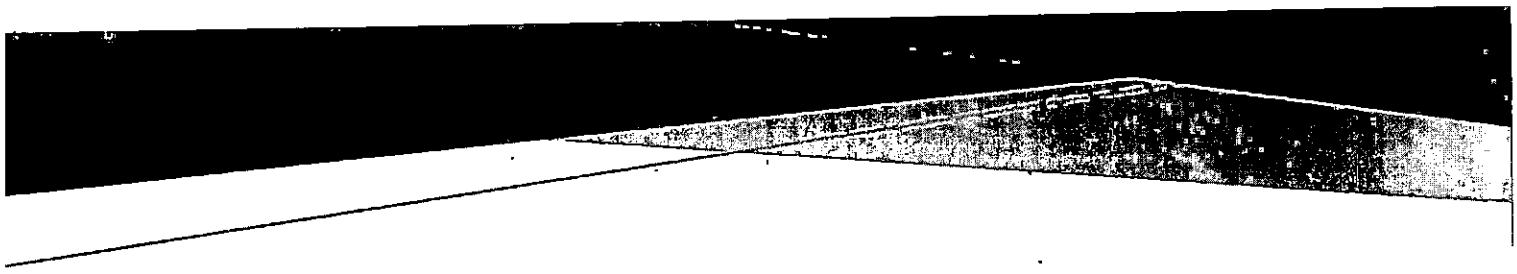

INFORMACIJA O USPJEŠNOSTI IMPLEMENTACIJE AKCIONOG PLANA ZA SPROVOĐENJE INFORMACIONE BEZBJEDNOSTI PREMA STANDARDU ISO 27002 NA NIVOU IPA OKVIRA ZA PERIOD 2025-2027

Ministarstvo finansija/Direktorat za upravljanje strukturama pretpristupne podrške EU

I UVOD

Vlada Crne Gore je, na sjednici održanoj 20. decembra 2024. godine, usvojila Akcioni plan za sprovođenje informacione bezbjednosti prema standardu ISO 27002 na nivou IPA okvira za period 2025-2027, koji je pripremljen od strane Ministarstva finansija u saradnji sa relevantnim institucijama. Naime, zaključkom Vlade br. 10-908/24-6659/4, Ministarstvo finansija/Direktorat za upravljanje strukturama pretpristupne podrške EU i Ministarstvo javne uprave zaduženi su za praćenje implementacije Akcionog plana za sprovođenje informacione bezbjednosti prema standardu ISO 27002 na nivou IPA okvira.

Struktura Predloga Akcionog plana ISO 27002 na nivou IPA okvira sastoji se od definisanih oblasti, te 16 osnova, sa jasno naznačenim ciljevima, mjerama, aktivnostima, odgovornostima i zaduženjima, rokovima za implementaciju mjera, neophodnim sredstvima i indikatorima.

Usvajanjem Akcionog plana ISO 27002 za IPA okvir, od strane Vlade Crne Gore, obezbijeđen je set konkretnih mjera informacione bezbjednosti za postizanje najvišeg nivoa informacione bezbjednosti mrežnih i informacionih sistema IPA struktura, uključujući sajber bezbjednost, podizanje svijesti službenika na IPA poslovima o važnosti stanja povjerljivosti, cjelovitosti, dostupnosti i zaštite podataka, što ispunjava početni zahtjev Evropske komisije u odnosu na date preporuke u ovoj oblasti, kada je u pitanju upravljanje sredstvima Evropske unije kroz Instrument pretpristupne podrške (IPA). Akcioni plan predstavlja ključni instrument za uspostavljanje i operativnu implementaciju Sistema za upravljanje bezbjednošću informacija (ISMS) u okviru svih institucija koje djeluju pod nadležnošću Instrumenta pretpristupne pomoći (IPA), uz podršku Ministarstva javne uprave.

U skladu sa obavezama definisanim Akcionim planom za sprovođenje informacione bezbjednosti prema standardu ISO/IEC 27001-27002, ali i Programom rada Vlade Crne Gore za 2025. godinu, predviđeno je dostavljanje analize o statusu realizacije aktivnosti u III kvartalu 2025. godine.

