Pravilnik o upravljanju uslugama trećih strana

SADRŽAJ

POPIS PRILOGA	
Prilog 1	
Prilog 2	
Prilog 3	

NAPOMENA:

Gore navedeni vezani dokumenti kojih je vlasnik Opća bolnica Varaždin su iz razloga jednostavnosti korištenja izrađeni kao zasebni dokumenti a smatraju se sastavnim dijelom ovog dokumenta. Isti su dostupni osoblju u skladu sa distribucijom pojedinog dokumenta te putem Intranet portala na način da se nalaze u istoj radnoj mapi gdje i ovaj priručnik.

VEZANI DOKUMENTI	
1	Politika sigurnosti informacijskog sustava
2	Pravilnik o primjerenom korištenju informacijskog sustava
3	Pravilnik o udaljenom pristupu informacijskom sustavu
4	Metodologija upravljanja rizicima informacijskog sustava
5	Zakon o tajnosti podataka
6	Uredba o mjerama informacijske sigurnosti
7	Zakon o javnoj nabavi
8	Pravilnik o provedbi postupaka jednostavne nabave
9	Pravilnik o upravljanju informacijskom imovinom
10	
11	

NAPOMENA:

Gore navedeni vezani dokumenti su izrađeni kao zasebni dokumenti nužni za pravilno razumijevanje sadržaja ovog dokumenta ali se ne smatraju njegovim sastavnim dijelom. Isti su dostupni osoblju putem Intranet portala.

Distribucija dokumenta

Broj kopije	Mjesto/lokacija/radno mjesto	Format	Količina	Datum	Potpis
	OPĆA BOLNICA VARAŽDIN				
1	Uprava	Tiskana kopija	1		
N/A	Rukovoditelji organizacijskih jedinica	Digitalna kopija	N/A		

Revizija dokumenta

Redni broj	Datum	Reviziju izradio	Reviziju odobrio	Naziv i broj poglavlja koje se mijenja/opis revizije
1	16.11.2022.	D. Uremović	D. Poljak	Cijelo izdanje

1. Namjena

Ovim dokumentom definirana su pravila upravljanja uslugama trećih strana Opće bolnice Varaždin (u nastavku: OBV ili Bolnica), procjena rizika eksternalizacije te uloge i odgovornosti ključne za provedbu odredbi ovog Pravilnika.

Definirana pravila donesena su u okviru upravljanja sigurnošću informacijskog sustava OBV te su usklađena s poslovnim i sigurnosnim zahtjevima te rezultatima procjene rizika informacijskog sustava OBV.

2. Opseg

Pravilnik o upravljanju uslugama trećih strana obuhvaća sve ugovorne odnose u opsegu ISMS-a koje OBV sklapa s trećim stranama.

Cilj Pravilnika je definirati pravila koja će omogućiti kvalitetno upravljanje uslugama trećih strana te umanjiti rizike informacijskog sustava od neovlaštenog pristupa i zloupotrebe od trećih strana.

3. Upravljanje uslugama trećih strana

Sa svim trećim stranama koje pružaju usluge OBV-u potrebno je sklopiti odgovarajući ugovor koji će osigurati kvalitetno i odgovorno pružanje usluga u skladu s poslovnim i sigurnosnim zahtjevima OBV te pravilima struke. Ugovor se sklapa sukladno zakonskim aktima te internim aktima OBV-a (npr. Pravilnik o provedbi postupaka jednostavne nabave).

Sukladno sustavu upravljanja sigurnošću informacijskog sustava OBV, ugovori s trećim stranama moraju sadržavati minimalno slijedeće elemente:

- jasnu definiciju predmeta ugovora,
- obveze naručitelja i izvršitelja,
- prava pristupa informacijskom sustavu,
- parametre kvalitete/razine pružene usluge i način njihovog mjerenja,
- izjavu o čuvanju poslovne tajne (ili kao sastavni dio ugovora ili kao prilog ugovoru),
- odgovornost za siguran rad s osobnim podacima sukladno GDPR uredbi,
- obvezu suglasnosti OBV-a za podugovaranje izvoditelja,
- trajanje ugovora i otkazni rok,
- ugovorne kazne i jamstva za izvršene usluge, u skladu s izvedivim.

Ukoliko treća strana pruža usluge razvoja softvera, ugovor mora dodatno sadržavati slijedeće odredbe:

- definiranje obveze korištenja sigurnih metoda razvoja softvera u skladu sa najboljim praksama,
- definiranje vlasništva nad programskim kodom.

Organizacijska jedinica OBV koja sklapa ugovor sa trećom stranom dužna je definirati odgovornu osobu koja će biti odgovorna za nadzor parametara ugovora te mjerenje razine pružene usluge u skladu s odredbama ugovora.

Svi ugovori koji se sklapaju sa trećim stranama moraju biti revidirani i odobreni od Uprave OBV i ovlaštene osobe Središnje službe općih, pravnih i kadrovskih poslova.

Organizacijska jedinica odgovorna za sklapanje ugovornog odnosa dužna je upoznati treću stranu i njezine zaposlenike s *Politikom sigurnosti informacijskog sustava* i svim internim aktima te sigurnosnim kontrolama koji se odnose na opseg ugovora i iz njihovog djelokruga rada prije omogućavanja pristupa informacijskom sustavu OBV.

