PROCEDURA ZA UPRAVLJANJE BEZBEDNOSNIM INCIDENTIMA IKT SISTEMA

Odgovoran za primenu procedure	Lice za bezbednost podataka Novica Krsmanović
Nosilac procedure	Rukovodilac Odseka informacionih sistema i tehnologija Novica Krsmanović
Proceduru odobrio	Direktor UDK Doc.dr Siniša Dučić

S a d r ž a j

1 SVRHA

Svrha procedure je da definiše aktivnosti i odgovorna lica koja upravljaju bezbednosnim incidentima ukoliko do njih dođe, s ciljem da se unapredi proces zaštite IKT resursa i smanji mogućnost narušavanja njihove bezbednosti sa svih aspekata.

2 PREDMET I PODRUČJE PRIMENE

Ova procedura utvrđuje odgovornost, aktivnosti kao i nosioce aktivnosti koje se sprovode prilikom reakcije na bezbednosne incidente.

Primenjuje se na sve zaposlene UDK koji pristupaju IKT i IS/BIS Heliant UDK radi izvršavanja radnih zadataka.

3 REFERENCE I VEZE SA DRUGIM DOKUMENTIMA

Procedura je u vezi sa sledećim dokumentima:

- Akt o bezbednosti IKT sistema Univerzitetske dečje klinike;
- Uputstvo o bezbednosti informaciono - komunikacionog sistema Univerzitetske dečje klinike;
- PR.BZB 01 Procedura za rad Odseka informacionih sistema I tehnologija
- PR.BZB 16 Procedura za obezbeđivanje rada tokom i nakon incidenta u IKT sistemu.

4 DEFINICIJE I SKRAĆENICE

UDK - Univerzitetska dečja klinika;

OJ - Organizaciona jedinica UDK;

Odsek informacionih sistema i tehnologija – sastavni deo Službe investicionog tehničkog održavanja, pomoćnih poslova, bezbednosti i zaštite na radu;

IKT sistem je informaciono-komunikacioni sistem UDK u smislu tehnološko-organizacione celine koja obuhvata:

1. elektronske komunikacione mreže u smislu zakona koji uređuje elektronske komunikacije;
2. uređaje ili grupe međusobno povezanih uređaja, takvih da se u okviru uređaja, odnosno u okviru barem jednog iz grupe uređaja, vrši automatska obrada elektronskih podataka korišćenjem računarskog programa;
3. elektronske podatke koji se čuvaju, obrađuju, pretražuju ili prenose pomoću sredstava iz tač. 1. i 2. a u svrhu njihovog rada, upotrebe, zaštite ili održavanja;
4. organizacionu strukturu putem koje se upravlja IKT sistemom;

Korisnik je zaposleni UDK koji ima pristup IKT sistemu radi obavljanja svojih poslovnih aktivnosti;

Administrator IKT - zaposleni Odseka informacionih sistema i tehnologija kome je dozvoljeno administriranje IKT i/ili BIS sistema**;**

BIS Heliant (informacioni sistem) je deo IKT sistema UDK koji je namenjen planskom prikupljanju, skladištenju, obradi i razmeni informacija / podataka o pacijentima i lečenju, kao i informacija koje su značajne za poslovne procese UDK, a na način takav da su informacije dostupne i upotrebljive svima koji su ovlašćeni da ih koriste;

Incident - unutrašnja ili spoljna okolnost ili događaj kojim se ugrožava ili narušava informaciona bezbednost;

Informaciona bezbednost predstavlja skup mera koje omogućavaju da elektronski podaci kojima se rukuje putem IKT sistema budu zaštićeni od neovlašćenog pristupa, kao i da se zaštiti tajnost, integritet, raspoloživost, autentičnost i neporecivost tih podataka, da bi IKT sistem funkcionisao kako je predviđeno, kada je predviđeno i pod kontrolom ovlašćenih lica;

Vendor - treće lice sa kojim UDK sarađuje po osnovu ugovora o održavanju IKT sistema ili njegovih delova;

Lice zaduženo za bezbednost podataka - zaposleni UDK, lice koje se bavi poslovima informacione bezbednosti;

Lice zaduženo za zaštitu podataka o ličnosti – zaposleni UDK, lice koje se bavi zaštitom podataka o ličnosti.

