Program podizanja svijesti o informacijskoj sigurnosti

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

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				
N/A	Uprava; Odbor ISMS	Digitalna kopija	N/A		
N/A	Odjel za informatiku	Digitalna kopija	N/A		
N/A	Središnja služba za opće, pravne i kadrovske poslove	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 Programom o podizanju svijesti zaposlenika i trećih strana o sigurnosti informacijskog sustava Opće bolnice Varaždin (u nastavku: OBV) omogućava se ostvarenje sljedećih ciljeva:

- zaposlenici i vanjski partneri su upoznati sa sigurnosnim kontrolama u OBV,
- zaposlenici i vanjski partneri su primjereno educirani o značaju informacijske sigurnosti te o svojim odgovornostima u zaštiti povjerljivosti, cjelovitosti i raspoloživosti informacija OBV,
- u konačnici viši stupanj zaštite osjetljivih informacija.

2. Opseg

Program se odnosi na sve zaposlenike OBV-a te na vanjske partnere/treće strane koji pristupaju i obrađuju podatke u informacijskom sustavu OBV-a.

3. Nadležnosti i odgovornosti

Voditelj sigurnosti informacijskog sustava (VSIS) je odgovoran za razvoj i ažuriranje ovog Programa. Također je odgovoran za provedbu smjernica koje se navode u Programu.

Rukovoditelj Odjela za informatiku brine o naprednim/specijalističkom pohađanju edukacije o informacijskoj sigurnosti u skladu s ovim Programom.

Rukovoditelj Središnje službe općih, pravnih i kadrovskih poslova brine o upoznatosti novih zaposlenika s internim dokumentima te osigurava upoznavanje zaposlenika s organizacijskom strukturom OBV.

4. Izvođenje programa podizanja svijesti o informacijskoj sigurnosti

Slijedećom tablicom prikazani su načini izvođenja programa podizanja svijesti o informacijskoj sigurnosti po grupama obuhvaćenih osoba:

Grupa/domena	Način izvođenja	Učestalost
Zapošljavanje novog djelatnika	Pristup na Intranet portal, mapa: Informacijska sigurnost. Zaposlenici su dužni pročitati dokumente. Način prihvaćanja akata je potpis zaposlenika na potpisnu listu za primitak akta. Također im se daje i organizacijska struktura OBV-a te	po dolasku na posao

	ih se upoznaje s voditeljima pojedine organizacijske jedinice, uključujući i funkciju VSIS. Opcionalno, dokumentaciju je moguće staviti i na oglasnu ploču, kako je predviđeno Pravilnikom o radu.	
Uvođenje u rad novog vanjskog partnera	Dostava dokumenata u elektroničkoj verziji: • Politika sigurnosti informacijskog sustava, • Pravilnik o primjerenom korištenju informacijskog sustava, • Pravilnik o upravljanju uslugama trećih strana, • Pravilnik o udaljenom pristupu informacijskom sustavu. Potrebna povratna informacija o pročitanosti dokumenata (npr. mailom).	po uvođenju novog vanjskog partnera
Informacije o ranjivostima i napadima	Po pojavi neke poznate ranjivosti ili napada koji su potencijalno primjenjivi i na informacijski sustav OBV-a, korisnicima u dosegu te ranjivosti/napada se šalje mail s pojašnjenjem odnosno upozorenjem	Po potrebi, u slučaju poznatog napada ili ranjivosti
Kratki podsjetnici na neke od sigurnosnih kontrola	Periodično (najmanje godišnje) slanje elektroničke pošte na zaposlenike s napomenama na neke od važećih sigurnosnih kontrola (npr. politika lozinke, upotreba maila i Interneta, prijava incidenta, klasifikacija informacija i sl.).	Minimalno 1 * godišnje
Zaposlenici u opsegu ISMS	Jednokratno slanje PPT prezentacije s osnovnim informacijama o uvođenju ISMS-a odnosno rizicima informacijske sigurnosti.	Jednokratno, jednom u tri godine
Voditelji viših organizacijskih jedinica	Jednokratna radionica i slanje PPT prezentacije s osnovnim pojmovima o zahtjevima GDPR uredbe.	Jednokratno i u slučaju promjene voditelja
Godišnja provjera znanja zaposlenika o informacijskoj sigurnosti	Provjera znanja zaposlenika o informacijskoj sigurnosti putem online testa s pitanjima. Nakon testa, ovisno o rezultatima moguće je poslati zaposlenicima dodatne materijale za poboljšanje znanja.	Godišnje
Napredna/ specijalistička edukacija	Potrebno je imati zapise o edukacijama vezanim za informacijsku sigurnost za ključna radna mjesta (vidjeti popis u nastavku programa).	Postepeno, u skladu s mogućnosti proračuna OBV
Ugrađivanje sigurnosnih kontrola pri	Ugrađivanje aktivnosti vezanih za informacijsku sigurnost (npr. gap analiza, procjena rizika, konfiguriranje dobrih sig. praksi, savjetovanje interne	Kontinuirano

