Procedura za upravljanje sigurnosnim zapisima

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	Procedura za upravljanje incidentima u informacijskom sustavu
4	

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

Cilj Procedure je definirati pravila i proces upravljanja operativnim, sistemskim i sigurnosnim zapisima (u nastavku dokumenta: zapisi informacijskog sustava), u cilju omogućavanja rekonstrukcije događaja, utvrđivanja odgovornosti za aktivnosti ostvarene na informacijskom sustavu, otkrivanja neovlaštenog pristupa i radnja provedenih na informacijskom sustavu, identifikaciju problema te osiguravanje dokazivosti i neporecivosti radnji u informacijskom sustavu Opće bolnice Varaždin (dalje u tekstu: OBV).

Procedurom su obuhvaćeni slijedeći aspekti upravljanja zapisima informacijskog sustava:

- vrste zapisa informacijskog sustava,
- opseg prikupljanja zapisa informacijskog sustava,
- kvaliteta i potpunost zapisa informacijskog sustava,
- pohrana i zaštita pristupa zapisima informacijskog sustava,
- uloge i odgovornosti.

2. Opseg

Ovom Procedurom obuhvaćene su sve komponente informacijskog sustava OBV-a koje omogućuju generiranje i bilježenje zapisa o aktivnostima provedenim na informacijskom sustavu.

3. Vrste zapisa

U okviru informacijskog sustava OBV-a, zapisi informacijskog sustava dijele se u tri kategorije:

- **Funkcionalni** – zapisi informacijskog sustava koji sadrže informacije o radu i funkcionalnom stanju informacijskog sustava. Zapisi unutar ove kategorije namijenjeni su prvenstveno djelatnicima Odjela za informatiku s ciljem praćenja ispravnosti i nadzora rada informacijskog sustava. U ovu kategoriju spadaju slijedeći tipovi zapisa:
    - pogreške operacijskog sustava vezane uz neispravnost i/ili probleme s hardverom,
    - pogreške u radu mrežnih servisa i/ili aplikacija,
    - statusi i informacije o pokretanju/zaustavljanju pojedinih mrežnih servisa i/ili aplikacija,
    - podaci o performansama komponenti informacijskog sustava,
    - dijagnostički zapisi i sl.
- **Sigurnosni** – zapisi informacijskog sustava koji sadrže informacije o sigurnosnim događajima u informacijskom sustavu. Zapisi unutar ove kategorije namijenjeni su Odjelu za informatiku i Voditelju sigurnosti informacijskog sustava s ciljem praćenja i nadzora sigurnosti informacijskog sustava te uočavanja potencijalnih sigurnosnih incidenata i odstupanja od uobičajenog stanja.

  U ovu kategoriju spadaju slijedeći tipovi zapisa:

- prijave za rad u informacijski sustav,
- upravljanje korisničkim računima,
- korištenje povlaštenih privilegija,
- nadzor udaljenog pristupa,
- informacije o propuštenim odnosno blokiranim konekcijama,
- izmjene konfiguracija u informacijskom sustavu,
- pristup podacima informacijskog sustava,
- brisanje/inicijalizacija log repozitorija i sl.

- **Poslovni** – zapisi informacijskog sustava koji sadrže informacije o korištenju poslovnih informacija pohranjenih u informacijskom sustavu. Zapisi unutar ove kategorije namijenjeni su prvenstveno vlasnicima poslovnih informacija koji ih nadziru, Voditelju sigurnosti informacijskog sustava te Odjelu za informatiku s ciljem nadzora neovlaštene upotrebe podataka pohranjenih u poslovnim aplikacijama.

  U ovu kategoriju spadaju slijedeći tipovi zapisa:

  - uvid u poslovne podatke,
  - izmjena poslovnih podataka,
  - brisanje poslovnih podataka.

4. Prikupljanje sigurnosnih zapisa

Zapisi se minimalno moraju bilježiti sa slijedećih komponenti informacijskog sustava OBV-a:

- mrežni uređaji (preklopnici, usmjerivači i druga mrežna oprema),
- operacijski sustavi poslužitelja informacijskog sustava,
- virtualizacijske okoline,
- produkcijska poslovna okruženja (poslovne aplikacije, aplikacijski poslužitelji, baze podatka i drugi softver koji se koristi za pristup informacijama kao npr. web i aplikacijski poslužitelji itd.),
- specijalizirani hardver/softver za nadzor i zaštitu informacijskog sustava (antivirus, IDS/IPS sustavi, vatrozid, uređaji za filtriranje web sadržaja itd.).

Svaki novi sustav koji se uključuje u informacijski sustav, a sukladno procjeni rizika, mora biti podešen da generira zapise informacijskog sustava. Bilo koje iznimke u informacijskom sustavu vezane uz odstupanje u odnosu na odredbe ove Procedure moraju biti odobrene i evidentirane.

