Politika sigurnosti informacijskog sustava

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 na Intranet portalu na način da se nalaze u istoj radnoj mapi gdje i ovaj priručnik.

VEZANI DOKUMENTI	
1	Pravilnik o primjerenom korištenju informacijskog sustava
2	Pravilnik o upravljanju uslugama trećih strana
3	Pravilnik o korištenju prijenosnih računala i mobilnih uređaja
4	Pravilnik o upravljanju informacijskom imovinom
5	Pravilnik o upravljanju mrežnom infrastrukturom
6	Pravilnik o udaljenom pristupu informacijskom sustavu
7	Pravilnik sigurnosne pohrane i arhiviranja
8	Pravilnik o upravljanju sigurnosnim zakrpama
9	Pravilnik o zaštiti od malicioznog koda
10	Politika kontinuiteta poslovanja
11	Pravilnik za upravljanje promjenama na informacijskom sustavu
12	Pravilnik o internom auditu informacijskog sustava
13	Metodologija upravljanja rizicima informacijske sigurnosti
14	Procedura upravljanja incidentima informacijske sigurnosti
15	Procedura upravljanja sigurnosnim zapisima
16	Procedura instalacije softvera
17	Procedura upravljanja pravima pristupa

18	Pravilnik o upravljanju kriptografskim kontrolama
19	Pravilnik o provjeri ranjivosti mrežnih resursa IS
20	Security awareness program
21	Pravilnik o klasifikaciji podataka
22	Zakon o tajnosti podataka
23	Zakon o informacijskoj sigurnosti
24	Uredba o mjerama informacijske sigurnosti
25	Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga
26	Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga
27	Pravilnik o standardima sigurnosne provjere (UVNS)
28	Pravilnik o standardima fizičke sigurnosti (UVNS)
29	Pravilnik o standardima sigurnosti podataka (UVNS)
30	Pravilnik o standardima organizacije i upravljanja područjem sigurnosti informacijskih sustava
31	Pravilnik o standardima sigurnosti poslovne suradnje (UVNS)
32	Zakon o provedbi opće uredbe o zaštiti podataka (GDPR)
33	Pravilnik o standardima sigurnosti neklasificiranih informacijskih sustava
34	

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

Ovom politikom uređuje se organizacija informacijske sigurnosti odnosno sustava upravljanja informacijskom sigurnošću (dalje u tekstu: ISMS) Opće bolnice Varaždin (dalje u tekstu: OBV ili Bolnica) te odgovornosti radnika vezano uz informacijsku sigurnost u skladu s primjenjivim standardima i zakonodavnim okvirom.

Provođenja odredbi ove Politike uređuje se posebnim provedbenim aktima (pravilnici i procedure).

2. Opseg

Ova politika i provedbeni akti primjenjuju se na sve informacijske sustave i procese unutar Opće bolnice Varaždin.

3. Definicije

Pregled pojmova i njihovo značenje:

Analiza rizika (*engl. risk analysis*) - postupak identificiranja prijetnji i ranjivosti te određivanja njihovog utjecaja i vjerojatnosti ostvarivanja.

Analiza utjecaja na poslovanje - proces analize poslovnih procesa i financijskih i operativnih posljedica koji bi na njih mogli imati poremećaji ili zastoji poslovanja.

Ciljano vrijeme oporavka (RTO - Recovery Time Objective) - maksimalno dozvoljeno vrijeme oporavka u kom je potrebno osposobiti minimalni skup funkcionalnosti procesa i informatičkih servisa.

Cjelovitost (cjelokupnost, integritet, engl. integrity) - svojstvo očuvanja točnosti i kompletnosti informacije.

Dokument – informacije na pratećem mediju (a medij može biti: papir, magnetski, elektronski ili optički kompjuterski disk, fotografski ili master uzorak ili njihova kombinacija). Kao primjer dokumenata možemo navesti: zakon, propis, norma, projekt, elaborat, nacrt, izvještaj, postupak, uputa, obrazac, zapis....

