Pravilnik o primjerenom korištenju informacijskog sustava

SADRŽAJ

POPIS PRILOGA	
Prilog 1	IZJAVA o upoznavanju s odredbama Pravilnika o primjerenom korištenju informacijskog sustava OBV
Prilog 2	IZJAVA o preuzimanju obveza iz Pravilnika o primjerenom korištenju informacijskog sustava OBV-a
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 korištenju prijenosnih računala i mobilnih uređaja
3	

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	Svim radnicima – Intranet portal	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

Ovaj Pravilnik uspostavlja standarde primjerenog korištenja informacijskog sustava OBV, te mu je cilj podizanje razine svijesti o sigurnosti unutar uspostavljene poslovne kulture povjerenja i integriteta.

Svi Korisnici informacijskog sustava dužni su djelotvorno, učinkovito, etično i na zakonski primjeren način koristiti sve dijelove informacijskog sustava.

Odgovornost je svakog Korisnika poznavati ove odredbe i u potpunosti ih se pridržavati.

Izuzeća od ograničenja se odnose na Korisnike koji djeluju prema dodijeljenim odgovornostima (npr. administratori sustava).

Ovaj Pravilnik se odnosi na sve korisnike i na svu opremu u vlasništvu ili najmu OBV.

2. Korištenje i vlasništvo

(1) Informacije koje se kreiraju, obrađuju ili prenose unutar informacijskog sustava OBV-a, smatraju se vlasništvom OBV-a.
(2) Informacije osobnog karaktera koje Korisnici kreiraju, pohranjuju ili šalju korištenjem pojedinih dijelova informacijskog sustava OBV-a, ne smatraju se privatnim vlasništvom Korisnika. Korisnici se odriču prava privatnosti nad takvim podacima.
(3) Korisnici su odgovorni primjenjivati razumno odlučivanje dok koriste informacijski sustav OBV-a u osobne svrhe.
(4) Ovlašteni zaposlenici OBV-a smiju nadzirati korištenje informacijskog sustava. Cilj ovakvog nadzora je osigurati povjerljivost, integritet i raspoloživost informacija i informacijskog sustava OBV-a kako bi se poslovne aktivnosti odvijale dosljedno i neprekinuto.
(5) Korisnici prihvaćaju mogućnost nadzora nad korištenjem pojedinih dijelova informacijskog sustava i bilježenja aktivnosti na sustavima i aktivnosti korisnika. Taj nadzor može biti nad internetskim adresama koje korisnici posjećuju, pregled materijala koji se preuzima s Interneta te nadzor nad servisom elektroničke pošte.

3. Prava pristupa

(1) Prava pristupa informacijskom sustavu OBV-a smiju se koristiti samo za definiranu namjenu.

(2) Nedopušteno korištenje prava pristupa povreda je radne obveze i može imati elemente za disciplinsku i pravnu odgovornost.

(3) Korisnik mora svoja prava pristupa informacijskom sustavu koristiti isključivo kroz vlastiti rad i ne smije nikome drugome omogućiti njihovo korištenje.

(4) Korisnik ne smije pokušati pristupiti dijelovima informacijskog sustava za koje nema odobrena prava pristupa ili eksplicitnu suglasnost odgovorne osobe za svaki pojedini dio.

(5) Korisnik je odgovoran za vjerodostojnost svih akcija koje su provedene pod njegovim korisničkim pravima.

(6) Mogućnost korisnika da sadržaj za koji je odgovorna druga osoba čita, mijenja ili kopira ne podrazumijeva i dopuštenje za takvu akciju.

(7) Ako Korisnik uoči mogućnost pristupa resursima koji nisu u okviru njegove poslovne funkcije dužan je obavijestiti nadređenu osobu ili Odjel za informatiku.

(8) Korisniku je zabranjeno pristupati bilo kojem dijelu informacijskog sustava koristeći korisnička prava i lozinke drugog korisnika.

4. Korisničko ime i lozinka

(1) Korisnici su odgovorni:

- za sve aktivnosti koje se izvrše korištenjem njihovog korisničkog računa,
- za zaštitu svih informacija korištenih ili spremljenih putem vlastitih korisničkih prava,
- za čuvanje korisničkih imena te izbor i čuvanje lozinki za pristup informacijskom sustavu.

