Pravilnik o internom auditu 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 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	
3	
4	
5	

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	OBV – svi radnici	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 definira načine, odgovornosti i učestalost provedbe internih audita sustava upravljanja informacijskom sigurnošću (u nastavku ISMS) u Općoj bolnici Varaždin (u nastavku: OBV), kao i čuvanje i vođenje zapisa koji su rezultat provedenih internih audita.

2. Opseg

Postupak se primjenjuje na sve poslovne procese odnosno organizacijske jedinice OBV-a.

3. Odgovornosti

Interni auditor za informacijsku sigurnost ima odgovornost za provođenje internog audita IS, izradu planova audita i izvještaja o provedenom auditu. Obavljanje audita se može prepustiti vanjskom partneru specijaliziranom za provođenje audita ISMS-a.

Ulogu internog auditora informacijskog sustava obnaša osoba koja odgovarajuće kompetencije definirane Politikom sigurnosti informacijskog sustava.

Uprava OBV-a je odgovorna za osiguravanje potrebnih resursa za efikasno provođenje internog audita ISMS-a.

Korisnici informacijskog sustava OBV dužni su dati sve podatke koji su potrebni u procesu internog audita ISMS-a.

Odbor za ISMS odobrava i daje eventualne prijedloge za provođenje izvanrednog audita informacijskog sustava. Odbor pregledava izvještaj o internom auditu IS i koristi nalaze i preporuke za poboljšanja sustava upravljanja informacijskom sigurnošću odnosno definiranje popravnih radnji.

Voditelj sigurnosti informacijskog sustava (VSIS) surađuje s internim auditorom IS pri odabiru metodologije audita te definiranju perioda za provođenje audita.

4. Period provođenja internog audita informacijskog sustava

Postupak internog audita IS provodi se jednom godišnje, u terminu definiranom u godišnjem planu internog audita OBV-a.

Izvanredni audit se može provesti po nalogu Uprave OBV-a, odnosno na prijedlog Odbora za ISMS.

Interni audit informacijskog sustava planira interni auditor IS u suradnji s Voditeljem sigurnosti informacijskog sustava.

5. Definiranje kriterija za odabir auditora

Interni audit IS može provoditi interni auditor IS ili vanjska tvrtka. Interni auditor mora biti adekvatno educiran za provedbu audita prema normi ISO 27001, što uključuje, ali nije ograničeno na:

- posjedovanje ISO 27001 Auditor/Lead Auditor ili CISA certifikata, i/ili
- završen akreditirani *ISO 27001 internal auditor* seminar, i/ili
- neki drugi certifikat za audit/reviziju informacijskog sustava.

Odabir vanjskog auditora se radi na prijedlog internog auditora IS u dogovoru s Odborom za ISMS.

Vanjski auditor mora dokazati kompetentnost u ovom području, što uključuje provedbu barem jednog audita sustava prema ISO 27001 normi, završen akreditirani *ISO 27001 Internal auditor* seminar i/ili posjedovanje minimalno jednog od slijedećih stručnih certifikata:

- ISO 27001 Internal Auditor certifikat,
- ISO 27001 Auditor/Lead Auditor certifikat,
- CISA (Certified Information Systems Auditor) certifikat,
- CISSP (Certified Information Systems Security Professional) certifikat.

6. Odabir metodologije

Metodologija koja će se koristiti za provedbu postupka internog audita IS određuje se od strane Internog auditora IS u dogovoru s Voditeljem za informacijsku sigurnost.

Potrebno je odabrati metodologiju koja će minimalno utjecati na odvijanje poslovnih procesa OBV-a.

7. Izrada izvještaja o provedenom internom auditu

Na temelju provedenog postupka internog audita, interni auditor IS je dužan izraditi završni izvještaj o rezultatima provedenog audita te o tome izvijestiti Odbor za ISMS.

Izvještaj o provedenom auditu mora minimalno sadržavati sljedeće elemente:

- podatke o poslovnom procesu nad kojim je proveden postupak audita,
- podatke o opsegu, cilju i vrsti provedenog audita te vremenskom periodu u kojem je isti proveden,
- nalaze, mišljenja i preporuke vezane uz adekvatnost sigurnosnih kontrola unutar opsega ISMS sustava,
- adekvatne dokaze koji potvrđuju iznesene nalaze i mišljenja,
- upravljački sažetak i mišljenje auditora.

Svi dokumenti i zapisi koji proizađu iz postupka internog audita IS trebaju biti prikladno pohranjeni i čuvani.

8. Korištenje softverskih alata i stručne pomoći

Za potrebe utvrđivanja nedostataka u sustavima transakcija i sličnih zapisa sa velikim brojem stavaka, kao i sustava sa kompleksnim pravilima kontrole pristupa gdje nije moguće dobiti kvalitetne rezultate samo na osnovu ručno odabranog uzorka, OBV će ukoliko tako odluči interni auditor IS, koristiti softverski alat za provođenje audita i kontrolu informacijskog sustava. Ovakav alat bi se koristio u dubinskim testovima poput:

- testiranja postojanja dvostrukih podataka,
- pronalaženje odstupanja od standardnih vrijednosti,
- pronalaženja propusta u pravilima pristupa (npr. na vatrozidu),
- pronalaženje korisničkih računa sa prekomjernim ovlastima i
- drugih odgovarajućih testova.

Osim softverskih alata, Interni auditor IS za potrebe audita tehnički zahtjevnih sigurnosnih mjera, može dodatno zatražiti savjet neovisnog stručnjaka.