Dokumentacija - set dokumenata koje povezuje zajednički subjekt (subjekt može biti predmet ili projekt, organizacijska jedinica, poslovni proces). Primjeri dokumentacije su: dokumentacija projekta izgradnje novog objekta, dokumentacija koja opisuje informacijski sustav, dokumentacija poslovnog procesa nabave pojedine robe ili usluge i slično.

Glavni popis dokumenata - lista u kojoj su popisane zadnje važeće revizije dokumenata. Za popis ISMS dokumenata se koristi lista dokumenata na portalu OBV.

Identifikacijska oznaka - brojčana oznaka dokumenta po kojoj se dokumenti mogu jednoznačno razlikovati među sobom. Oznake se primjenjuju putem intranet portala za informacijsku sigurnost.

Imovina (engl. asset) - svaka dodirljiva ili nedodirljiva stvar (informacija) koja ima neku vrijednost za organizaciju. Sa stanovišta sustava za upravljanje informacijskom sigurnošću, posebno je zanimljiva informacijska imovina.

Incident - nepogoda i izvanredan neželjeni poslovni događaj.

Informacijska imovina - informacije, podaci, kao i sva materijalna i nematerijalna sredstva koja služe za prikupljanje, obradu, spremanje ili distribuciju informacija značajnih u poslovnom procesu (npr. ljudski resursi, baze podataka, programski moduli, dokumentacija, ugovori, informatička oprema, dijelovi infrastrukture, pomoćne usluge i slično).

Informacijska sigurnost (engl. information security) - očuvanje povjerljivosti, cjelovitosti i raspoloživosti informacijske imovine; može uključiti i svojstva poput autentičnosti, uračunljivosti, ne-poricanja i pouzdanosti.

Informacijski sustav - Skup poslovnih procesa obuhvaćenih primjenom informacijske tehnologije sa ciljem prikupljanja, prijenosa, obrade, primjene i arhiviranja svih informacija bitnih za poslovanje tvrtke.

Integritet - Osobina očuvanja autentičnosti i cjelovitosti imovine (engl. integrity).

IT servis - Usluga podrške poslovnog procesa ili njegovog dijela podržana primjenom informatičke tehnologije.

Kontrola (engl. control) - svaka administrativna, upravljačka, tehnička ili zakonska metoda koja se koristi u svrhu umanjenja rizika. Uključuje politike, pravilnike, procedure, računalne programe, razne tehnologije i organizacijsku strukturu.

Korisnici – radnici tvrtke te druge fizičke i pravne osobe koje koriste i/ili čiji poslovni procesi ovise o informacijskim sustavima tvrtke.

Korisnik dokumenta - osoba na koju je dokument naslovljen ili odgovoran za primjenu dokumenta.

Kriza - kritičan događaj (obilne snježne padavine, poplave, požari, potresi, štrajkovi i masovni nemiri, teroristički napad, itd..), koji može dramatično utjecati na normalno funkcioniranje tvrtke.

Maksimalna tolerancija gubitka podataka (RPO – Recovery Point Objective) – ciljana frekvencija izrade pričuvne pohrane podataka.

Neusklađenost/Nesukladnost - svako odstupanje od sigurnosnih propisa ili narušavanje bilo kojeg od sigurnosnih zahtjeva za bilo koji dio informacijskog sustava.

Obrazac - koristi se kontinuirano u poslovanju, ponavlja se njegov standardni oblik, ali su podaci u njemu svaki put drugačiji, ne smatra se dokumentom u užem smislu.

Objektivni dokaz (objektivna evidencija) - kvalitativna ili kvantitativna informacija, zapis ili izjava o činjenici, u svezi sigurnosti informacijskog sustava i pridržavanju propisanih pravila vezano uz sigurnost informacijskih sustava. Objektivni dokaz je temeljen na promatranju, mjerenju ili testiranju i može biti verificiran.