(2) Korisnik ne smije:

- odavati lozinke drugim korisnicima, čak ni administratorima sustava,
- otkriti drugim osobama drugačije oblike pristupa na sustav,
- držati lozinke u pisanom obliku na vidljivom ili lako dostupnom mjestu,
- lozinke držati pohranjene u memoriji računala niti ih slati elektroničkom poštom,
- uključivati lozinku u bilo koju automatsku proceduru ili makro sekvencu.

(3) U slučaju sumnje na ugrožavanje lozinke, korisnik je dužan o tome obavijestiti Odjel za informatiku ili Voditelja sigurnosti informacijskog sustava (VSIS).

(4) Korisnik je dužan poštovati sljedeća pravila za odabir lozinke:

- Lozinke moraju biti kombinacija slova i brojki,
- Lozinke moraju sadržavati najmanje 10 znakova,
- Lozinke treba mijenjati najmanje svakih 180 dana ili kraće ako je tako propisano za pojedini sustav,
- Promijenjena lozinka ne smije biti ista kao jedna od prethodne 3 lozinke,
- Inicijalna lozinka za pristup nekom sustavu mora se promijeniti prilikom prve prijave na sustav.

(5) Korisnika se potiče da se pridržava nekih smjernica za odabir lozinke kako bi se smanjio rizik od ugrožavanja sigurnosti lozinke, tako da lozinka ne bi trebala:

- sadržavati dva ili više identičnih znakova u nizu,
- biti riječ iz rječnika bilo kojeg jezika,
- sadržavati osobne podatke (ime, prezime, datum rođenja, OIB i slično),
- sadržavati očite sekvence tipki s tipkovnice,
- biti identična onima koje se koriste u privatne svrhe (npr. pristup privatnom e-mailu i slično).

(6) Ako korisnik zaboravi lozinku ili smatra da je ugrožena tajnost postojeće lozinke, administrator sustava će mu omogućiti da unese novu.

5. Korištenje informacijskog sustava

(1) Korisnicima nije dopušteno:

- instalirati programske pakete na osobna računala bez odobrenja i podrške Odjela za informatiku,
- mijenjati postavke programa instaliranih na osobnim računalima kojima je svrha zaštita informacijskog sustava (npr. antivirusni programi, osobni vatrozidi i slično),
- pokušavati zaobilaziti ili izbjegavati redovite mjere sigurnosti na bilo koji način,
- svjesno provoditi akcije koje nepotrebno zauzimaju resurse sustava ili uzrokuju slabe performanse rada sustava (npr. na slanje masovnih ili lančanih poruka elektroničke pošte, kompjuterske igre, ispis nepotrebnih kopija dokumenata ili iskorištavanja mrežnih resursa na bilo koji drugi način),
- pokretati programe za nadzor i analizu mrežnog prometa, provjeru ranjivosti, napade na lozinke ili bilo koje druge alate kojima mogu doći u neovlašten posjed informacija,
- kopirati konfiguracijske datoteke sustava,
- takve datoteke neovlašteno koristiti za namjenu koja je različita od osnovne namjene,
- takve datoteke neovlašteno davati na uvid drugim osobama.

(2) Korisnici su dužni poslovne podatke kreirane ili obrađene osobnim računalima, a koji su značajni za poslovanje OBV-a, pohranjivati na mrežnim poslužiteljima prema uputama Odjela za informatiku i/ili VSIS-a.

(3) Svi mediji za pohranu podataka preuzeti iz vanjskog okruženja kao i datoteke preuzete s Interneta ili drugih računala koja ne pripadaju OBV-u, moraju biti provjereni kako bi se eliminirali računalni virusi ili drugi potencijalno zlonamjerni softver. Ove odredbe vrijede i za datoteke koje se prenose s kućnih računala u vlasništvu korisnika.

(4) Korisnici su dužni pridržavati se uputa o zaštiti od računalnih virusa te spriječiti bilo kakvu aktivnost koja uvećava rizike unošenja računalnih virusa i drugog zlonamjernog koda.

6. Korištenje Interneta

(1) Internet se smatra značajnim poslovnim resursom te se smije koristiti isključivo u poslovne i edukacijske svrhe povezane uz poslovnu funkciju korisnika.

(2) Sve informacije koje korisnici preuzimaju s Interneta, a služe u poslovne svrhe, moraju biti iz vjerodostojnih izvora.

(3) Prava pristupa i korištenja Interneta Korisnicima se dodjeljuju na temelju pisanog zahtjeva njihovih nadređenih rukovoditelja i potvrđenog od strane rukovoditelja Odjela za informatiku.

