TRUST WHITEPAPER · 2026.

SIGURNOST · PRIVATNOST · USKLAĐENOST · UPRAVLJANJE

Inženjerski pristup izgradnji povjerenja.

Kako ITO gradi, održava i upravlja ključnim softverom za državne institucije, javnu sigurnost i kritičnu infrastrukturu.

ISO 9001 | ISO/IEC 27001 | ISO/IEC 27701 | ISO 30301 | Sigurnosna dozvola · Ministarstvo sigurnosti BiH

IT Odjel Mostar d.o.o. · ito.dev/en/trust-center · security@ito.dev

SAŽETAK

Softver kojem institucije mogu vjerovati godinama

Ključnom softveru nije dovoljna samo inovativnost. Potrebni su mu sigurnost, transparentnost, odgovornost i dugoročna predanost.

ITO projektira platforme za institucije kojima su pouzdanost, sigurnost, zaštita podataka i kontinuitet rada presudni: ministarstva, policijska tijela, granične i obavještajne službe, regulatore, zavode za zapošljavanje i gradove.

Ovaj dokument opisuje kako čuvamo to povjerenje. Obuhvaća naše neovisno certificirane sustave upravljanja, sigurnosne kontrole ugrađene u svaku platformu, način na koji institucije zadržavaju potpuno vlasništvo i kontrolu nad podacima, našu arhitekturu i siguran razvojni ciklus te načela kojima se vodimo u primjeni umjetne inteligencije.

Kroz sve se provlači jedno načelo: **institucije zadržavaju kontrolu**. ITO razvija sigurnu, auditabilnu i interoperabilnu tehnologiju. Institucija određuje tko smije pristupiti informacijama, koji tijekovi rada postoje, koliko se dugo podaci čuvaju i tko donosi odluke.

SADRŽAJ

4 × ISO
certificirana sustava upravljanja, neovisno auditirana svake godine

Sigurnosna dozvola
izdana od Ministarstva sigurnosti BiH

Podaci klijenta
svi operativni podaci ostaju u vlasništvu i pod kontrolom institucije

01 · NAŠ MODEL POVJERENJA

Šest stupova povjerenja

01

Sigurnost po dizajnu

Sigurnost je dio cijelog životnog ciklusa softvera: arhitekture, razvoja, uvođenja, nadzora i stalnog unapređenja.

02

Privatnost po dizajnu

Institucije zadržavaju kontrolu nad operativnim podacima. Naše platforme podržavaju zakonitu, transparentnu i odgovornu obradu.

03

Usklađenost

Naši procesi i tehnološke prakse slijede međunarodne standarde kvalitete, informacijske sigurnosti, privatnosti i upravljanja informacijama.

04

Interoperabilnost

Sigurna, standardizirana sučelja prema postojećim državnim sustavima, registrima, senzorima i infrastrukturi.

05

Auditabilnost

Kritične radnje, aktivnosti korisnika i administrativne izmjene bilježe se radi odgovornosti i sljedivosti.

06

Odgovorne inovacije

Tehnologija podupire ljudske odluke, čini institucije učinkovitijima i jača povjerenje javnosti.

Institucija određuje. Platforma omogućuje.

Zakonodavstvo

Pravni okvir određuje ovlasti i obveze institucije.

→

Institucija klijent

- Politike i postupci
- Korisničke uloge i ovlasti
- Pravila čuvanja podataka
- Odobrenja i operativne odluke

→

ITO platforma

- Sigurnost i audit
- Tijekovi rada i obavijesti
- Integracije i API-ji
- Izvještavanje

> ITO gradi siguran softver. Svaka institucija ostaje odgovorna za svoja operativna pravila, korisničke ovlasti, politike čuvanja podataka i zakonitu uporabu sustava te ostaje vlasnik i voditelj svojih podataka, postupaka i odluka.

02 · CERTIFIKATI I STANDARDI

Neovisno provjereno

Za nas usklađenost nije jednokratni certifikat. To je način na koji se softver razvija, projekti vode i informacije štite. Naša četiri sustava upravljanja svake godine auditiraju neovisna certifikacijska tijela.

ISO 9001

UPRAVLJANJE KVALITETOM

Strukturirana isporuka projekata, zadovoljstvo klijenata i stalno unapređenje, uz upravljanje kvalitetom ugrađeno u svaku fazu razvoja softvera.

Provjera kod SGS-a ↗

ISO/IEC 27001

UPRAVLJANJE INFORMACIJSKOM SIGURNOŠĆU

Okvir za prepoznavanje, upravljanje i stalno smanjivanje rizika informacijske sigurnosti u cijeloj organizaciji.