Odbor za ISMS (dalje u tekstu: Odbor) - krovno tijelo za upravljanje informacijskom sigurnošću koje na temelju preporuka Voditelja sigurnosti informacijskog sustava (VSIS) i unutarnjeg revizora informacijskog sustava donosi strateške odluke o informacijskoj sigurnosti i planira sredstva pomoću kojih se provode odluke i implementiraju sigurnosne mjere.

Oporavak operacije - sposobnost organizacije da odgovori na štetne događaje prema Planu za upravljanje kontinuitetom poslovanja i nastavi s redovitim poslovanjem u predviđenom vremenskom roku.

Planiranje kontinuiteta poslovanja - proces razvoja i dokumentiranje pravila i procedura koje omogućuju organizaciji da reagira na nepredviđene događaje i u predviđenom i prihvatljivom vremenu nastavi poslovanje.

Postupak (engl. procedure) - specificiran način izvršenja aktivnosti.

Povjerljivost – osobina da informacija nije učinjena dostupnom ili otkrivena neovlaštenim osobama, entitetima ili procesima (engl. confidentiality).

Preostali rizik (engl. residual risk) - rizik koji je preostao nakon primjene odluka za tretiranje rizika.

Prihvaćanje rizika (engl. risk acceptance) - je jedna od mogućnosti tretiranja rizika i predstavlja odluku za prihvaćanja mogućih negativnih posljedica koje proizlaze iz navedenog rizika.

Prijetnja (engl. threat) - potencijalno ostvariv neželjen i/ili štetan događaj. Kombinacija rizika, ishoda tog rizika i mogućnosti da se štetni događaja dogodi.

Proces (engl. process) - skup aktivnosti koje su međusobno povezane ili su u međudjelovanju, koji pretvara ulazne veličine u izlazne.

Procjena rizika – postupak u kojem se procjenjuje i rangira izloženost informacijske imovine riziku korištenjem odabrane metodologije.

Ranjivost (engl. vulnerability) - je slabost u informacijskom sustavu ili dijelu informacijske imovine koju bi mogla iskoristiti neka prijetnja.

Raspoloživost – osobina dostupnosti i upotrebljivosti imovine na zahtjev ovlaštenog subjekta (engl. availability).

Rizik - sprega vjerojatnosti neželjenog događaja i njegovih posljedica.

Sigurnosna mjera - sredstvo upravljanja rizikom, uključujući pravilnike, procedure, smjernice, praksu ili organizacijske strukture, koje mogu biti administrativne, tehničke, upravne ili zakonodavne naravi.

Skrbnik za IT servis – osoba odgovorna za ispravno operativno izvođenje IT servisa. Vodi brigu o računalnom sustavu i mreži, sistemskom softveru i sistemskim podacima, aplikativnom softveru i podacima, o primljenim ulaznim i o izlaznim podacima koje proizvodi informacijski sustav, o dokumentaciji IT servisa, prijenosnim medijima i drugim resursima informacijskog sustava koji omogućuju njegov ispravan rad.

Sustav upravljanja informacijskom sigurnošću (ISMS) - Sustav upravljanja unutar organizacije, temeljen na upravljanju poslovnim rizicima, sa zadaćom skrbljenja o uspostavi, implementaciji, redovnom upravljanju, nadzoru, pregledavanju, održavanju i poboljšavanju informacijske sigurnosti unutar te organizacije.

Tretiranje rizika (engl. risk treatment) - postupak odabira načina nošenja sa prepoznatim rizikom. Postoje četiri osnovne metode nošenja sa prepoznatim rizikom: prihvaćanje, izbjegavanje, prebacivanje i smanjenje.

Unutarnji revizor informacijskog sustava – osoba ili osobe odgovorne za redovito provođenje unutarnje revizije ISMS-a sukladno zahtjevima Sustava upravljanja informacijskom sigurnošću.

Upravljanje kontinuitetom poslovanja – holistički proces koji identificira potencijalne prijetnje i utjecaje koje te prijetnje mogu imati na odvijanje poslovnih procesa tvrtke, te uspostava okvira za upravljanje u slučaju nepredviđenih neželjenih događaja, pružajući efikasne odgovore kako bi se zaštitili interesi tvrtke.