9. Postupak provedbe internog audita informacijskog sustava

Postupak internog audita započinje slanjem uvodne izjave svim voditeljima organizacijskih jedinica koji će biti uključeni u postupak audita, nakon čega interni auditor IS započinje s prikupljanjem svih potrebnih podataka i dokumenata za audit.

Nakon što auditor utvrdi postojanje i valjanost osnovnog dijela dokumentacije ISMS-a, internim auditom IS je potrebno slijedeće:

- Potvrditi da se OBV zaista i ponaša u skladu s propisanom Politikom sigurnosti informacijskog sustava i pripadajućim provedbenim aktima.
- Potvrditi da ISMS zadovoljava sve zahtjeve propisanih sigurnosnih politika te da ostvaruje ciljeve postavljene Politikom sigurnosti informacijskog sustava i u skladu sa zahtjevima regulative.

Nakon što utvrdi ispravno funkcioniranje obveznog dijela ISMS-a, auditor provjerava postojanje i ispravno funkcioniranje sigurnosnih kontrola (odabranih na temelju procjene rizika) u dijelu organizacije koji je predmet audita.

Pri određivanju opsega potrebne dokumentacije i zapisa koji će se provjeravati tijekom audita sigurnosnih kontrola, Interni auditor IS koristi **kontrolne liste** i rezultate procjene rizika odnosno plan za tretiranje rizika. Pri tome može zatražiti savjet stručnih osoba koje Voditelj sigurnosti informacijskog sustava proglasi mjerodavnima po pitanju implementacije specifične sigurnosne kontrole.

Ocjenjivanje sigurnosnih kontrola ISMS-a, obavlja se na temelju **testiranja sukladnosti i sadržaja** (*engl. Compliance – Substantive test*).

- **Test sukladnosti** provjerava jesu li kontrole implementirane na način kako je propisano (zakonom, pravilnicima, internim priručnicima i procedurama), dok **test sadržaja** pruža dokaze kako implementirane sigurnosne mjere štite povjerljivost, integritet i raspoloživost kritičnih poslovnih informacija.

  Testiranje sukladnosti obavlja se primjenom raznih tehnika poput intervjua, pregleda dokumentacije, anketiranja zaposlenika i vanjskih partnera, promatranjem implementacije i sl.

- **Testiranje sadržaja** obavlja se metodom uzorkovanja, gdje se za testirane sigurnosne kontrole odabire slučajni zapisi ili drugi dokazi koji trebaju dokazati ispravno funkcioniranje sigurnosne kontrole.

  Za provođenje **testa sadržaja** u onim slučajevima gdje ručno uzorkovanje ne može dati dobar rezultat zbog velikog broja stavki (npr. analiza transakcija), Interni auditor IS može odlučiti o korištenju nekog od specijaliziranih alata u tu svrhu.

Za vrijeme internog audita, auditor radi zapis temeljem kontrolne liste (*engl. „check list"*) koju obavezno prilaže uz **Izvještaj o internom auditu informacijskog sustava**. Sve utvrđene neusklađenosti moraju se usuglasiti s odgovornom osobom za auditirani proces, a samo one neusklađenosti za koje je utvrđen objektivni dokaz upisuju se u izvještaj.

U slučaju neslaganja odgovorne osobe za auditirani proces s nalazom auditora, konačnu odluku donosi Odbor za ISMS.

Nakon obavljenog audita, Interni auditor IS održava završni sastanak sa odgovornim osobama gdje ih upoznaje s rezultatima audita. Na temelju preporuka auditora, za svaku utvrđenu nesukladnost zajednički se dogovaraju popravne radnje i rokovi.

10. Izvješćivanje

Izvješće internog auditora treba predstavljati uredan zapis ciljeva audita, opsega, metodologije, nalaza, mišljenja i preporuka.

Interni auditor prvo izrađuje nacrt izvješće o rezultatima audita. Prije izrade konačnog izvješća, u pravilu, auditor treba raspraviti s vlasnikom auditiranog procesa o nalazima i preporukama iz nacrta izvješća, kako bi se izbjegla moguća kriva tumačenja auditora. Nakon toga, sastavlja se konačno izvješće u koje se stavlja očitovanje, odnosno dogovoreni rokovi i načini provođenja danih preporuka.

Konačno izvješće se prvom dostavlja Odboru za ISMS.

Nakon toga, dostavlja se Upravi OBV-a koja ne mora nužno biti upoznat sa svim detaljima izvješća. Radi toga je bitno da izvješće bude uravnotežena slika kompletnog procesa audita, a ne samo popis neusklađenosti te obvezno mora sadržavati upravljački sažetak.

Svako izvješće o obavljenom auditu treba sadržavati:

- Naziv audita,
- datum izrade,
- ime, prezime i kontakt podatke internog auditora IS te popis ostalih auditora koji su sudjelovali u izvođenju audita,
- predmet i područja koja su obuhvaćena auditom,
- cilj audita,
- mišljenja auditora,
- upravljački sažetak (globalni pogled na opće stanje i najvažnije preporuke),
- detaljan izvještaj o svakom nalazu s dokazima koji podupiru iskaz auditora, a sadrži ocjenu revidiranih područja, nedostatke i slabosti, nezakonitosti i nepravilnosti auditiranih područja,
- preporuke za poboljšanja s naznačenim prioritetima, dogovorenim načinom i rokovima za provođenje preporuka, te
- pozitivne nalaze sustava unutarnjih sigurnosnih mjera.

11. Završne i prijelazne odredbe

Pravilnik stupa na snagu i primjenjuje se danom njegovog donošenja.

KLASA: 011-02/23-01/19

URBROJ: 2186-192-30-23-1

U Varaždinu, 28.03.2023.

RAVNATELJ

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