Prilog I

Akcijski plan provedbe usklađivanja sustava HAPIH-a s propisanim regulatornim zahtjevima NIS2 direktive

Sadržaj

1. Svrha i načela izrade Akcijskog plana usklađivanja 2
2. Vremenski okvir provedbe usklađivanja (faze) 2
3. Popis aktivnosti Akcijskog plana 3
4. Sažetak prioritetnih aktivnosti Akcijskog plana usklađivanja 9
5. Referentna dokumentacija 10

1. Svrha i načela izrade Akcijskog plana usklađivanja

Akcijski plan usklađivanja izrađuje se temeljem identificiranih nalaza GAP analize te definira konkretne mjere, aktivnosti, resurse i odgovornosti potrebne za jačanje kibernetičke sigurnosti i usklađivanje sustava HAPIH-a s propisanim regulatornim zahtjevima. Plan uključuje vremenski okvir provedbe te prioritizaciju mjera prema razini identificiranog rizika i utjecaju na kontinuitet laboratorijskih i administrativnih funkcija HAPIH-a. Aktivnosti su usmjerene na minimiziranje rizika koji bi mogli ugroziti obradu laboratorijskih uzoraka, upravljanje zdravstveno relevantnim podacima, sigurnost informacijskih sustava te pouzdanost usluga HAPIH-a povezanih sa zaštitom zdravlja i sigurnošću hrane.

2. Vremenski okvir provedbe usklađivanja (faze)

Faza 1 (0. – 2. mjesec projekta usklađivanja): uspostava upravljačkog okvira, ključnih politika, metodologija, registara i ključnih operativnih procedura.
Faza 2 (3. – 4. mjesec projekta usklađivanja): razrada operativnih procedura, radnih uputa, obrazaca zapisa te implementacija mjera, testiranja, revizije i daljnje unaprjeđenje sustava kibernetičke sigurnosti.

3. Popis aktivnosti Akcijskog plana

ID	Mjera / UKS	Aktivnost	Ishod/Dokaz	Odgovornost	Resursi provedbe	Prioritet	Mjesec projekta
AP-01	1	Formalno potvrditi upravljački okvir kibernetičke sigurnosti (mandat, ovlasti, odgovornosti) i uskladiti interne akte o ulozi odgovorne osobe za kibernetičku sigurnost	Odluka/akt uprave; opis uloga i odgovornosti; imenovanja/ovlaštenja, kroz sistematizaciju radnih mjesta ili novi interni akt.	Uprava HAPIH-a	Voditelj informacijske sigurnosti, CISO;	VISOK	0. - 2.
AP-02	1	Izraditi i usvojiti krovnu Politiku kibernetičke sigurnosti (s pripadajućim tematskim politikama ili kao zajedničku integriranu politiku kibernetičke sigurnosti)	Usvojena politika/tematske politike; objava i dostupnost zaposlenicima. Tematske politike specificirane su kroz dokument *„Završno izvješće _GAP_Analiza_20260121“.*	Uprava HAPIH-a	Voditelj informacijske sigurnosti, CISO;IT podrška; Vlasnici procesa	VISOK	0. - 2.
AP-03	2	Uspostaviti metodologiju upravljanja informacijskom imovinom i Registar informacijske imovine	Metodologija; Registar; Klasificirana informacijska imovina po kritičnosti	Uprava HAPIH-a;	Voditelj informacijske sigurnosti, CISO; Vlasnici procesa;	VISOK	0. - 2.
AP-04	3	Izraditi i usvojiti Metodologiju upravljanja rizicima kibernetičke sigurnosti	Metodologija upravljanja rizicima kibernetičke sigurnosti	Uprava HAPIH-a;	Voditelj informacijske sigurnosti, CISO; IT podrška	VISOK	0. - 2.
AP-05	3	Uspostaviti i voditi Registar rizika kibernetičke sigurnosti	Registar rizika; Plan tretmana rizika	Voditelj informacijske sigurnosti, CISO;	Vlasnici procesa/rizika	VISOK	0. - 2.