Upravljanje rizikom (engl. risk management) - proces koji uključuje sve aktivnosti koje tvrtka koristi u svrhu upravljanja i kontrole rizika (procjenu rizika, tretiranje rizika i komunikacija).

Vlasnik informacijske imovine (engl. owner) - osoba ili organizacijska jedinica kojem je povjerena formalna odgovornost za brigu o informacijskoj imovini. Ovaj pojam ne podrazumijeva vlasništvo nad imovinom u pravnom smislu.

Vlasnik poslovnog procesa – osoba odgovorna za upravljanje svojim poslovnim procesom.

Voditelj sigurnosti informacijskog sustava (VSIS) - osoba odgovorna za nadzor implementacije tehničkih sigurnosnih mjera na informatičkim sustavima koje koristi tvrtka, te redovito praćenje njihove efikasnosti.

Vrednovanje rizika (engl. risk evaluation) - postupak pridjeljivanja ocjene prepoznatom riziku u skladu s unaprijed određenim kriterijem.

Zapis – popunjeni obrazac, dokument koji navodi postignute rezultate ili daje dokaze o provedenim radnjama, dokument koji daje objektivnu evidenciju o kvaliteti proizvoda odnosno aktivnostima koje utječu na kvalitetu proizvoda.

Događaj informacijske sigurnosti (Information security event) – identificirana pojava u stanju sustavu, usluzi ili mreži koja upućuje na moguću povredu politika informacijske sigurnosti, propust kontrola ili nepoznata situacija koja može biti relevantna za informacijsku sigurnost.

Incident informacijske sigurnosti (Information security incident) – jedan ili niz neželjenih ili neočekivanih događaja informacijske sigurnosti koji imaju veliku vjerojatnost ugrožavanja poslovnih procesa i prijetnje informacijskoj sigurnosti.

4. Interesne strane i zahtjevi

4.1 Interesne strane relevantne za ISMS

- Postojeći dobavljači s kojima OBV ima ugovoreno održavanje infrastrukture u opsegu ISMS-a (aplikativna, mrežna, sistemska infrastruktura, sustav kontrole pristupa, sustav video nadzora i sl.)
- Korisnici i klijenti (pacijenti)
- OBV
- Radničko vijeće
- Regulatori (Ministarstvo zdravstva i dr.)
- Republika Hrvatska (sva zakonska regulativa).

4.2 Zahtjevi

Zahtjevi interesnih strana:

- Postojeći dobavljači s kojima OBV ima ugovoreno održavanje ICT infrastrukture (aplikativna, mrežna, sistemska infrastruktura, sustav kontrole pristupa, sustav video nadzora i sl.) - tijekom samog procesa osigurati očuvanje povjerljivosti svih informacija koje se razmjenjuju.

- Korisnici i klijenti - demonstracija primjene najboljih svjetskih praksi i standarda iz područja informacijske sigurnosti prethodno razmatranju bilo kakve poslovne suradnje ili pružanja usluga.

- OBV – Usklađivanje kritičnih procesa sa najboljim svjetskim standardima i praksama. Tijekom pružanja informatičke podrške osigurati očuvanje povjerljivosti, cjelovitosti i raspoloživosti svih informacija koje se razmjenjuju, a sukladno Zakonu o tajnosti podataka i Uredbi o mjerama informacijske sigurnosti te Zakonu o kibernetičkoj sigurnosti.

- Radničko vijeće – davanje mišljenja na pravilnike i dokumentaciju OBV-a kako bi se utvrdila usklađenost sadržaja dokumentacije sa Zakonom o radu te gospodarskim i socijalnim pravima zaposlenih u OBV-u.