5 ODGOVORNOSTI

Svaki zaposleni je dužan da se ponaša u skladu sa procedurom i u skladu sa svojim zaduženjima će snositi odgovornost na osnovu Pravilnika o disciplini i ponašanju zaposlenih UDK.

Saradnici UDK, kao i vendori su dužni da se ponašaju u skladu sa ugovorom koji sadrži klauzulu poverlivosti (kao i potpisanom Izjavom o poverljivosti podataka – eksterna) i u skladu sa njim će snositi odgovornost.

Obaveza rukovodioca svake organizacione jedinice UDK je da upozna sa ovom procedurom sve zaposlene i novozaposlene, bilo da su u radnom odnosu za stalno ili na određeno vreme.

Za kontrolu sprovođenja procedure odgovorni su rukovodilac Odseka informacionih sistema i tehnologijai Lice za bezbednost podataka IKT UDK.

6 OPIS PROCEDURE

6.1 Incidenti

Vrste incidenata detaljno su opisane u PR.BZB16 Procedura za obezbeđivanje rada tokom i nakon incidenta u IKT sistemu.

6.2 Priprema i planiranje odgovora na incidente

Administrator IKT UDK, zajedno sa informatičarem na poslovima tehničke podrške se na svakodnevnom nivou bavi poslovima planiranja, detekcije, analize bezbednosti IKT.

Potrebno je da oba lica poseduju odgovarajuća tehnička znanja kako bi na najbrži i odgovarajući način mogli da odgovore na bezbednosne incidente.

Lice zaduženo za bezbednost podataka u saradnji sa rukovodiocem Odseka informacionih sistema i tehnologija je u obavezi da pripremi, redovno unapređuje u skladu sa dostupnom IT tehnologijom, „Plan za prevenciju bezbednosnih rizika“ i pripremi nekoliko metoda komunikacije koje bi mogle da se primene u zavisnosti od incidenta.

Moguće metode komunikacije su: elektronska pošta, veb sajtovi (interni, eksterni, portali), telefonska komunikacija, govorna poruka, pisano izveštavanje, direktan kontakt.

6.3. Postupanje u slučaju bezbednosnih incidenata

U UDK se primenjuju mere koje obezbeđuju kontinuitet obavljanja posla u vanrednim okolnostima u skladu sa Procedurom obezbeđivanje kontinuiteta poslovanja tokom i nakon incidenta, kao i druge mere koje bi omogućile da IKT sistem u što kraćem roku bude u funkcionalnom stanju.

6.4. Izveštavanje o događajima u vezi sa bezbednošću informacija

Ukoliko bilo koji zaposleni UDK u toku svog rada na IKT resursima UDK zapazi neobične aktivnosti, u obavezi je da odmah obavesti Administratora IKT o uočenim i utvrđenim slabostima IKT sistema. Potrebno je to uraditi u što kraćem roku, kako bi se eventualni incidenti ili narušavanje bezbednosti informacija sprečili i predupredio nastanak štete.

Zaposleni koji smatra da je došlo do zloupotrebe podataka ili je primetio neke neuobičajene događaje u IKT sistemu mora što je pre moguće da pripremi opis problema i prijavi ga putem elektronske pošte Administratoru IKT i/ili telefonskim pozivom.

Administrator IKT vrši proveru prijavljenog incidenta i ukoliko posumnja da je u pitanju bezbednosni incident obaveštava rukovodioca Odseka informacionih sistema i tehnologija i Lice zaduženo za bezbednost podataka UDK.

Događaji u vezi sa bezbednošću podataka i informacija se ocenjuju timski od strane odgovornih lica Odseka informacionih sistema i tehnologija i u skladu sa tim se donosi odluka da li je potrebno da se klasifikuju kao incidenti narušavanja bezbednosti informacija.