Implementacija ISMS-a u IPA strukturama nije samo tehničko pitanje već predstavlja strateški proces upravljanja informacijama, kojim se obezbjeđuje integritet, povjerljivost i dostupnost podataka od značaja za dio državne uprave i projekte finansirane iz evropskih fondova. ISO politika informacione bezbjednosti, u ovom kontekstu, služi kao okvir za usklađivanje internih procedura sa međunarodnim standardima, jačanje institucionalne otpornosti i transparentnosti u radu IPA tijela.

II OPŠTI PREGLED

Cilj ove Informacije je da Vladi Crne Gore pruži pregled ostvarenih rezultata do sada, identifikaciju ključnih izazova u procesu implementacije, planirane aktivnosti u narednom periodu, preporuke za unaprijeđenje operativne i regulatorne implementacije sistema za upravljanje bezbjednošću informacija. Do trećeg kvartala 2025. godine, realizovan je značajan dio aktivnosti definisanih Akcionim planom i predstavljen je u nastavku prema uočenom napretku u ostvarenju operativnih ciljeva i ispunjavanju indikatora.

III OPŠTI DIO - NAPREDAK O OSTVARENJU CILJEVA IZ OBLASTI USPOSTAVLJANJA OKVIRA ZA MONITORING I IMPLEMENTACIJU ISMS-a I AKCIONOG PLANA

Implementacija i širenje Sistema za upravljanje bezbijednošću informacija (ISMS) uključuje uspostavljanje, upravljanje i kontinuirano poboljšanje okvira za bezbjednost informacija organizacije zasnovanog na standardu ISO/IEC 27002. ISMS je dizajniran da zaštiti povjerljivost, integritet i dostupnost informacija primjenom procesa upravljanja rizikom. Implementacija i širenje ISMS-a je strateški projekat koji zahtijeva posvećenost u cijeloj organizaciji, od najvišeg menadžmenta do svakog zaposlenog. Ovaj Akcioni plan navodi ključne korake za uspostavljanje robusnog ISMS-a, sa ciljem da efektivno zaštiti informaciona sredstva uz obezbjeđivanje usklađenosti sa međunarodnim standardima i propisima. Instance za koje je ovaj Akcioni plan primjenljiv čine veoma složen ekosistem zbog njihove međuzavisnosti u realizaciji IPA projekata, različitih nivoa složenosti i različitog nivoa ovlašćenja koje imaju nad svojim odgovornostima za bezbjednost informacija. Ovo je razlog što ova oblast obuhvata sve procese koje treba da usmjerava, prati i ocjenjuje Direktorat za upravljanje strukturama pretpristupne podrške EU u Ministarstvu finansija, prepoznat kao Upravljačka struktura u IPA III perspektivi.

Ključne aktivnosti za ovu oblast uključuju:

III-1 Stupanje na snagu IS politike

U skladu sa definisanim obavezama iz Akcionog plana, ključna aktivnost, koja predstavlja okvir za pravovremeno upravljanje bezbjednošću informacija jeste donošenje Politike bezbjednosti informacija. Ova aktivnost je realizovana u saradnji sa ekspertom angažovanim na projektu tehničke podrške Direktoratu za upravljanje strukturama pretpristupne podrške EU u Ministarstvu finansija, te kroz saradnju sa Ministarstvom javne uprave i predstavnicima IPA tijela. Politika važi za sve procese i informacije povezane sa IPA fondovima, za sve zaposlene, izvođače i treće strane, kao i za sve vrste informacionih sredstava (informacije, hardver, softver, podaci i usluge). Funkcionalni stubovi ove politike odnose se na: **Upravljanje sredstvima** (imenovanje vlasnika informacija; inventar i klasifikacija podataka po sistemu: „strogo povjerljivo, povjerljivo, interno, javno"; zaštita tokom čuvanja/obrade/prenosa), **Kontrolu pristupa** (periodični pregledi i brzo ukidanje pristupa), **Ljudski faktor** (obuke, jasne odgovornosti, disciplinski okvir), **Prihvatljivu upotrebu** (pravila za rad na daljinu, lozinke, e-poštu, internet, USB, backup i zaštitu ličnih podataka), **Upravljanje promjenama** (klasifikacija promjena, CAB, procjena rizika, testiranje i „rollback" plan), **Fizičku bezbjednost** (kontrole ulaza, „clear desk", nadzor, zaštita opreme i arhive), **Upravljanje incidentima** (obavezno i hitno prijavljivanje, klasifikacija, tim za odgovor, istraga, obnova i učenje).