- Regulatori i Republika Hrvatska – zadovoljenje zahtjeva regulatora vezano uz sigurnost informacija što uključuje i
  - Zakon o informacijskoj sigurnosti,
  - Zakon o tajnosti podataka,
  - Zakon o zaštiti osobnih podataka,
  - Zakon o radu,
  - Zakon o zaštiti na radu,
  - Zakon o sustavu unutarnjih kontrola u javnom sektoru,
  - Zakon o arhivskom gradivu i arhivima,
  - Zakon o javnoj nabavi,
  - Zakon o pravu na pristup informacijama,
  - Uredba o mjerama informacijske sigurnosti,
  - Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/18),
  - Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 68/18),
  - Opća uredba o zaštiti osobnih podataka (GDPR),
  - Zakon o provedbi Opće uredbe o zaštiti podataka (NN 42/18),
  - Pravilnik o standardima sigurnosti neklasificiranih informacijskih sustava,
  - i svih ostalih povezanih zakona i podzakonskih akata Republike Hrvatske.

5. Sustav upravljanja informacijskom sigurnošću

Svrha sigurnosne politike je kroz primjenu odgovarajućih sigurnosnih mjera očuvanje povjerljivosti, cjelovitosti i raspoloživosti informacijske imovine OBV-a, njenih partnera i klijenata te kontinuitet rada informacijskih sustava, ključnih za nesmetano odvijanje poslovanja.

Ova politika i provedbeni akti, sačinjavaju program informacijske sigurnosti, koji mora omogućiti:

- fizičku zaštitu informacijskih sustava i okoline u kojoj su smješteni,
- očuvanje povjerljivosti informacija,
- očuvanje cjelovitosti informacija,
- jamstvo o trajnoj raspoloživosti kritičnih informacija,
- sprječavanje neovlaštenog objavljivanja informacija,
- sprječavanje uvida u privatne podatke radnika, drugih pravnih i fizičkih osoba u svrhe koje bi bile različite od zahtjeva poslovnog procesa ili protivne zakonskim odredbama,
- ispunjavanje svih drugih zakonskih ili ugovornih obaveza o zaštiti podataka,
- kontinuiranu edukaciju iz područja informacijske sigurnosti, dostupnu svim djelatnicima,
- istragu i izvješćivanje o svim sumnjivim ili dokazanim povredama i/ili slabostima sigurnosti informacijskog sustava.

Kako bi se omogućili mjerenje učinkovitosti upravljanja sigurnošću informacijskog sustava, OBV će uspostaviti sustav metrika za ključne sigurnosne kontrole informacijskog sustava. Uspostavljene sigurnosne metrike moraju biti mjerljive te moraju jednoznačno definirati kriterije na temelju kojih se procjenjuje učinkovitost odabranih sigurnosnih kontrola.

5.1 Ciljevi ISMS-a

Poslovodstvo OBV sustavno upravlja ciljevima informacijske sigurnosti.

Definirani ciljevi informacijske sigurnosti trebaju biti konkretni, u skladu s Politikom sigurnosti informacijskog sustava i kad god je to moguće mjerljivi. Ciljevi se definiraju, prate i održavaju, te o tome postoje zapisi. Na svim razinama rukovođenja i organiziranja utvrđena je odgovornost za ostvarenje ciljeva.

Ciljevi informacijske sigurnosti trebaju biti u skladu s ciljevima poslovanja, te osigurati

- očuvanje raspoloživosti, povjerljivosti i cjelovitosti informacija,
- podizanje razine sigurnosti informacijskog sustava
- podizanje razine svijesti korisnika informacijskog sustava

Ciljevi ISMS-a se definiraju, prate i održavaju od strane Odbora za ISMS. Njihova evaluacija se provodi minimalno jednom godišnje u sklopu donošenja Upravine ocjene.

Za ciljeve se evidentiraju slijedeće informacije:

- Cilj – područje cilja koje je u skladu s ovom politikom
- Odgovoran – navodi se odgovorna osoba/osobe za provedbu cilja
- Rok dovršetka – navodi se rok do kada je potrebno realizirati pojedini cilj
- Evaluacija rezultata/mjerilo – navodi se mjerilo kojim se evaluira ostvarenost cilja

O postignuću ciljeva po potrebi se informiraju zainteresirane strane.