ID	*Mjera / UKS*	*Aktivnost*	*Ishod/Dokaz*	*Odgovornost*	*Resursi provedbe*	*Prioritet*	*Mjesec projekta*
AP-06	4	Operacionalizirati upravljanje digitalnim identitetima	Dokumentirana procedura za upravljanje digitalnim identitetima; Evidencije; Revizije	Voditelj informacijske sigurnosti, CISO;	IT podrška	VISOK	0. - 2.
AP-07	4	Izraditi i usvojiti proceduru upravljanja lozinkama i MFA	Usvojena procedura upravljanja lozinkama i MFA	Voditelj informacijske sigurnosti, CISO;	IT podrška	VISOK	0. - 2.
AP-08	4	Formalizirati i objediniti postojeće sigurnosne prakse pri zapošljavanju i odlasku zaposlenika / zaduženje i razduženje opreme i prava pristupa	Usvojena procedura za sigurnosne prakse pri zapošljavanju i odlasku zaposlenika; Evidencije/zapisi o primjeni.	HR	Voditelj informacijske sigurnosti, CISO; IT podrška	SREDNJI	3. - 4.
AP-09	5	Provesti pravila osnovne kibernetičke higijene	Usvojene radne upute iz područja osnovne kibernetičke higijene (detaljno specificirano kroz dokument: *Završno izvješće _GAP_Analiza_20260121*; dostupnost zaposlenicima	Voditelj informacijske sigurnosti, CISO;	IT podrška; Voditelj informacijske sigurnosti, CISO;	VISOK	0. - 2.
AP-10	5	Izraditi Program osposobljavanja zaposlenika na temu kibernetičke sigurnosti	Usvojen program osposobljavanja zaposlenika	HR	Voditelj informacijske sigurnosti, CISO; IT podrška	SREDNJI	3. - 4.
AP-11	5	Uspostaviti sustav učenja na daljinu (eLearning) te evidenciju provedenih edukacija	Evidencije o provedenim edukacijama	HR	Voditelj informacijske sigurnosti,	SREDNJI	3. - 4.

ID	Mjera / UKS	Aktivnost	Ishod/Dokaz	Odgovornost	Resursi provedbe	Prioritet	Mjesec projekta
					CISO; IT podrška		
AP-12	6	Formalizirati i dokumentirati upravljanje sigurnošću mreže	Dokumentirana procedura upravljanja sigurnošću mreže; Evidencije sigurnosnih događaja u pogledu pristupa mrežnoj infrastrukturu HAPIH-a (dokazi o nadzoru mreže / EDR/IDS/IPS evidencije događaja i postupanja po istima)	Voditelj informacijske sigurnosti, CISO;	IT podrška; Voditelj informacijske sigurnosti, CISO;	SREDNJI	3. - 4.
AP-13	7	Formalizirati i dokumentirati logičku i fizičku kontrolu pristupa	Dokumentirana procedura upravljanja logičkom i fizičkom kontrolom pristupa; Evidencije.	Voditelj informacijske sigurnosti, CISO;	IT podrška; Voditelj informacijske sigurnosti, CISO;	VISOK	0. - 2.
AP-14	7	Formalizirati i dokumentirati upravljanje dnevničkim zapisima	Dokumentirana procedura upravljanja dnevničkim zapisima; Evidencije dnevničkih zapisa/arhive	Voditelj informacijske sigurnosti, CISO;	IT podrška; Voditelj informacijske sigurnosti, CISO;	SREDNJI	3. - 4.
AP-15	8	Uspostaviti Registar izravnih IKT dobavljača	Registar dobavljača uspostavljen/dokumentiran	Nabava;	Voditelj informacijske sigurnosti, CISO;IT podrška	VISOK	0. - 2.