Značaj usvojene Politike bezbjednosti informacija predstavlja zajednički „minimum" zaštite za sva IPA tijela, čime se obezbjeđuje dosljednost i smanjuje rizik od različitih praksi, što su i zahjtevi Evropske komisije kada je riječ o IPA fondovima.

Nakon odobrenja politike od strane Nacionalnog službenika za ovjeravanje (NAO), ista je stupila na snagu 1. avgusta 2025. godine i dostavljena svim IPA tijelima, koja su Upravljačkoj sturkturi

dostavila Interne distributivne liste o preuzimanju referentnog dokumenta. Politika je podložna konstantnom unaprijeđivanju i ažuriranju od strane svih IPA tijela, ukoliko je to neophodno.

III -2 Imenovanje službenika za ISMS u svim IPA tijelima

Uloga službenika za sistem upravljanja informacionom bezbjednošću (ISMS) uspostavlja se radi obezbjeđivanja pune primjene i nadzora nad sprovođenjem Politike informacione bezbjednosti u okviru svakog IPA tijela. Imenujući ovu osobu, tijelo obezbjeđuje postojanje jasno definisane odgovornosti za koordinaciju aktivnosti i nadzor nad poštovanjem utvrđenih principa i procedura. Predstavnik djeluje kao kontakt tačka između svog tijela i nadležnih centralnih struktura (kasnije Upravnog odbora za praćenje AP), obezbjeđujući pravovremeno izvještavanje, razmjenu informacija i usklađivanje rada sa jedinstvenim okvirom informacione bezbjednosti.

Njegova uloga obuhvata i stalno praćenje stanja informacione bezbjednosti, uključivanje u procjene rizika i praćenje sprovođenja odgovarajućih mjera, kao i iniciranje i koordinaciju aktivnosti vezanih za postupanje u slučaju incidenata i promjena koje imaju uticaj na bezbjednost informacija. Predstavnik je zadužen i za učešće na obukama i sprovođenje ostalih aktivnosti kojima se podiže svijest zaposlenih, čime se obezbjeđuje da Politika ne ostane samo formalni dokument, već da bude sastavni dio svakodnevne prakse.

Na taj način, ISMS službenik, na nivou IPA tijela, ima ključnu ulogu u obezbjeđivanju dosljedne primjene politike, jačanju odgovornosti unutar organizacije i uspostavljanju trajne kulture bezbjednosti informacija.

U cilju realizacije ove aktivnosti koja se odnosi na imenovanje predstavnika za ISMS u svim IPA tijelima, Nacionalni službenik za ovjeravanje (NAO) uputio je zahtjev svim relevantnim IPA tijelima za imenovanje službenika koji će biti zaduženi za praćenje ISMS u svojim jedinicama. Ovaj zahtjev je definisan i prethodno odobrenom Politikom informacione bezbjednosti (1.PO.01), koja je stupila na snagu 1. avgusta 2025. godine. Sva IPA tijela su dostavila dokaze o imenovanju službenika za implementaciju ISMS u okviru njihovih jedinica.

IV REALIZOVANE AKTIVNOSTI PO OSNOVAMA I BUDUĆE AKTIVNOSTI ZA USPJEŠNU IMPLEMENTACIJU AKCIONOG PLANA

Implementacija Akcionog plana bezbjednosne politike u IPA institucijama na osnovu ISO standarda 27002 dodatno će biti ostvarena realizacijom ostalih aktivnosti i to prvo - donošenjem Rješenja o obrazovanju Odbora za praćenje realizacije Akcionog plana, nakon što prethodno bude upućen zahtjev da IPA tijela/institucije imenuju članove projektnog tima prema datim instrukcijama i članove Upravnog odbora na nivou visoko-rukovodnog kadra. Nakon toga se očekuje da nacionalno IPA tijelo, u ovom slučaju Nacionalni službenik za ovjeravanje, dostavi informaciju o usvojenoj odluci Evropskoj komisiji. Kada je riječ o uspostavljanju linije izvještavanja o realizaciji Akcionog plana, ovaj cilj će biti ispunjen i definisan gore navedenim rješenjem i detaljno razrađen u sekciji zadaci odbora.

Biće kreirane instrukcije za redovno izvještavanje prema Upravnom odboru i nadležnim tijelima, uključujući mjesečne i kvartalne izvještaje. Shodno Akcionom planu, gore navedena IS politika, takođe će biti dostavljena svim članovima Upravnog odbora, na upoznavanje.