Provjera kod RIGCERT-a ↗

ISO/IEC 27701

UPRAVLJANJE PRIVATNOŠĆU INFORMACIJA

Proširuje naš sigurnosni okvir strukturiranim upravljanjem privatnošću i odgovornošću za osobne podatke.

Provjera kod RIGCERT-a ↗

ISO 30301

UPRAVLJANJE INFORMACIJAMA

Upravljanje životnim ciklusom informacija i dokumentacije organizacije, kako bi bile točne, dostupne i pravilno vođene.

Provjera kod RIGCERT-a ↗

Sigurnosna dozvola · Ministarstvo sigurnosti Bosne i Hercegovine

ITO posjeduje sigurnosnu dozvolu koju je izdalo Ministarstvo sigurnosti BiH i radi s institucijama iz policijskog, graničnog i obavještajnog sektora.

STANDARDI I OKVIRI KOJE SLIJEDIMO

- OWASP Secure Coding Practices i OWASP Top 10
- Microsoft Secure Development Lifecycle
- NIST Cybersecurity Framework (gdje je primjenjivo)
- Zero Trust načela i Privacy by Design
- Dobre prakse za REST API, OpenAPI, OAuth2, JWT

CIKLUS STALNOG UNAPREĐENJA

- Godišnji certifikacijski auditi i upravine ocjene
- Procjene rizika i interni auditi
- Korektivne radnje i optimizacija procesa
- Sigurnosna svijest i zrelost sigurnog razvoja

U PLANU

SOC 2 · Usklađivanje s ISO/IEC 42001 · Certifikat za siguran razvoj softvera

03 · SIGURNOST

Sigurnost ugrađena u svaku fazu

Gradimo softver za državne institucije, provedbu zakona i javni sektor, gdje su povjerljivost, cjelovitost i dostupnost informacija presudni. Sigurnost se promišlja u svakoj fazi, od početne arhitekture do dugoročnog održavanja.

Povjerljivost

Osjetljivim informacijama mogu pristupiti samo ovlašteni korisnici s jasno određenim odgovornostima, uz RBAC, snažnu autentifikaciju i detaljne ovlasti.

Cjelovitost

Mehanizmi audita, kontrole valjanosti i sljedivost štite operativne podatke i digitalne dokaze od neovlaštenih izmjena.

Dostupnost

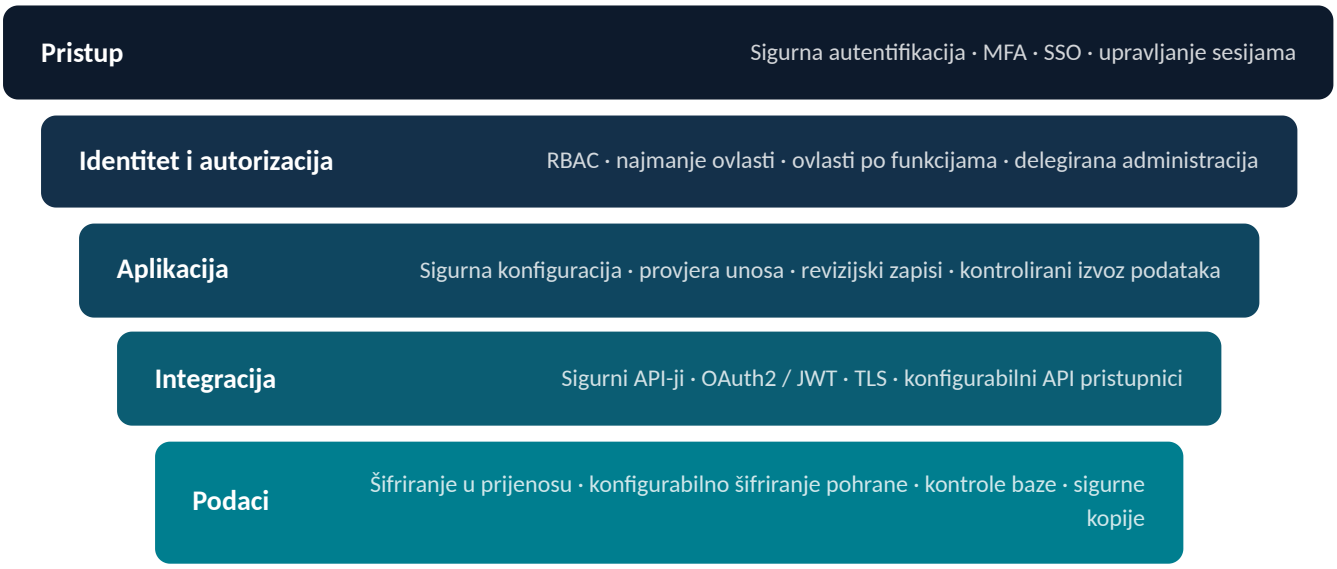
Redundancija, sigurnosne kopije, planiranje oporavka od katastrofe i instalacije visoke dostupnosti održavaju ključne sustave u radu kada su najpotrebniji.