(4) Korisnicima nije dopušteno koristiti Internet:

- radi pribavljanja financijske koristi u privatne namjene,

- kroz aktivnosti koje uzrokuju neprimjereno opterećenje računalnih resursa,
- za preuzimanje materijala neprihvatljivog sadržaja s vanjskih internetskih poslužitelja i pohranjivanje istih na računalima OBV-a.

(5) OBV ne preuzima odgovornost za materijal koji korisnici pregledavaju ili preuzimaju s Interneta, a koji bi mogao imati neprikladan ili uvredljiv sadržaj.

(6) OBV zadržava pravo onemogućavanja pristupa web sadržajima koji se smatraju neprimjerenima za poslovanje.

7. Korištenje elektroničke pošte

(1) Korisnici su dužni slati elektroničkom poštom ili drugim oblicima elektroničke komunikacije samo istinite i pouzdane informacije.

(2) Odredbe ovog članka se odnose na elektroničke poruke koje se šalju unutar mreže OBV-a i Internetom.

(3) Korisnici ne smiju:

- kreirati niti pohranjivati materijale čiji je sadržaj uznemiravajući, nepristojan, klevetnički, na bilo koji način neprihvatljiv ili zakonski nedopušten,
- sudjelovati u aktivnostima čija je namjera uznemiravati ili vrijeđati druge osobe, niti na bilo koji način širiti materijale s uvredljivim sadržajem,
- komunicirati s osobom koja u porukama koristi pseudonim ili zadržava anonimnost,
- otvarati/spremati sadržaj niti odgovarati pošiljatelju u slučaju primitka unaprijed nezatraženog komercijalnog e-maila (sa ili bez priloga) od nepoznatog izvora izvan OBV-a (spam).

(4) Korisnici su dužni:

- pružiti točne podatke o svom identitetu prilikom slanja poruka elektroničke pošte,
- poruke elektroničke pošte koje sadrže poslovne podatke relevantne za pojedine poslovne transakcije, za donošenje budućih poslovnih odluka ili korištene za donesene poslovne odluke, pohraniti sukladno uputama Odjela za informatiku.

(5) Bez prethodne suglasnosti izvornog pošiljatelja, nije dopušteno u vanjsko okruženje prosljeđivati poruke primljene u OBV-ov adresni prostor. Od ove odredbe može se odstupiti samo ako se nedvojbeno radi o javnim podacima.

(6) Elektronička se pošta može slati velikom broju osoba istovremeno korištenjem distribucijskih lista samo na temelju unaprijed planirane i odobrene aktivnosti. Ako se takve poruke šalju osobama izvan OBV-a, onda je potrebno prethodno dobiti njihovu suglasnost za takav postupak, a svaka poruka mora sadržavati uputu o odjavi s distribucijske liste.

(7) Korisnici se upozoravaju da nije uputno otvarati privitke elektroničkoj pošti osim kada postoji potvrda slanja od strane pošiljatelja i kada se automatskom provjerom utvrdi odsutnost virusa i drugog zlonamjernog softvera.

(8) Prilozi nepoznatih pošiljatelja su primarni izvori računalnih virusa i treba im pristupati s najvišom razinom opreza.

(9) Sve poruke elektroničke pošte koje izlaze izvan domene OBV-a, odnosno poslovnim partnerima, klijentima, trećim stranama itd., moraju sadržavati Izjavu o odricanju od odgovornosti:

Napomena: Ova poruka sadrži podatke povjerljive prirode, isključivo namijenjene osobama označenima kao primateljima te se pristup od strane bilo koje druge osobe smatra neovlaštenim. Ako niste označeni primatelj, svaka distribucija, kopiranje, umnožavanje ili otkrivanje sadržaja trećim osobama je strogo zabranjeno i smatra se protuzakonitim. Ako ste dobili ovu poruku, a niste označeni primatelj, molimo Vas da sto prije obavijestite pošiljatelja poruke i uništite sve postojeće kopije. Ova napomena također potvrđuje da je ova elektronička poruka testirana na postojanje računalnih virusa.

Disclaimer: The information in this email is confidential and it is intended solely for the addressee. Access to this email by anyone else is unauthorized. If you are not the intended recipient, any distribution, copying, duplication or disclosure is prohibited and may be unlawful. If you have received this email in error, please notify the sender immediately and destroy it, and all copies of it. This footnote also confirms that this email message has been swept for the presence of computer viruses.