Kreiranje akcionog plana za „Uspostavljanje konteksta, upravljanje rizicima i ciljevi“ uključuje strukturirani pristup razumijevanju okruženja u kojem IPA tijela rade, identifikovanje i upravljanje rizicima kao i postavljanje jasnih ciljeva. Nacrt opsega je predložen kao „Usluge i informacije u vezi sa IPA fondovima “i treba ga dalje izvoditi za svako IPA tijelo. U kontekstu upravljanja rizicima, Direktorat za upravljanje strukturama pretpristupna podrška EU organizuje panele za upravljanje rizicima na nivou IPA struktura dva puta u toku godine, na kojima predstavnici IPA jedinica, osim iznošenja generalnih rizika, mogu predstaviti rizike koji se odnose na implementaciju ISMS sistema. Ove aktivnosti će biti prenešene i pri izradi ažuriranog Priručnika o procedurama za IPA tijela, u vezi sa politikom upravljanja rizicima. Aktivnosti poput sprovođenja kontrola na osnovu Plana tretmana rizika, te uspostavljanje praćenja rizika, preuzimanje korektivnih radnji, sprovodi se kontinuirano do kraja 2026. godine, kako je i predviđeno Akcionim planom.

Definisanje i saopštavanje uloga i odgovornosti u oblasti bezbjednosti informacija ključno je za uspostavljanje jasne strukture upravljanja, koja podržava strategiju bezbjednosti informacija organizacije. Kao što je prethodno navedeno, ove aktivnosti će biti realizovane formiranjem projektnih timova i Upravnog odbora sa jasnom segregacijom dužnosti.

Procjena učinka i poboljšanje informacione bezbjednosti je od ključnog značaja da se osigura da su bezbjednosne mjere efektivne i da se razvijaju kako bi odgovorile na nove prijetnje i organizacione promjene. Ova oblast će biti aktuelna nakon određenog perioda funkcionisanja Sistema upravljanja bezbjednošću podataka, a to je najkasnije do kraja 2025. godine. Modaliteti interne revizije i razvijanje strategije će se koristiti, nakon obuka internog osoblja za međusobnu reviziju, te kada proces bude predstavljen organu koji bi vršio internu reviziju ili ukoliko se pokaže neophodnim da podugovarač, kao eksterno osoblje za pružanje ove usluge, bude neophodan da izvrši reviziju. Ova aktivnost će biti sprovedena nakon izrade plana za obavljanje interne revizije.

Kreiranje Akcionog plana za sprovođenje informacione bezbjednosti prema standardu ISO 27002 na nivou IPA okvira, ima za cilj i podizanje svijesti, edukaciju i obuku o bezbjednosti informacija, što je od suštinskog značaja da bi svi članovi organizacije stekli znanje i vještine potrebne za zaštitu informacionih sredstava. Ova inicijativa ima za cilj da podstakne kulturu bezbjednosti, smanji vjerovatnoću bezbjednosnih incidenata i obezbijedi da zaposleni mogu da reaguju na prijetnju na odgovarajući način. U skladu sa navedenim, održavanje prvog seta obuka će biti realizovano po angažovanju eksperta iz ove oblasti.

Kada je riječ o primjeni kontrole ljudi u informacionoj bezbjednosti, ista uključuje uspostavljanje politika, procedura i praksi koje se fokusiraju na ljudske elemente informacione bezbjednosti. Aktivnosti koje se odnose na donošenje politika i ažuriranju procedura, ispunjene su u obimu navedenom u prethodnom dijelu ove Informacije.

Kao što je navedeno u Akcionom planu, upravljanje imovinom je kritična komponenta bezbjednosti informacija, koje se fokusira na identifikaciju, klasifikaciju i zaštitu sredstava organizacije.

Efikasno upravljanje imovinom osigurava da su vrijedne informacije i fizička sredstva na odgovarajući način zaštićeni od prijetnji. Aktivnosti predviđene za ovu osnovu odnose se na

inventar sredstava, klasifikaciju i politiku prihvatljivog korišćenja, a koje se u IPA tijelima već djelimično sprovode, i biće detaljno izvršene na osnovu standarda 27001-2, sekcije A5.9,A5.10, A5.11, A5.12, A5.13, A8.10, A8.11.