5. Pohrana i zaštita zapisa

U trenutku kada se stvore uvjeti za centralno prikupljanje zapisa informacijskog sustava, za sve zapise u opsegu bilježenja potrebno je odrediti lokaciju na koju se pohranjuju, prava pristupa zapisima i rok čuvanja pohranjenih zapisa.

Za sustave koji prikupljaju zapise potrebno je osigurati sljedeće:

- osigurati integritet pohranjenih zapisa i onemogućiti promjene,
- ograničiti pristup zapisima u skladu s poslovnim potrebama, pri čemu se treba služiti načelom minimalnih ovlasti (eng. *need-to-know*).

6. Sinkronizacija vremena

Svi produkcijski sustavi OBV-a konfigurirani su za korištenje jednog od internih NTP poslužitelja za održavanje sinkronizacije vremena s drugim sustavima u okolini.

Interni NTP poslužitelji konfigurirani su tako da zahtijevaju ažuriranje vremena od provjerenih i pouzdanih javno dostupnih NTP poslužitelja.

Klijentski sustavi OBV-a koji su u mogućnosti dobiti podatke o postavkama vremena internih NTP poslužitelja kontroliraju se listama kontrole pristupa (Access Control Lists - ACLs).

NTP sustav se redovno ažurira najnovijim verzijama softvera.

7. Incidenti

U slučaju da djelatnik zadužen za pregledavanje sigurnosnih zapisa uoči pojedinačni događaj ili primijeti međuodnos dvaju ili više odvojenih događaja koji upućuju na sigurnosni problem/prijetnju, dužan je prijaviti sigurnosni incident sukladno *Proceduri za upravljanje incidentima u informacijskom sustavu*.

8. Uloge i odgovornosti

Vlasništvo nad zapisima informacijskog sustava definirano je na slijedeći način:

- **Vlasnik funkcionalnih i sigurnosnih zapisa** je Odjel za informatiku.
- **Vlasnik poslovnih zapisa** je organizacijska jedinica (Služba/Odjel), koja je vlasnik informacija za koje je omogućeno bilježenje zapisa informacijskog sustava.

Administrator sustava unutar Odjela za informatiku odgovoran je za:

- podešavanje pravila bilježenja zapisa informacijskog sustava koje će omogućiti generiranje zapisa informacijskog sustava u skladu s poslovnim zahtjevima Odjela te uputama Voditelja sigurnosti informacijskog sustava,
- osiguravanje kvalitete i potpunosti zapisa informacijskog sustava,

- periodično pregledavanje svih tipova zapisa informacijskog sustava u domeni vlastite nadležnosti,
- obavještavanje Rukovoditelja Odjela za informatiku i Voditelja sigurnosti informacijskog sustava o svim detektiranim događajima koji upućuju na sigurnosne incidente, kršenje Politike sigurnosti informacijskog sustava i drugih internih akata koji iz nje proizlaze.

Voditelj sigurnosti informacijskog sustava odgovoran je za:

- davanje pisanih preporuka i uputa Odjelu za informatiku za podešavanje pravila bilježenja zapisa informacijskog sustava (eng. *auditing* politike), s ciljem usklađivanja sa sigurnosnim, poslovnim i regulatornim zahtjevima,
- periodično pregledavanje zapisa informacijskog sustava za koje je omogućena pohrana i pregled,
- poduzimanje korektivnih mjera u slučaju detekcije sigurnosnih događaja koji upućuju na kršenje *Politike sigurnosti informacijskog sustava* i drugih internih akata koji iz nje proizlaze.

Vlasnik poslovnih informacija za poslovne zapise informacijskog sustava, a za koje smatra da je nužno pohranjivati, odgovoran je za:

- specifikaciju zahtjeva za generiranje i bilježenje zapisa informacijskog sustava, Odjelu za informatiku i Voditelju sigurnosti informacijskog sustava. Zahtjev mora sadržavati minimalno slijedeće informacije:
  - poslovni razlog zbog kojeg se zahtjeva generiranje i bilježenje zapisa za poslovne informacije informacijskog sustava,
  - potencijalnu štetu koja može proizaći uslijed događaja koji je potrebno bilježiti,
  - popis informacija za koje se zahtjeva bilježenje zahtjeva sa preciznim opisom njihove lokacije,
  - korisničke akcije za koje se želi generirati i bilježiti zapis informacijskog sustava (pristup/čitanje, izmjena, brisanje).

9. Završne i prijelazne odredbe

Procedura stupa na snagu i primjenjuje se danom njezinog donošenja.

KLASA: 011-02/23-01/3

URBROJ: 2186-192-30-23-1

U Varaždinu, 28.03.2023.

RAVNATELJ

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