operativnim aktivnostima i u projektima	revizije i sl.) pri operativnim aktivnostima i u izvođenju projekata.	

4.1 Sadržaj PPT prezentacije

PPT prezentacija koja se šalje zaposlenicima u opsegu ISMS-a treba imati sljedeća poglavlja odnosno domene:

- Uvod u koncepte informacijske sigurnosti (povjerljivost, cjelovitost, raspoloživost, rizici),
- Primjeri rizici odnosno prijetnji na informacijsku sigurnost,
- Regulatorne i/ili zakonske obveze za uvođenje ISMS-a,
- Pojašnjenje ISMS-a (što znači sustav te od čega se sastoji),
- Dokumentacija o sigurnosti informacijskog sustava (pravilnici, procedure, ...),
- Upravljanje informacijskom imovinom uključujući upravljanje rizicima,
- Sigurnosne kontrole.

4.2 Online test provjere znanja

Periodično (preporučeno jednom godišnje) zaposlenicima koji imaju pristup računalima (informacijskom sustavu OBV) se šalje poveznica (link) s online testom na koji je potrebno odgovoriti.

Rezultati se analiziraju te se poduzimaju odgovarajuće mjere (npr. ponovno slanje onima koji nisu popunili test, dodatna edukacija za one koji su slabo riješili test i sl.).

Online test će se izraditi s nekim od besplatnih i raspoloživih alata za tu svrhu (npr. Google Surveys).

4.3 Napredna/specijalistička edukacija o informacijskoj sigurnosti

Za pojedina radna mjesta koja su neposredno vezana uz informacijsku sigurnost, potrebno je osigurati primjerenu edukaciju, a kao potvrdu o tome imati zapise u vidu edukacijskih materijala ili potvrda odnosno certifikata o završenim edukacijama i prisustvovanju na konferencijama.

Radna mjesta odnosno funkcije za koje se očekuje primjerena edukacija o informacijskoj sigurnosti su:

- VSIS (voditelj sigurnosti informacijskog sustava) – neki od certifikata poput CISA, CISM, CRISC, CISSP i sl.;
- Administrator mrežnog servisa;
- Administrator baza podataka;
- Sistemski administrator za operativne sustave;
- Razvojni inženjer za ključne aplikativne sustave.

Ukoliko je neka od funkcija ili radnog mjesta eksternalizirana na vanjske partnere/treće strane, potrebno je voditi računa o potrebnim zapisima prilikom nabavljanja usluga odnosno proizvoda. Zapisi mogu primjerice uključivati:

- potvrde s odslušane edukacije,
- potvrde sudjelovanja na konferencijama,
- certifikate za pojedine domene informacijske sigurnosti,
- kupljene knjige, časopise i druge materijale,
- potvrde s online tečajeva ili drugih online kanala (npr. online foruma, baza podataka i sl.).

Napredna odnosno specijalistička edukacija o informacijskoj sigurnosti se planira svake godine u skladu s mogućnostima proračuna OBV.

5. Izvješćivanje

VSIS izvještava o provedbi programa podizanja svijesti o informacijskoj sigurnosti u sklopu godišnjeg izvješća o radu VSIS-a. Izvješće se šalje ISMS odboru na usvajanje.

6. Nepridržavanje

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

7. Završne i prijelazne odredbe

Pravilnik stupa na snagu i primjenjuje se danom njegovog donošenja.

KLASA: 011-02/23-01/2

URBROJ: 2186-192-30-23-1

U Varaždinu, 28.03.2023.

RAVNATELJ

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