privatnosti. Zahtijeva da aplikacije primjenjuju zaštitu privatnosti već u fazi projektiranja i osiguraju zakonitu obradu, šifriranje i zadržavanje osobnih i osjetljivih podataka u svim okruženjima.

10.5 P24 – Politika sigurnog razvoja. Pruža širi okvir za ugradnju sigurnosti u životni ciklus razvoja softvera, dok ova politika definira konkretne zahtjeve i tehničke kontrole koje se moraju implementirati na razini aplikacijskog sloja.

10.6 P30 – Politika odgovora na incidente. Propisuje strukturirano postupanje s incidentima sigurnosti aplikacija, uključujući ranjivosti utvrđene nakon uvođenja ili tijekom penetracijskih testiranja, te definira postupke eskalacije, ograničavanja i oporavka.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001:2022

11.1.1 Točka 8.1 – Operativno planiranje i upravljanje: zahtijeva da sigurnost aplikacija bude ugrađena u procese i sustave radi osiguravanja povjerljivosti, cjelovitosti i dostupnosti.

11.2 ISO/IEC 27002:2022

11.2.1 Kontrole 8.25–8.26: detaljno utvrđuju očekivanja za sigurnost na razini aplikacijskog sloja, uključujući prakse sigurnog kodiranja, modeliranje prijetnji, arhitekturne kontrole i provjeru softvera trećih strana.

11.2.2 Kontrola iz Priloga A 8.25 – Životni ciklus razvoja sustava: propisuje integraciju sigurnosti tijekom cijelog životnog ciklusa aplikacije.

11.2.3 Kontrola iz Priloga A 8.26 – Zahtjevi sigurnosti aplikacija: propisuje definiranje i provedbu tehničkih kontrola radi zaštite aplikacija od zlouporabe i kompromitacije.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Security Testing and Evaluation razvojnih inženjera: propisuje statičko, dinamičko i penetracijsko testiranje tijekom razvoja.

11.3.2 SA-15 – Proces razvoja, standardi i alati: uspostavlja formalne standarde za siguran razvoj aplikacija.

11.3.3 SI-10 – Provjera ulaznih podataka: zahtijeva kontrolne mehanizme za sprječavanje napada ubacivanjem koda i napada na parsiranje.

11.4 GDPR EU (2016/679)

11.4.1 Članak 25 – Zaštita podataka po dizajnu i prema zadanim postavkama: zahtijeva integraciju zaštite podataka i privatnosti u logiku aplikacija i radne tokove.

11.4.2 Članak 32 – Sigurnost obrade: propisuje odgovarajuće tehničke mjere, kao što su provjera ulaznih podataka, šifriranje i sigurne kontrole pristupa.

11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Članak 21(2)(f): zahtijeva upravljanje ranjivostima i sigurne prakse tijekom životnog ciklusa aplikacija za ključne i važne subjekte.

11.5.2 Članak 23 – Prijavljivanje sigurnosnih incidenata: zahtijeva mogućnosti zapisivanja događaja i praćenja na razini aplikacijskog sloja radi otkrivanja i prijavljivanja značajnih incidenata.

11.6 Uredba EU DORA (2022/2554)

11.6.1 Članak 9 – Upravljanje IKT rizicima: obvezuje financijske subjekte da osiguraju da su aplikacije sigurne, testirane i otporne na prijetnje kibernetičkoj sigurnosti.

11.6.2 Članak 11 – Testiranje IKT alata: potiče periodična penetracijska testiranja i vježbe crvenog tima za kritične aplikacije i usluge.

11.7 COBIT 2019

11.7.1 BAI03 – Upravljanje identifikacijom i izgradnjom rješenja: uspostavlja zahtjeve projektiranja i kontrola tijekom razvoja aplikacija.

11.7.2 BAI09 – Upravljanje aplikacijama: naglašava sigurno održavanje, praćenje i unapređenje aktivnih aplikacija.

11.7.3 DSS05 – Upravljanje sigurnosnim uslugama: povezuje zaštitu aplikacija sa širim sigurnosnim operacijama i kontrolama organizacije.