8. Održavanje čistog stola i praznog zaslona

(1) Svi korisnici informatičkih servisa u OBV-u i svi zaposlenici u opsegu sustava upravljanja informacijskom sigurnošću u OBV-u moraju usvojiti

a) politiku čistog stola za papirnatu dokumentaciju (pravilnici, upute, interni dopisi, ugovori i slično) i uklonjive medije (CD, DVD, vanjski disk, USB stick i slično) klasificirane prema Pravilniku o klasifikaciji podataka, i

b) politiku praznog zaslona za opremu za obradu informacija (računala, tableti, mobiteli i dr.).

(2) Svi korisnici informatičkih servisa u OBV-u moraju osigurati da su zasloni računala zaštićeni zaporkom prilikom napuštanja radne okoline ili privremenog ostavljanja računala bez nadzora. Zasloni računala se automatski zaključavaju nakon maksimalno 20 minuta bez aktivnosti korisnika na računalu.

(3) Svi korisnici informatičkih servisa u OBV-u su nakon završetka rada dužni zatvoriti sve aktivne veze, osim u slučajevima kad se one mogu zaštititi odgovarajućim mehanizmom za blokiranje, te izvršiti odjavu s glavnih računala, poslužitelja i uredskih računala tako da nastavak rada bude moguć samo uz novu prijavu korisnika.

(4) Svi radnici u opsegu sustava upravljanja informacijskom sigurnošću u OBV-u dužni su osigurati sljedeće:

a) da su njihove radne površine (uredi, stolovi, otvorene površine namještaja) čiste nakon što napuste svoje radno mjesto ili ga privremeno ostave bez nadzora,

b) da su papir ili računalni mediji koji sadrže osjetljive informacije spremljeni na siguran način tako da im je onemogućen neovlašten pristup (npr. u ormariće pod ključem),

c) da su sa pisača odmah nakon ispisa uklonjeni dokumenti koji sadrže osjetljive informacije,

d) da prilikom slanja ili primanja faks poruka sa osjetljivim informacijama transfer drže pod nadzorom (npr. na način da odašiljanje ili primanje poruke pričekaju pokraj faks uređaja, kao i potvrdu o slanju i potvrdu primitka s druge strane),

e) da fotokopirne uređaje i ostale tehnologije reprodukcije (npr. skeneri, digitalne kamere) koriste samo uz odobrenje vlasnika osjetljivih informacija koje namjeravaju reproducirati,

f) da na svako kršenje odredbi ove politike upozore svoje kolege i suradnike.

9. Sigurnosni incidenti

(1) Korisnici su dužni sukladno u najkraćem mogućem roku izvijestiti o:

- svakom događaju koji ukazuje na povredu mjera sigurnosti,
- svakom događaju koji ukazuje na pojavu sigurnosnih incidenata,
- svakom primijećenom nedostatku u sustavu sigurnosti informacijskog sustava OBV-a.

(2) Odgovorne osobe se moraju izvijestiti na način koji je definiran u procedurama i pravilnicima. Događaji koji se mogu okarakterizirati kao povreda povjerljivosti podataka moraju se prijaviti nadređenoj osobi.

(3) U slučaju da korisnici iz vanjskih izvora prime obavijest o pojavi virusa ili neke druge sigurnosne prijetnje, takvu su obavijest dužni proslijediti isključivo odgovornom zaposleniku Odjela za informatiku i/ili VSIS-u.

(4) Nije dopušteno takve obavijesti proslijediti drugim korisnicima u obliku masovne ili lančane elektroničke pošte.

(5) Korisnicima nije dopušteno javno objavljivati podatke o pojavi sigurnosnih incidenata, o problemima ili ranjivostima sustava i računalne mreže OBV-a, osim ako takav postupak ne odobri Uprava OBV-a.

10.Edukacija i podizanje svijesti o informacijskoj sigurnosti

10.1. Podizanje svijesti o informacijskoj sigurnosti

(1) Cilj podizanja svijesti o informacijskoj sigurnosti je omogućiti fizičkim osobama koje pristupaju informacijskoj imovini u opsegu sustava upravljanja informacijskom sigurnošću u OBV-u da prepoznaju potencijalne sigurnosne probleme, događaje i incidente i reagiraju u skladu s potrebama njihove poslovne funkcije.