6. Upravljanje rizicima informacijske sigurnosti

ISMS osigurava provedbu procesa upravljanja rizicima informacijske sigurnosti.

Proces upravljanja rizicima provodi se putem konkretnih sigurnosnih mjera, provedbom kojih će OBV osigurati ispunjenje ciljeva sustava ISMS-a.

Sigurnosne mjere donosi Uprava, na temelju prijedloga Odbora za ISMS (dalje u tekstu Odbor).

Proces upravljanja rizicima informacijske sigurnosti sastoji se od dvije osnovne i krovne aktivnosti: definiranje i unaprjeđenje postupka procjene rizike te provedbe postupka procjene rizika.

Proces procjene rizika obuhvaća:

- Identifikaciju i određivanje vrijednosti važnih informacija te aplikacija i sustava na kojima se nalaze,
- Određivanje prijetnji i ranjivosti identificirane imovine,
- Procjenu i izračun rizika informacijske sigurnosti na identificiranu imovinu
- Odabir kontrolnih ciljeva i opcija (mogućnosti) za tretiranje rizika,
- Definiranje i implementiranje sigurnosnih mjera za sve rizike koje je potrebno umanjiti.
- Odluku o potrebi provođenja procjene rizika donosi Odbor, na temelju poslovnih zahtjeva i važnosti pojedinih informacijskih sustava.

7. Nadležnosti i odgovornosti

U provođenju ISMS-a, sudjeluju sljedeće osobe i tijela:

- Uprava,
- Odbor za ISMS,
- Unutarnji revizor za informacijsku sigurnost,
- Voditelj sigurnosti informacijskog sustava (VSIS),
- Službenik za zaštitu osobnih podataka (SZOP),
- Vlasnici informacijske imovine.

Nadležnosti i odgovornosti prilikom korištenja informacijskih sustava OBV, definiraju se za sljedeće funkcije unutar Opsega:

- Rukovoditelji organizacijskih jedinica,
- Radnici (unutarnji korisnici informatičkih usluga koji nemaju rukovodeću ulogu),
- Druge pravne i fizičke osobe.

7.1 Uprava (Glavni direktor, savjetnici direktora)

Uprava:

- Imenuje članove Odbora,
- Imenuje Voditelja sigurnosti informacijskog sustava,
- Imenuje Unutarnjeg revizora informacijskog sustava,
- Donosi provedbene akte ove politike,
- Odgovara za uspostavu ISMS-a.

7.2 Odbor za ISMS

Odbor je nadležan za izradu programa informacijske sigurnosti i nacrta ove Politike, praćenje provođenja informacijske sigurnosti, dodjeljivanje uloga ljudskim resursima, definiranje odgovornosti, koordinaciju pri uvođenju ISMS-a te predlaganje mjera informacijske sigurnosti.

Članovi Odbora su:

- Član Uprave,
- Voditelj sigurnosti informacijskog sustava (VSIS),
- Unutarnji revizor informacijskog sustava,
- Rukovoditelj Odjela za informatiku,
- Po potrebi rukovoditelji organizacijskih jedinica (direktori, predstojnici službi/odjela) ili od njih ovlaštene osobe.

Redovite sjednice Odbora održavaju se 1x godišnje, a u slučaju potrebe, na prijedlog Uprave ili VSIS-a, sazivaju se izvanredne sjednice.

Odbor na sjednicama razmatra prijedloge VSIS-a vezano uz unaprjeđenje informacijske sigurnosti te na temelju izvješća Unutarnjeg revizora informacijskog sustava o provedenim revizijama sustava donosi odluke o preventivnim mjerama informacijske sigurnosti.

Pojedini članovi Odbora, za koje je primjenjivo, su odgovorni za praćenje trendova informacijske sigurnosti te informacija o novim ranjivostima kroz razne kanale poput kontinuiranih edukacija te pretplata na članke uglednih svjetskih organizacija iz domene informacijske sigurnosti.

Odbor izrađuje godišnja izvješća o stanju informacijske sigurnosti za Upravu.