Organizacijska jedinica koja je odgovorna za sklapanje ugovora dužna je s trećom stranom definirati pravila sigurne razmjene informacije i komunikacije na projektu sukladno *Zakonu o tajnosti podataka* i *Uredbi o mjerama informacijske sigurnosti*.

Pravila udaljenog pristupa informacijskom sustavu OBV za treće strane definirana su *Pravilnikom o udaljenom pristupu informacijskom sustavu*.

Pri isteku ugovora trećoj strani potrebno je pravovremeno ukinuti sva prava pristupa informacijskom sustavu OBV. Organizacijska jedinica odgovorna za sklapanje ugovornog odnosa dužna je uputiti Odjelu za informatiku zahtjev za ukidanjem prava pristupa informacijskom sustavu.

Za ugovorne odnose vezane uz pružanje specifičnih usluga sa značajnijim utjecajem na poslovanje i sigurnost informacijskog sustava OBV, OBV trećoj strani može sugerirati ili inzistirati na certifikaciji predmetnih usluga prema ISO/IEC 9001 i/ili ISO/IEC 27001 normama.

4. Procjena rizika eksternalizacije

OBV će periodično, minimalno svake dvije godine, provjeravati temeljne podatke, rad i osposobljenost ključnih vanjskih partnera (trećih strana) kako bi se smanjili rizici od mogućih prekida poslovanja trećih strana koji bi utjecali na rad informacijskog sustava OBV-a. Ova provjera proširuje postojeću procjenu rizika koja se radi sukladno Metodologiji upravljanja rizicima informacijskog sustava.

Popis ključnih trećih strana se radi na temelju klasifikacije aspekata informacijske imovine u registru informacijske imovine u alatu AlterRisk odnosno za materijalno značajne eksternalizacije o čemu odlučuje Odbor ISMS.

Treće strane će se procjenjivati temeljem upitnika procjene rizika eksternalizacije. Vrednovanjem odgovora iz upitnika, dobije se procjena rizika rada s trećom stranom sa stanovišta informacijske sigurnosti.

Sukladno Metodologiji upravljanja rizicima informacijskog sustava, niski rizici se mogu odmah prihvatiti dok je za ostale rizike potrebno odrediti mjere za smanjenje rizika. Preostali visoki rizici moraju biti odobreni od strane Odbora ISMS i direktora OBV.

5. Uloge i odgovornosti

U svim slučajevima u kojem informacijski sustav OBV-a koristi ili istom ima pristup vanjski partner i njegovi zaposlenici, OBV je obvezna pribaviti izjavu vanjskog partnera prema obrascu izjave koji se nalazi u prilogu *Pravilnika o primjerenom korištenju informacijskog sustava* i čini njegov sastavni dio (Prilog 2), potpisanu od strane osoba ovlaštenih za zastupanje vanjskog partnera.

Potpisanu izjavu vanjskog partnera OBV će smatrati primjerenim dokazom da su vanjski partner i svi njegovi zaposlenici koji koriste ili imaju pristup informacijskom sustavu OBV-a upoznati s ovim Pravilnikom i njegovim odredbama.

Odgovorne osobe organizacijske jedinice OBV u čijoj je nadležnosti poslovni odnos između OBV i vanjskog partnera, ovlaštene od strane nadležnog rukovoditelja, dužne su

- upoznati vanjskog partnera i zaposlenike vanjskog partnera koji pristupaju ili koriste informacijski sustav OBV unutar poslovnih prostorija OBV i s drugim aktima OBV koji se odnose na korištenje i zaštitu informacijskog sustava OBV, sukladno opsegu posla kojeg te osobe obavljaju na informacijskom sustavu.
- vršiti nadzor parametara ugovora te mjerenje razine pružene usluge u skladu s odredbama ugovora,
- inicirati ukidanje ovlasti pristupa informacijskom sustavu nakon isteka ugovorne obveze,
- definirati pravila sigurne komunikacije i razmjene informacija.
- izvršiti provjeru ugovora te njihovu pravnu valjanost i usklađenost s internim aktima OBV-a.

Voditelj sigurnosti informacijskog sustava (VSIS) dužan je korisnike informacijskog sustava periodički educirati i osvješćivati o aktualnim sigurnosnim prijetnjama i primjerenom korištenju informacijskog sustava OBV-a u skladu s odredbama *Pravilnika o primjerenom korištenju informacijskog sustava*.

Voditelj sigurnosti informacijskog sustava (VSIS) provodi periodične procjene rizika eksternalizacije trećih strana, uz pomoć rukovoditelja organizacijskih jedinica u čijoj je nadležnosti poslovni odnos između OBV-a i vanjskog partnera/treće strane.

Odjel za informatiku dužan je osigurati tehničke preduvjete koji će korisnicima omogućiti primjereno korištenje informacijskog sustava u skladu s odredbama ovog Pravilnika.

6. Nepridržavanje

Svako nepridržavanje ovog pravilnika i ostalih sigurnosnih politika, zakona, općih akata i drugih dokumenata u OBV može biti sankcionirano sukladno zakonskim propisima i internim aktima OBV-a.

7. Završne i prijelazne odredbe

Pravilnik stupa na snagu i primjenjuje se danom njegovog donošenja.

KLASA: 011-02/23-01/9

URBROJ: 2186-192-30-23-1

U Varaždinu, 28.03.2023.

RAVNATELJ

Dr. sc. Damir Poljak, mag.soc.geront.