(2) U tu svrhu OBV mora imati razvijen program podizanja svijesti o informacijskoj sigurnosti.

(3) Program podizanja svijesti o informacijskoj sigurnosti mora biti jasno definiran, zadovoljavati poslovne i sigurnosne zahtjeve te biti održavan i prilagođavan rezultatima procjene rizika i promjenama u okruženju rizika informacijske sigurnosti u opsegu sustava upravljanja informacijskom sigurnošću u OBV-u.

(4) Program podizanja svijesti o informacijskoj sigurnosti u OBV-u mora osim djelatnika na primjeren način obuhvatiti i sve fizičke osobe koje pristupaju informacijskoj imovini i prostorima u kojima se nalazi informacijska imovina u opsegu sustava upravljanja informacijskom sigurnošću u OBV-u (vanjski konzultanti, ugovorni suradnici, servisno osoblje i sl.).

(5) Kod angažiranja treće strane obvezno je obuhvatiti i postupke osiguranja svijesti zaposlenika treće strane o njihovim odgovornostima vezanima uz informacijsku sigurnost.

10.2. Edukacija o informacijskoj sigurnosti

(1) Edukacija o informacijskoj sigurnosti mora biti usmjerena ka postizanju optimalne razine svijesti i razumijevanja obveza u području informacijske sigurnosti kod zaposlenika OBV-a u odnosu na funkcije i odgovornosti koje taj zaposlenik ima unutar organizacije.

(2) Svi zaposlenici koji pristupaju informacijskoj imovini u opsegu sustava upravljanja informacijskom sigurnošću u OBV-u moraju biti obuhvaćeni planom edukacije u području informacijske sigurnosti.

(3) Edukacija za pojedine zaposlenike definirana planom edukacije mora odgovarati zahtjevima poslovne funkcije koju zaposlenik obavlja, njegovim sigurnosnim odgovornostima i vještinama.

(4) Za svakog novog zaposlenika mora se obaviti inicijalna edukacija prije dobivanja ovlasti za pristup informacijskoj imovini. Ova inicijalna edukacija mora sadržavati sigurnosne zahtjeve, zakonske obveze, obuku o ispravnoj uporabi informacijske imovine, informacije o disciplinskom procesu, te upoznavanje s politikama i pravilnicima informacijske sigurnosti u OBV-u.

(5) Ova inicijalna edukacija se na odgovarajući način primjenjuje i za zaposlenike kojima su promijenjene ovlasti za pristup informacijskoj imovini.

(6) Osoblje koje koristi mobilna računala mora biti dodatno educirano radi podizanja svijesti o posebnim rizicima pri ovakvom načinu rada.

11.Korištenje mobilnih uređaja

11.1. Uvod

OBV omogućuje svojim zaposlenicima korištenje prijenosnih uređaja kao što su mobiteli, pametni telefoni, dlanovnici (PDA), i slični mobilni uređaji za pristup internim resursima OBV-a, sinkronizaciju podataka i spajanje na Internet.

Kako su navedeni uređaji mali i prenosivi te obzirom da imaju veliki kapacitet za čuvanje podataka, rizik gubitka uređaja je velik, kao i mogući gubitak osjetljivih dokumenata.

U nastavku teksta definiraju se prava i obaveze korisnika kako bi se na adekvatan način zaštitili mobilni uređaj i njihov sadržaj.

11.2. Podaci na mobilnim uređajima

(1) Nije dozvoljeno posuđivanje mobilnog uređaja drugim zaposlenicima, osobama izvan OBV-a niti članovima obitelji.

(2) Ako se mobilni uređaji koriste za spremanje i sinkronizaciju podatka, potrebno je primijeniti sljedeće metode zaštite u ovisnosti u klasifikacijskoj razini informacija koji se nalaze na mobilnom uređaju prema Zakonu o tajnosti podataka:

- **Neklasificirano** i **Interno** – podatke na mobilnom uređaju je potrebno zaštititi korištenjem enkripcije ili lozinke (PIN-a).
- **Osjetljivo** - podatke na mobilnom uređaju je potrebno zaštititi korištenjem enkripcije i lozinke (PIN-a).

(3) Na mobilne uređaje ne smije se instalirati nelicencirani niti zlođudni softver.

(4) Na svim uređajima koji to podržavaju, mora biti instalirani antivirusni softver, koji treba biti održavan ažurnim prema naputcima proizvođača softvera.