Kontrola pristupa je ključna u zaštiti informacionih sredstava organizacije. Kontrola pristupa osigurava da samo ovlašćeni pojedinci imaju pristup određenim resursima, štiteći na taj način osjetljive informacije od neovlašćenog pristupa, otkrivanja i izmjene. Kontrola pristupa se trenutno sprovodi u svim relevantnim IPA jedinicama i ova aktivnost se sprovodi kontinuirano. Detaljna imlementacija politike kontrole pristupa biće primijenjena na osnovu postojeće politike bezbjednosti informacija i daljeg razvijanja matrice kontrole pristupa, koju administratori treba da koriste da bi je primijenili na sredstva u okviru obuhvata.

Upravljanje incidentima kod bezbjednosti informacija podrazumijeva skiciranje strukturisanog pristupa identifikovanju, reagovanju na bezbjednosne incidente i oporavku od njih, kako bi se njihov uticaj minimizirao i spriječile se buduće pojave ovog tipa. Odobrena politika bezbjednosti informacija već predviđa modalitete sprječavanja incidenata, a ova tema ući će i u sastav ažuriranog Priručnika o procedurama. Preostali zadaci, poput zakonitog prikupljanja dokaza u slučajevima koji mogu voditi pravnim postupcima i sprovođenja dubljih analiza većih incidenata, planirani su nakon trećeg kvartala 2025. godine i dalje.

U narednom periodu, nakon pripremnih aktivnosti u oblasti oporavka i pravljenja rezervnih kopija, razviće se politika kontinuiteta poslovanja sa jasno definisanim ciljevima, kao i politika pravljenja rezervnih kopija. Sljedeće aktivnosti odnose se na izradu i implementaciju planova kontinuiteta poslovanja u četvrtom kvartalu 2025. godine, dok je njihovo održavanje, testiranje i ažuriranje predviđeno za 2026. godinu.

U oblasti životnog ciklusa razvoja sistema i upravljanja promjenama planirano je donošenje i primjena procedura za kontrolu promjena, kroz ažurirani Priručnik o procedurama, kao i definisanje bezbjednosnih zahtjeva u okviru životnog ciklusa razvoja sistema. Aktivnosti vezane za pregled procesa upravljanja promjenama, kao i izvještavanje na osnovu definisanih indikatora, planirane su za 2026. godinu.

Kada je riječ o sigurnosti mreže, aktivnosti u ovoj oblasti još nijesu započele, budući da su planirane za drugu polovinu godine. Od trećeg kvartala predviđeno je razvijanje i implementacija politika i procedura za bezbjedan prenos podataka, sprovođenje procjena ranjivosti mreže i jačanje mrežnih servisa, uključujući segmentaciju mreže i strogu kontrolu pristupa. Ove aktivnosti predstavljaju ključne mjere za jačanje otpornosti na mrežne prijetnje.

Sve navedene aktivnosti, uključujući završene i planirane, biće blagovremeno ažurirane u Priručniku o procedurama, kako bi se obezbijedila dosljedna primjena i održavanje usklađenosti sa standardom ISO 27002.

V ZAKLJUČAK

Na osnovu sprovedenih aktivnosti u okviru implementacije Akcionog plana za sprovođenje informacione bezbjednosti prema standardu ISO 27002, može se konstatovati da su u prethodnom periodu realizovane ključne pripremne mjere i stvoreni svi neophodni preduslovi za nastavak primjene Akcionog plana u narednom periodu. Donošenjem Politike informacione bezbjednosti, imenovanjem ISMS predstavnika u IPA tijelima, te razvojem osnovnih politika i procedura, uspostavljen je institucionalni okvir koji omogućava dalju operacionalizaciju mjera predviđenih planom.

S obzirom na navedeno, predlaže se da Vlada Crne Gore usvoji ovu Informaciju i donese odgovarajuće zaključke kojima će potvrditi dosadašnji napredak u implementaciji Akcionog plana, podržati nastavak realizacije preostalih aktivnosti u skladu sa planiranom dinamikom i obavezati sva nadležna tijela da blagovremeno izvještavaju o sprovođenju mjera i obezbijede kontinuirano ažuriranje Priručnika o procedurama, kako bi se održala puna usklađenost sa međunarodnim standardima i zahtjevima Evropske komisije.