ID	*Mjera / UKS*	*Aktivnost*	*Ishod/Dokaz*	*Odgovornost*	*Resursi provedbe*	*Prioritet*	*Mjesec projekta*
AP-16	8	Izraditi i usvojiti proceduru upravljanja izravnim IKT dobavljačima	Dokumentirana procedura upravljanja izravnim IKT dobavljačima	Nabava;	Voditelj informacijske sigurnosti, CISO;IT podrška	VISOK	0. - 2.
AP-17	8	Standardizirati procjenu ugovora s ključnim (izravnim) IKT dobavljačima	Obrazac procjene; Evidencije o provedenim procjenama ugovora/sporazuma s IKT dobavljačima	Pravna služba	Nabava; Voditelj informacijske sigurnosti, CISO; IT podrška	SREDNJI	3. - 4.
AP-18	9	Dopuniti postupak internog razvoja IS sigurnosnim zahtjevima	Dopunjena postojeća procedura internog razvoja ("Postupak za izradu računalnih programa")	Voditelj informacijske sigurnosti, CISO;	Voditelj informacijske sigurnosti, CISO; IT podrška	SREDNJI	3. - 4.
AP-19	9	Uspostaviti proceduru upravljanja promjenama u informacijskim i mrežnim sustavima	Dokumentirana procedura upravljanja promjenama; Evidencija promjena u IS.	Voditelj informacijske sigurnosti, CISO;	Voditelj informacijske sigurnosti, CISO; IT podrška	SREDNJI	3. - 4.
AP-20	10	Izraditi i usvojiti proceduru upravljanja kriptografijom	Usvojena procedura upravljanja kriptografijom	Voditelj informacijske sigurnosti, CISO;	Voditelj informacijske sigurnosti, CISO; IT podrška	SREDNJI	3. - 4.
AP-21	11	Uspostaviti proces upravljanja kibernetičkim incidentima	Razvijena i usvojena procedura za upravljanje	Voditelj informacijske sigurnosti, CISO;	Voditelj informacijske sigurnosti,	VISOK	0. - 2.

ID	Mjera / UKS	Aktivnost	Ishod/Dokaz	Odgovornost	Resursi provedbe	Prioritet	Mjesec projekta
			kibernetičkim incidentima; Evidencije incidenata		CISO; IT podrška		
AP-22	11	Uspostaviti formalni kanal prijave sigurnosnih incidenata, za zaposlenika	Evidencija prijava sigurnosnih incidenata	Voditelj informacijske sigurnosti, CISO;	Voditelj informacijske sigurnosti, CISO; IT podrška	VISOK	0. - 2.
AP-23	12	Izraditi i usvojiti pravila/politika kontinuiteta poslovanja	Usvojena pravila/politika kontinuiteta poslovanja	Uprava HAPIH-a;	Voditelj informacijske sigurnosti, CISO; Vlasnici procesa; IT podrška	VISOK	0. - 2.
AP-24	12	Izraditi Plan kontinuiteta poslovanja (BCP)	Usvojen BCP	Uprava HAPIH-a;	Voditelj informacijske sigurnosti, CISO; Vlasnici procesa; IT podrška	VISOKI	0. - 2.
AP-25	12	Izraditi Plan oporavka IKT sustava (DRP)	Usvojeni DRP	Uprava HAPIH-a;	Voditelj informacijske sigurnosti, CISO; IT podrška	VISOK	0. - 2.
AP-26	12	Provesti testiranja BCP/DRP	Zapisnici testova BCP i DRP planova	Voditelj informacijske sigurnosti, CISO; IT podrška	Voditelj informacijske sigurnosti, CISO; Vlasnici	SREDNJI	3. - 4.

ID	Mjera / UKS	Aktivnost	Ishod/Dokaz	Odgovornost	Resursi provedbe	Prioritet	Mjesec projekta
					procesa; IT podrška		
AP-27	12	Izraditi Plan upravljanja kibernetičkim krizama i komunikacijom - CMCP	Usvojen CMCP plan	Uprava HAPIH-a;	Voditelj informacijske sigurnosti, CISO; Vlasnici procesa; IT podrška	VISOK	0. - 2.
AP-28	13	Izraditi i usvojiti Pravila/Politiku fizičke sigurnosti	Usvojena pravila/politika fizičke sigurnosti	Uprava HAPIH-a;	Voditelj informacijske sigurnosti, CISO; Vlasnici procesa; IT podrška	SREDNJI	3. - 4.
AP-29	Nadzor, Revizije	Uspostaviti metrike, obrasce i praksu izvještavanja Uprave o stanju kibernetičke sigurnosti	Uspostavljena metrika za sustav kibernetičke sigurnosti; Obrasci Izvješća	Voditelj informacijske sigurnosti, CISO;	Voditelj informacijske sigurnosti, CISO;	SREDNJI	3. - 4.
AP-30	Nadzor, Revizije	Uspostaviti i provesti minimalno 2-godišnji ciklus redovitih revizija i ocjene sustava kibernetičke sigurnosti prema propisanim kriterijima i alatima za „važne“ subjekte te izvijestiti nacionalno nadležno tijelo – zakonska obveza.	Definiran Plan obveznih i kontrolnih revizija; Izvješće za nadležno tijelo	Uprava HAPIH-a	Voditelj informacijske sigurnosti, CISO;	SREDNJI	3. - 4.