Odgovornost

Svaka kritična radnja može se pripisati autentificiranom korisniku, a sveobuhvatni revizijski zapisi podupiru upravljanje i regulatornu usklađenost.

Višeslojna zaštita

Sustavima javnog sektora potrebno je više slojeva zaštite, a ne jedan zaštitni mehanizam. Naša arhitektura kombinira komplementarne kontrole na razini pristupa korisnika, aplikacija, integracija i podataka.



Upravljanje identitetom i pristupom

- Integracija s Microsoft Active Directoryjem i LDAP-om
- Jedinstvena prijava i višefaktorska autentifikacija gdje je potrebno
- Organizacijska hijerarhija i ovlasti temeljene na ulogama
- Delegirana administracija i detaljna autorizacija po funkcijama

Prava pristupa definiraju i održavaju isključivo ovlašteni djelatnici institucije klijenta.

Zaštita podataka

- TLS šifrirana komunikacija i sigurna API autentifikacija
- Sigurnosne kontrole baze podataka i šifriranje osjetljivih podataka
- Sigurni postupci izrade kopija i sigurna pohrana dokumenata
- Zaštita digitalnih dokaza i kontrolirani izvoz podataka

Vlasništvo nad podacima uvijek ostaje instituciji klijentu.

Audit i sljedivost

Potpuna vidljivost administrativnih i operativnih aktivnosti podupire odgovornost, forenzičku analizu i operativno upravljanje. Bilježimo:

- Događaje autentifikacije korisnika
- Administrativne i konfiguracijske izmjene
- Radnje u tijekovima rada i sistemske događaje
- Obradu dokaza i životni ciklus dokumenata
- API interakcije

Sigurna interoperabilnost

Integracije nikada ne smiju oslabiti sigurnost. Naše se platforme s vanjskim sustavima povezuju putem:

- REST API-ja sa specifikacijama OpenAPI
- OAuth2 i JWT autentifikacije
- TLS šifriranja s kraja na kraj
- Konfigurabilnih API pristupnika i sigurnih integracija servisa

Sigurnost je zajednička odgovornost

ITO isporučuje siguran, otporan i interoperabilan softver. **Institucije klijenti** određuju operativne politike, korisničke ovlasti, pravila čuvanja podataka i zakonitu uporabu sustava.

Odgovorno prijavljivanje ranjivosti

Sigurnosni upiti, prijave ranjivosti i zahtjevi za dokumentacijom: **security@ito.dev**

Sigurno po dizajnu · Višeslojna zaštita · Najmanje ovlasti · Zero Trust načela · Privatnost po dizajnu · Auditabilnost · Sigurne integracije · Odgovorno prijavljivanje ranjivosti · Stalno unapređenje

Privatnost od prve linije arhitekture

Naš je softver osmišljen za zakonitu obradu, institucionalno upravljanje i dugoročnu zaštitu podataka građana. Privatnost se promišlja od najranijih faza arhitekture sustava, a ne dodaje nakon razvoja.

Vlasništvo nad podacima

Institucije su vlasnici svojih operativnih podataka. ITO obrađuje informacije u njihovo ime, a vlasništvo, upravljanje i kontrola ostaju instituciji.

Ograničenje svrhe

Informacije se obrađuju samo za jasno određene institucionalne svrhe, bez nepotrebne obrade.

Smanjenje količine podataka

Sustavi obrađuju samo ono što je potrebno za ovlaštene zadatke, a vidljivost se može prilagoditi svakoj organizacijskoj ulozi.

Transparentnost

Administrativne radnje su sljedive i provjerljive kroz revizijske zapise kritičnih događaja.

Odgovornost

Tehnologija podupire odgovornost institucije. Ne zamjenjuje je.