7.3 Voditelj sigurnosti informacijskog sustava (VSIS)

VSIS nadzire provođenje cjelokupnog ISMS-a te analizira potrebe za izmjenama ove Politike i pripadajućih provedbenih akata.

VSIS na nalaze prethodnih procjena rizika i plana tretiranja rizika izrađuje nacrt godišnjeg plana informacijske sigurnosti koji uključuje:

- praćenje ukupnog stanja sigurnosti informacijskog sustava,
- termin i opseg provedbe detaljne procjene rizika,
- primjenu sigurnosnih mjera odnosno plana za tretiranje rizika,
- planove za provedbu projekata kojima je svrha poboljšati sigurnost informacijskog sustava.

VSIS provjerava provedbu mjera informacijske sigurnosti u svim organizacijskim dijelovima tvrtke i na svim dijelovima informacijskog sustava u opsegu ISMS-a.

Ako VSIS uoči odstupanje od propisanih mjera sigurnosti, dužan je provesti postupak koji će voditi otklanjanju uočenih nedostataka i otkrivanju uzroka i počinitelja.

VSIS je dužan izvještavati Upravu odnosno Odbor, o otkrivenim sigurnosnim incidentima informacijske sigurnosti, te o slučajevima nepoštivanja odredbi ove Politike i pripadajućih provedbenih akata.

VSIS sudjeluje u postupku izrade i razvoja informacijskih sustava radi primjene zahtjeva sigurnosti.

VSIS je odgovoran za nadzor implementacije tehničkih sigurnosnih mjera na informatičkim sustavima koje koristi tvrtka, te redovito praćenje njihove efikasnosti.

VSIS provodi postupak analize sigurnosnih incidenata informacijske sigurnosti na IT sustavima tvrtke.

VSIS brine o bilježenju nesukladnosti/neusklađenosti s ISMS-om na temelju nadzora uspostavljenih sigurnosnih kontrola u informacijskom sustavu.

7.4 Unutarnji revizor informacijskog sustava

Unutarnji revizor informacijskog sustava odgovoran je za redovito provođenje unutarnje revizije ISMS-a te brigu o svim zapisima nastalima provođenjem unutarnjih revizija.

Na temelju rezultata revizije, unutarnji revizor izrađuje prijedlog korektivnih mjera.

Unutarnji revizor informacijskog sustava obavezan je izvješće o nalazima unutarnje revizije i preporuke za unaprjeđenje ISMS-a prezentirati na sjednici Odbora.

Unutarnji revizor informacijskog sustava mora posjedovati primjerene kvalifikacije za reviziju iste.

7.5 Vlasnici informacijske imovine

Vlasnik informacijske imovine je osoba iz pojedinog poslovnog područja Bolnice zadužena za informacije koje se pohranjuju, prenose i obrađuju u informacijskim sustavima.

Vlasnika informacijske imovine za svako pojedino poslovno područje je rukovoditelj organizacijske jedinice odnosno od rukovoditelja imenovana osoba.

Vlasnici informacijske imovine dužni su sudjelovati u postupku određivanja sigurnosnih zahtjeva koji provodi VSIS, po pitanju povjerljivosti, integriteta i raspoloživosti, odnosno postupku procjene rizika za sve informacije koje su u njihovoj nadležnosti.

Vlasnici informacijske imovine nadziru rad uspostavljenih sigurnosnih kontrola te u suradnji s VSIS-om bilježe ISMS nesukladnosti.

7.6 Rukovoditelji organizacijskih jedinica

Rukovoditelji organizacijskih jedinica su odgovorni za praćenje provođenja odredbi ove Politike i pridržavanja pratećih provedbenih akata te za osiguravanje resursa potrebnih za implementaciju mjera unutar svojeg područja rada.

Rukovoditelji su dužni upoznati sve radnike i druge pravne i fizičke osobe u njihovom području rada sa postojanjem ove Politike i pripadajućih provedbenih akata te obvezom pridržavanja odredbi istih, kao i poduzimati odgovarajuće mjere u slučaju nepoštivanja tih odredbi od strane radnika.