6.5 Zapisivanje aktivnosti u okviru upravljanja incidentima i postupanje sa sudskim dokazima

Administrator IKT i rukovodilac Odseka informacionih sistema i tehnologijavode evidenciju o svim incidentima, kao i prijavama incidenata. Prema proceduri za obezbeđivanje rada tokom i nakon incidenta u IKT sistemu UDK, u obavezi su da periodično i po potrebi ukoliko to događaji nalažu, izveštavaju odgovorno lice – Lice zaduženo za bezbednost podataka.

U skladu sa Pravilnikom o ponašanju zaposlenih UDK se mogu (u zavisnosti od težine prekršaja bezbednosnih procedura) sprovesti disciplinski, prekršajni ili krivični postupak.

Administrator IKTa je:

- nadležan za planiranje, praćenje, analizu, izveštavanje i preduzimanje aktivnosti na planu sprovođenja usvojene politike i procedura o bezbednosti IKT sistema;
- autorizovan za preduzimanje hitnih i neodložnih mera u slučaju postojanja neposredne opasnosti za podatke i dokumentaciju koje su pod merama zaštite,
- nadležan za internu pojedinačnu ili grupnu edukaciju zaposlenih iz oblasti IKT bezbednosti u saradnji sa Licem za bezbednost podataka UDK.

Administrator IKT je primenom procedura za identifikaciju, sakupljanje, nabavku i čuvanje informacija u obavezi da prikuplja sva elektronska i papirna dokumenta koje mogu da služe kao dokaz u slučaju pokretanja kaznenih mera unutar organizacije.

Uz postojeće procedure rada i bezbednosti IKT sistema, potrebno je u nastupajućem periodu generisati i sledeća dokumenta:

- Plan za obezbeđenje kontinuiteta poslovanja za hardverske komponente IKT i
- Plan oporavka od neželjenih događaja IKT servera,

Koji definišu sve korake za identifikaciju, sakupljanje, nabavku i čuvanje informacija koje mogu da služe kao dokaz u slučaju pokretanja kaznenih mera unutar organizacije.

Prikupljeno znanje iz navedene analize i rešavanja incidenata koji su narušili bezbednost informacija, zaposleni UDK odnosno odgovorna lica, koriste da bi se identifikovali incidenti koji se ponavljaju i smanjila verovatnoća i uticaj budućih incidenata.

6.6 Odgovor na incidente i komunikacija sa internim i eksternim osobama/organizacijama

Ukoliko se evidentira događaj klasifikovan kao incident, tada se obaveštava Lice zaduženo za bezbednost podataka, koje u skladu sa svojim ovlašćenjima, prema članu 4. Zakona o informacionoj bezbednosti, obaveštava:

- Lice za zaštitu podataka o ličnosti,
- Direktora UDK,
- RATEL i CERT.

Obaveštenje o incidentu mora da sadrži sledeće podatke:

- vrstu incidenta;
- opis incidenta;
- vreme pojave incidenta;
- trajanje incidenta;
- posledice koje je incident izazvao;

- preduzete aktivnosti radi ublažavanja incidenta;
- dodatne relevantne informacije.

Svaki incident se posle njegovog saniranja detaljno razmatra i izveštaj podnosi Timu za koordinaciju i podršku implementaciji bezbednosti IKT.

Izveštaj treba da sadrži sledeće elemente:

- Vreme nastanka,
- Uzrok nastanka,
- Odgovorna lica,
- Procenu štete koja je nastala,
- Procenu štete koja je mogla da nastane,
- Način saniranja,
- Predlog preventivnih mera da se u budućnosti ne bi ponovio incident,
- Predlog korektivnih mera.

7 PRAVNI OSNOV

- Zakon o informacionoj bezbednosti („Sl.glasnik RS", br. 6/2016, 94/2017);
- Zakon o zdravstvenoj dokumentaciji i evidencijama u oblasti zdravstva („Sl.glasnik RS", br. 123/2014, 106/2015, 105/2017, 25/2019);
- Zakon o zaštiti podataka o ličnosti („Sl.glasnik RS", br. 87/2018).