Uloge i odgovornosti

INSTITUCIJA KLIJENT	ITO
Voditelj obrade podataka	Razvoj i održavanje softvera
Upravljanje korisnicima i odobravanje pristupa	Sigurnosna ažuriranja
Operativne politike i unutarnje upravljanje	Tehnička podrška i dokumentacija
Zakonska usklađenost i pravna osnova obrade	Sistemska integracija
Čuvanje podataka i postupci autorizacije	Kvaliteta proizvoda i sigurna arhitektura

> Institucija određuje korisničke uloge, organizacijsku hijerarhiju, ovlasti, politike čuvanja podataka, pravnu osnovu obrade, postupke odobravanja, politike revizije i koje su integracije dopuštene. ITO osigurava platformu koja ta pravila provodi u praksi.

Privatnost po dizajnu u šest načela

01
Smanjenje količine podataka
Obrađuju se samo informacije potrebne za operativne svrhe.

02
Ograničenje pristupa
Ovlasti koje definira klijent određuju tko što vidi.

03
Podjela dužnosti
Administrativne odgovornosti mogu se rasporediti na više uloga.

04
Auditabilnost
Kritične radnje ostaju sljedive.

05
Sigurna komunikacija
Podaci koji se razmjenjuju među sustavima zaštićeni su u prijenosu.

06
Prilagodljivo čuvanje
Rokovi čuvanja slijede važeće propise i politiku institucije.

Životni ciklus podataka pod kontrolom institucije

01	02	03	04	05	06	07
Prikupljanje	Provjera	Obrada	Pohrana	Operativna uporaba	Arhiviranje	Brisanje

Svaka faza slijedi politike koje određuje institucija. Naš pristup vode načela GDPR-a, Privacy by Design, ISO/IEC 27701, ISO/IEC 27001 i dobre prakse upravljanja informacijama.

Česta pitanja

Tko je vlasnik operativnih podataka?
Institucija klijent. ITO ne stječe vlasništvo nad operativnim podacima klijenta.

Odlučuje li ITO tko smije pristupiti informacijama?
Ne. Ovlasti definiraju i održavaju isključivo ovlašteni djelatnici institucije klijenta.

Mogu li institucije same podesiti politike čuvanja?
Da. Rokovi čuvanja slijede važeće propise i interne politike upravljanja.

Pristupa li ITO operativnim podacima?
Samo kada to institucija izričito odobri radi održavanja, otklanjanja kvarova ili podrške, i uvijek u skladu s ugovornim obvezama i sigurnosnim postupcima.

05 · ARHITEKTURA

Modernizacija bez zamjene

Naše arhitekture omogućuju institucijama da moderniziraju rad bez zamjene sustava koje već imaju. Naša inženjerska filozofija počiva na otvorenosti, interoperabilnosti i dugoročnoj održivosti.

01

Modularno po dizajnu

Neovisni funkcionalni moduli, uvedeni po potrebi, koji zajedno rade kao jedan integrirani ekosustav.

02

Najprije interoperabilnost

Osmišljeno za sigurnu integraciju s postojećim registrima, bazama podataka, senzorima i poslovnim aplikacijama.

03

Neovisnost o proizvođaču

Radi s različitim hardverom, operacijskim sustavima i protokolima, bez vezivanja uz jednog proizvođača.

04

Skalabilnost

Od jednog odjela do nacionalnog uvođenja, uz isti model sigurnosti i upravljanja.

05

Sigurnost kroz arhitekturu

Identitet, kontrola pristupa, sigurni API-ji, šifriranje, auditabilnost, nadzor i otpornost arhitektonske su odluke.

06

Operativna otpornost

Visoka dostupnost, kopije i oporavak, distribuirana instalacija te rad bez veze gdje je primjenjivo.

Referentna arhitektura

PRISTUP	Web portali · Mobilne aplikacije · Usluge za građane · Operaterske konzole
PRISTUPNIK	**API pristupnik · servisi identiteta i sigurnosti**
MODULI	Upravljanje predmetima · Registri · Operacije · E-plaćanja · Upravljanje imovinom · Upravljanje posjetiteljima
ZAJEDNIČKI SERVISI	Identiteti i uloge · Organizacijska struktura · Mehanizam tijekova rada · Obavijesti · Audit · Izvještavanje · Konfiguracija · Upravljanje API-jima
INTEGRACIJA	**REST · OpenAPI · MQ · SOAP (gdje je potrebno) · razmjena datoteka · X-Road**
VANJSKI SUSTAVI	Nacionalni registri · Pružatelji identiteta · Platni sustavi · DMS · GIS · LPR / radar · IoT senzori · ERP / BI · Platforme e-uprave · X-Road

05 · ARHITEKTURA

Modeli instalacije

Institucije biraju model instalacije koji odgovara njihovim operativnim i regulatornim zahtjevima.