4. Sažetak prioritetnih aktivnosti Akcijskog plana usklađivanja

Ovaj Akcijski plan usklađivanja jasno je strukturiran prema mjerama Uredbe o kibernetičkoj sigurnosti te raspoređen u dva ključna vremenska razdoblja (trajanja) projekta (0. – 2. mjeseca trajanja projekta usklađenja i 3. – 4. mjeseca trajanja projekta usklađenja), uz jasno definirane prioritete, odgovornosti i ishode.

Najviši prioritet (VISOK) u razdoblju 0. – 2. mjeseca trajanja projekta usklađivanja usmjeren je na uspostavu temeljnih upravljačkih i organizacijskih preduvjeta sustava kibernetičke sigurnosti. To uključuje formalno potvrđivanje upravljačkog okvira i uloge odgovornih osoba za kibernetičku sigurnost (AP-01), izradu i usvajanje krovne Politike kibernetičke sigurnosti i pripadajućih tematskih politika (AP-02), uspostavu metodologije upravljanja informacijskom imovinom i registra informacijske imovine (AP-03) te metodologije upravljanja rizicima i registra rizika kibernetičke sigurnosti (AP-04, AP-05). Ove aktivnosti čine osnovu za sustavno upravljanje kibernetičkim rizicima i predstavljaju preduvjet za sve daljnje tehničke i operativne mjere.

U istom razdoblju prioritetno se provode i ključne **operativne sigurnosne mjere** s izravnim utjecajem na zaštitu informacijskih i mrežnih sustava i podataka, uključujući upravljanje digitalnim identitetima i lozinkama (AP-06, AP-07), provođenje pravila osnovne kibernetičke higijene (AP-09), formalizaciju logičke i fizičke kontrole pristupa (AP-13), uspostavu registra izravnih IKT dobavljača i procedura upravljanja dobavljačima (AP-15, AP-16) te uspostavu procesa i kanala za upravljanje kibernetičkim incidentima (AP-21, AP-22). Također, u ovom razdoblju se izrađuju ključni dokumenti kontinuiteta poslovanja i oporavka (AP-23, AP-24, AP-25, AP-27), čime se osigurava otpornost HAPIH-a na ozbiljne poremećaje i incidente.

Srednji prioritet (SREDNJI) u razdoblju 3. – 4. mjeseca trajanja projekta usklađivanja odnosi se na daljnju operativnu razradu, standardizaciju i jačanje zrelosti sustava. To uključuje formalizaciju sigurnosnih praksi vezanih uz zapošljavanje i odlazak zaposlenika (AP-08), provedbu programa osposobljavanja i e-učenja zaposlenika (AP-10, AP-11), dokumentiranje upravljanja sigurnošću mreže i dnevničkim zapisima (AP-12, AP-14), standardizaciju procjene ugovora s IKT dobavljačima (AP-17) te dopunu procedura internog razvoja i upravljanja promjenama informacijskih sustava (AP-18, AP-19, AP-20).

U završnoj fazi ovog razdoblja naglasak je stavljen na **testiranje, nadzor i kontinuirano poboljšanje**, uključujući provođenje testiranja BCP/DRP planova (AP-26), uspostavu metrika i sustava izvještavanja Uprave o stanju kibernetičke sigurnosti (AP-29) te uspostavu redovitog ciklusa revizija i zakonski obveznog izvještavanja nadležnog tijela (AP-30).

Zaključno, prioritetne aktivnosti Akcijskog plana jasno pokazuju da je fokus u početnoj fazi projekta usklađivanja na uspostavi upravljačkog okvira, politika, metodologija i ključnih registara, dok se u nastavku projektne provedbe sustav nadograđuje kroz operativne procedure, edukaciju zaposlenika, testiranja, nadzor i revizije. Ovakav fazni i prioritetni pristup omogućuje HAPIH-u postupno, ali sustavno jačanje razine kibernetičke sigurnosti i ispunjenje regulatornih zahtjeva uz kontrolirani rizik za kontinuitet poslovanja.

5. Referentna dokumentacija

- Zakon o kibernetičkoj sigurnosti (NN 14/2024)
- Uredba o kibernetičkoj sigurnosti (135/2024)
- Završno izvješće_GAP_Analiza_20260121