(5) Potrebno je koristiti lozinku ili PIN prilikom uključenja uređaja ako to mobilni uređaj podržava.

11.3. Fizička sigurnost

(1) Mobilni uređaji ne smiju se ostavljati na vidljivom mjestu u vozilu dok je korisnik odsutan.

(2) Mobilni uređaje ne smiju se ostavljati u vozilu preko noći.

(3) Ako se korisnik nalazi na javnom mjestu ili sastanku, mobilni uređaj mora se koristiti na odgovarajući način pazeći na privatnost i fizičku zaštitu uređaja.

(4) Prilikom putovanja mobilni uređaji moraju se nositi u ručnoj prtljazi osim u slučajevima kada prijevoznik propisuje drugačije.

12.Nepridržavanje

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

13.Završne i prijelazne odredbe

Pravilnik stupa na snagu i primjenjuje se danom njegovog donošenja.

Prilog 1

IZJAVA
o upoznavanju s odredbama
Pravilnika o primjerenom korištenju informacijskog sustava
Opće bolnice Varaždin (OBV)

Ovom Izjavom _____, _____
(ime i prezime) (matični broj zaposlenika)

(u daljnjem tekstu: Korisnik informacijskog sustava OBV)

potvrđuje da je upoznat s odredbama Pravilnika o primjerenom korištenju informacijskog sustava OBV.

Korisnik informacijskog sustava OBV je svjestan da u slučaju postupanja protivno odredbama Pravilnika podliježe odgovornosti sukladno internim aktima OBV.

Ova Izjava je sačinjena u dva (2) primjerka od kojih jedan (1) primjerak zadržava OBV, a jedan (1) korisnik informacijskog sustava OBV. Primjerak za OBV se pohranjuje u dosjeu zaposlenika.

U _____, _____ godine
(domicilno mjesto OJ OBV) (datum)

_____
(potpis)

Prilog 2

IZJAVA

o preuzimanju obveza iz Pravilnika o primjerenom korištenju informacijskog sustava Opće bolnice Varaždin (OBV-a)

Ovom Izjavom društvo _____
(naziv društva)

Iz _____, _____, _____,
(sjedište društva) (OIB) (MBS)

zastupano po ovlaštenoj osobi _____, _____,
(funkcija) (ime i prezime)

_____, _____,
(prebivalište) (OIB)

(u daljnjem tekstu: Društvo Korisnik informacijskog sustava OBV)

potvrđuje

da je upoznat s Pravilnikom o primjerenom korištenju informacijskog sustava OBV, (u daljnjem tekstu: Pravilnik), da je razumio njegove odredbe te da u potpunosti prihvaća obveze koje proizlaze iz istog, za vrijeme trajanja Ugovora/Narudžbenice _____ od _____ dana _____godine (dalje: Ugovor) između OBV i društva Korisnika.

Društvo Korisnik informacijskog sustava prilikom potpisivanja ove Izjave obvezuje se OBV-u dostaviti popis svojih zaposlenika koji će obavljati poslove iz Ugovora vezane uz korištenje informacijskog sustava OBV-a.

Društvo Korisnik informacijskog sustava potpisom ove Izjave potvrđuje da su svi njegovi zaposlenici koji će obavljati poslove iz Ugovora vezane uz korištenje informacijskog sustava OBV-a upoznati s Pravilnikom i obvezani na pridržavanja Pravilnika za cijelo vrijeme važenja Ugovora.

U slučaju promjene zaposlenika koji će obavljati poslove iz Ugovora vezane uz korištenje informacijskog sustava OBV-a, Društvo Korisnik informacijskog sustava OBV-a se obvezuje dostaviti OBV-u novi popis svojih zaposlenika koji će obavljati te poslove, i to prije nego što ti zaposlenici započnu s obavljanjem navedenih poslova.

Ova Izjava je sačinjena u dva (2) primjerka od kojih jedan (1) primjerak zadržava OBV, a jedan (1) primjerak zadržava Društvo Korisnik informacijskog sustava OBV-a.

Primjerak za OBV se pohranjuje kod Odgovorne osobe ovlaštene od nadležnog rukovoditelja organizacijske jedinice OBV-a za čije potrebe je zaključen Ugovor s Društvom Korisnikom informacijskog sustava kao vanjskim partnerom.

KLASA: 011-02/23-01/16

URBROJ: 2186-192-30-23-1

U Varaždinu, 28.03.2023.

RAVNATELJ

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