- Vlastita infrastruktura
- Privatni oblak
- Državni oblak
- Hibridno
- Izolirana okruženja
- Klasteri visoke dostupnosti
- Lokacije za oporavak od katastrofe

Tehnološki stog

BACKEND	.NET · ASP.NET Core · C#
FRONTEND	React · Flutter · Blazor
BAZA PODATAKA	SQL Server · PostgreSQL · Elastic
RAZMJENA PORUKA	RabbitMQ · Azure Service Bus (ako je primjenjivo)
NADZOR	Elastic · Kibana · Prometheus · Grafana
IDENTITET	Active Directory · LDAP · OAuth2 · JWT
API	REST · OpenAPI · Swagger
KONTEJNERI	Docker

Performanse i skalabilnost

- Horizontalno skaliranje i raspodjela opterećenja
- Predmemoriranje i asinkrona obrada
- Distribuirani servisi i pozadinski procesi
- Obrada vođena događajima

Načela protoka podataka

Informacije se trebaju kretati sigurno i samo kada je to potrebno.

- Minimalno kretanje podataka
- Sigurne, šifrirane integracije
- Upravljanje pod kontrolom institucije
- Auditabilnost i sljedivost

Dugoročna održivost

- Otvoreni standardi i neovisnost o proizvođaču
- Kompatibilnost s prethodnim verzijama i modularne nadogradnje
- Prilagodljive integracije
- Postupna digitalna transformacija

Ne gradimo projekte. **Gradimo platforme.**

Ne zamjenjujemo postojeće sustave. **Integriramo ih.**

Ne vežemo klijente uz zatvorene ekosustave. **Gradimo interoperabilne arhitekture.**

Ne gradimo softver za danas. **Razvijamo platforme održive i u sljedećem desetljeću.**

06 · SIGURAN RAZVOJ

Sigurnost je ugrađena, a ne dodana naknadno

Svako ITO rješenje razvija se strukturiranom metodologijom koja spaja softversku arhitekturu, sigurnosni inženjering, osiguranje kvalitete i stalno unapređenje.

01	02	03	04	05	06	07	08	09
Poslovna analiza	Arhitektura rješenja	Sigurnosni pregled	Razvoj	Pregled koda	Testiranje	Uvođenje	Nadzor	Stalno unapređenje

Sigurnosni pregled

Prije implementacije procjenjujemo autentifikaciju, autorizaciju, površinu napada, zaštitu podataka, auditabilnost, integracije i rizike.

Testiranje

Funkcionalno, regresijsko, integracijsko, performansno i sigurnosno testiranje, nakon čega slijedi korisničko testiranje prihvaćanja.

Kontrolirano uvođenje

Provjera uvođenja, provjera konfiguracije, provjere migracije, plan povratka i dokumentacija izdanja.

Razvojni standardi

Kontrola verzija temeljena na Gitu, međusobni pregled koda, CI/CD načela gdje je primjenjivo, sigurno programiranje, čista i slojevita arhitektura te OWASP preporuke.

Upravljanje promjenama

Svaka značajnija promjena prolazi procjenu utjecaja, planiranje, implementaciju, testiranje, odobrenje, uvođenje i pregled.

Siguran lanac opskrbe

Pouzdani, podržani dobavljači i komponente, dokumentirane ovisnosti, praćenje ranjivosti i upravljanje ažuriranjima.

DOKUMENTACIJA KOJA JE DIO PROIZVODA

- Poslovna analiza i funkcionalna specifikacija
- Arhitektonska i API dokumentacija
- Upute za instalaciju i administratorski priručnici
- Korisnički priručnici, bilješke o izdanjima i dnevnici promjena

ŠTO MJERIMO

- Kvaliteta koda
- Sigurnosni nalazi
- Pokrivenost testovima
- Stabilnost izdanja
- Performanse
- Vrijeme otklanjanja grešaka
- Potpunost dokumentacije
- Povratne informacije klijenata

07 · ODGOVORNA UMJETNA INTELIGENCIJA

AI koji pomaže ljudima, a ne zamjenjuje ih

Umjetna inteligencija može poboljšati operativnu učinkovitost, situacijsku svijest i analizu podataka u javnoj sigurnosti. Mora uvijek ostati pod ljudskim nadzorom i unutar pravnog okvira koji određuje nadležna institucija.