Rukovoditelji informacijske imovine nadziru rad uspostavljenih sigurnosnih kontrola te u suradnji s VSIS bilježe ISMS nesukladnosti.

7.7 Radnici

Svi radnici, koji se prilikom obavljanja svojih redovitih radnih zadataka koriste s informacijskim sustavima i u njima pohranjenim informacijama, dužni su pridržavati se odredbi ove Politike i provedbenih akata te su obvezni prijaviti uočene sigurnosne propuste ili incidente informacijske sigurnosti.

7.8 Druge pravne i fizičke osobe

Druge pravne i fizičke osobe koje su prilikom izvršavanja poslova u doticaju s informacijskim sustavima Bolnice i u njima pohranjenim informacijama, dužni su pridržavati se odredbi ove Politike i svih provedbenih akata koji iz njega proizlaze, što mora biti utvrđeno formalnim dokumentom prije omogućavanja pristupa druge pravne i fizičke osobe informacijskim sustavima OBV.

7.9 Službenik za zaštitu osobnih podataka (SZOP)

Službenik za zaštitu osobnih podataka:

- obavještava ili savjetuje voditelja ili izvršitelja obrade, te zaposlenike koji obrađuju osobne podatke o njihovim obvezama iz Uredbe (GDPR),
- nadzire poštivanje Uredbe i njihovih politika i ostale regulative vezane uz zaštitu osobnih podataka,
- dodjeljuje odgovornosti za zaštitu osobnih podataka zaposlenicima i trećim stranama uključenim u prikupljanje i obradu osobnih podataka,
- podiže svijest zaposlenika i provodi edukacije iz područja zaštite osobnih podataka,
- ugrađuje zaštitu privatnosti u revizijske procese,
- savjetuje kod provedbe procjene učinka na zaštitu podataka i nadzire procese upravljanja rizikom u obradama osobnih podataka,
- vodi evidenciju zbirki odnosno obrada osobnih podataka,
- upravlja procesom obrade zahtjeva ispitanika u svezi njihovih prava sukladno zahtjevima Uredbe,
- surađuje s nadzornim tijelima (npr. Agencijom za zaštitu osobnih podataka).

8. Kompetencije ekspertnih uloga u ISMS-u

Ključne ekspertne uloge u pogledu provedbe poslova vezane uz upravljanje sustava informacijskom sigurnošću su *Voditelj sigurnosti informacijskog sustava* (VSIS, eng. Chief Information Security Officer) te *Unutarnji revizor informacijskog sustava.*

Za navedene radne uloge kontinuirano se podupire održavanje kompetencija u vidu pohađanja stručnih edukacija, tečaja, seminara, konferencija i slično.

Zahtjevi po pitanju kompetencija za navedene radne uloge sadrže minimalno:

- sveučilišna naobrazba, VSS elektrotehničkog ili informatičkog smjera odnosno ekonomija i management,
- radno iskustvo od najmanje 2 godine na istim ili sličnim poslovima,
- posjedovanje nekog od certifikata ili završenih treninga vezano uz informacijsku sigurnost i/ili reviziju IT/informacijskih sustava , odnosno neki od certifikata ili završenih treninga vezanih uz ISO 27001 (ili implementacijski ili revizorski treninzi),
- izrazite organizacijske sposobnosti, sposobnost procjene, planiranja i odlučivanja te nadasve proaktivan pristup radu.

9. Revizija pravilnika

Ova Politika predmet je kontinuirane revizije i poboljšanja, u svrhu očuvanja njene usklađenosti s poslovnim ciljevima te zakonskim i ugovornim obvezama OBV.

Revizija ove Politike provodi se u planiranim intervalima (jednom godišnje) i kod pojave značajnijih promjena u poslovanju.

10. Završne i prijelazne odredbe

Politika stupa na snagu i primjenjuje se danom njezinog donošenja.

KLASA: 011-02/23-01/20

URBROJ: 2186-192-30-23-1

U Varaždinu, 28.03.2023.

RAVNATELJ

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