01

Ljudski nadzor

Ljudi ostaju odgovorni za odluke. AI analizira, otkriva obrasce i određuje prioritete događaja.

02

Odgovornost

AI ne prenosi pravnu odgovornost s institucija na softver.

03

Transparentnost

Korisnici vide što je pokrenulo preporuku i koje su informacije analizirane.

04

Pravednost

Učinkovitost i relevantnost modela stalno se procjenjuju u okviru institucionalnog upravljanja.

05

Sigurnost

AI servisi zaštićeni su istim kontrolama kao i ostatak platforme.

06

Stalno unapređenje

Modeli, skupovi podataka i ponašanje procjenjuju se i unapređuju tijekom cijelog životnog ciklusa.

Tehnologija smije

- Analizirati
- Povezivati
- Preporučivati
- Određivati prioritete
- Vizualizirati

Tehnologija ne smije samostalno

- Donositi pravne odluke
- Utvrđivati krivnju
- Zamijeniti ovlaštene službenike
- Zaobići institucionalne postupke

AI U PRAKSI (RENATA)

Prepoznavanje registarskih oznaka, klasifikacija vozila, poboljšanje slike, prioritizacija događaja, otkrivanje anomalija i pametna pretraga. Cilj je smanjiti ponavljajući rad, a ne automatizirati institucionalne odluke. AI funkcije su **opcionalne, prilagodljive i mogu se isključiti**.

OBJAŠNJIVOST

Preporuke dolaze s popratnim dokazima, pokazateljima pouzdanosti, povezanim operativnim podacima i sljedivim tijekovima rada.

UPRAVLJANJE

Institucije određuju pravnu osnovu, operativne politike, postupke odobravanja, korisničke ovlasti, opseg uvođenja i prihvatljivu uporabu. Svaka AI mogućnost procjenjuje se s obzirom na operativni, sigurnosni i utjecaj na privatnost.

USKLAĐENO S

- Akt EU o umjetnoj inteligenciji
- OECD načela o AI-ju
- ISO/IEC 42001
- NIST AI RMF
- AI usmjeren na čovjeka

Institucije zadržavaju kontrolu

Tehnologija nikada ne smije određivati ovlasti institucije. Institucije određuju ovlasti, a tehnologija ih omogućuje. Povjerenje nastaje kada su tehnologija, institucije i pravne odgovornosti jasno razdvojene.

Institucije određuju

- Tko smije pristupiti informacijama i što je dostupno
- Koji tijekovi rada, lanci odobravanja i integracije postoje
- Koliko se dugo informacije čuvaju, arhiviraju i brišu
- Organizacijsku strukturu, politike revizije i operativne odluke

ITO je odgovoran za

- Softverski inženjering i sigurnu arhitekturu
- Održavanje proizvoda, kvalitetu i sigurnosna ažuriranja
- Interoperabilnost i tehničku dokumentaciju
- Tehničku podršku

Vlasništvo nad podacima

Operativne informacije ostaju vlasništvo institucije klijenta. ITO ne stječe vlasništvo nad operativnim podacima klijenta.

Otvorena arhitektura

Otvoreni API-ji, dokumentirane integracije i neovisnost o proizvođaču znače da klijenti nikada ne ovise o našim zatvorenim tehnološkim odlukama.

Upravljanje u praksi

Jasno određene odgovornosti, dokumentirani postupci, podjela dužnosti, kontrolirano upravljanje promjenama i stalni nadzor.

Načela kojima se vodimo

- Tehnologija treba osnaživati institucije, a ne ih zamjenjivati.
- Auditabilnost jača odgovornost.
- Interoperabilnost štiti javna ulaganja.
- Transparentnost jača povjerenje.
- Sigurnost štiti povjerenje javnosti.
- Inovacije uvijek trebaju poštovati upravljanje.

GRAĐANI VJERUJU INSTITUCIJAMA. INSTITUCIJE VJERUJU TEHNOLOGIJI.

Tehnologija mora biti dostojna tog povjerenja.

Rado ćemo podijeliti dodatnu sigurnosnu dokumentaciju, odgovoriti na due diligence upitnike i provesti vaš sigurnosni tim kroz bilo koju ITO platformu.

SIGURNOST I PRIJAVA RANJIVOSTI	**security@ito.dev**
TRUST CENTER	**ito.dev/en/trust-center**
OPĆI UPITI	**info@ito.ba · +387 36 830 003**
TVRTKA	**IT Odjel Mostar d.o.o., Mostar, Bosna i Hercegovina**