

	UNIVERZITETSKA DEČJA KLINIKA, BEOGRAD TIRŠOVA 10			PR.BZB 16
	IZDANJE/IZMENA 1/0	VAŽI OD 01.12.2020.	STRANA 1 od 9	

PROCEDURA ZA OBEZBEĐIVANJE RADA TOKOM I NAKON INCIDENTA U IKT SISTEMU UDK

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

	IZDANJE / IZMENA	VAŽI OD	STRANA	PR.BZB 16
	1/0	01.12.2020.	2 od 9	

S a d r ž a j

1	SVRHA	3
2	PREDMET I PODRUČJE PRIMENE	3
3	REFERENCE I VEZE SA DRUGIM DOKUMENTIMA	3
4	DEFINICIJE I SKRAĆENICE.....	3
5	ODGOVORNOSTI	4
6	OPIS PROCEDURE.....	4
6.1	Incidenti.....	4
6.2	Vrste incidenata.....	4
6.3	Aktivnosti u slučaju bezbednosnog incidenta.....	5
6.4	Kontinuitet poslovanja tokom bezbednosnog incidenta.....	6
6.4.1	Incidenti koji uzrokuju prekid u funkcionisanju sistema ili dela sistema	6
6.4.2	Incidenti u vezi neovlašćenog pristupa, gubitka, izmene ili oticanja podatka	8
6.4.3	Incidenti u vezi provaljivanja u IKT sistem	8
6.5	Aktivnosti nakon incidenta.....	9
7	PRAVNI OSNOV.....	9

	IZDANJE / IZMENA	VAŽI OD	STRANA	PR.BZB 16
	1/0	01.12.2020.	3 od 9	

1 SVRHA

Svrha procedure je da obezbedi potrebne procese u radu IKTa kako bi se funkcionisanje UDK obavljalo nesmetano u slučaju incidenta i to kako za vreme incidenta, tako i posle eventualnog neželjenog događaja, s ciljem da se unapredi bezbednost podataka.

2 PREDMET I PODRUČJE PRIMENE

Ova procedura utvrđuje aktivnosti, nosioce aktivnosti i odgovornosti koje se sprovode prilikom događanja incidenta i nakon toga, u cilju obezbeđivanja kontinuiteta rada UDK tokom i nakon bezbedonosnog incidenta.

Primenjuje se na sve zaposlene UDK koji pristupaju IKT UDK radi izvršavanja svojih radnih zadataka.

3 REFERENCE I VEZE SA DRUGIM DOKUMENTIMA

Procedura je u vezi sa 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 09 Procedura o zaštiti od zlonamernog softvera;
- PR.BZB 12 Procedura za izradu rezervnih kopija (*backup-a*);
- PR.BZB 14 Procedura uključivanja i isključivanja servera;
- PR.BZB 15 Procedura za upravljanje bezbednosnim incidentima IKT sistema

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;

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;

	IZDANJE / IZMENA	VAŽI OD	STRANA	PR.BZB 16
	1/0	01.12.2020.	4 od 9	

Lista IKT resursa i usluga Odseka informacionih sistema i tehnologija je elektronska baza evidencija IKT resursa i usluga koje Odsek pruža u UDK;

Radna stanica je personalni računar sačinjen od hardverskih i softverskih komponenti sa monitorom, tastaturom i mišem, namenjena obavljanju poslovnih aktivnosti;

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;

Zahtev za uslugu Odseka - Zahtev za uslugom Odseka informacionih sistema i tehnologija;

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

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 su dužni da se ponašaju u skladu sa ugovorom i potpisanom Izjavom o poverljivosti i u skladu sa njima 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 tehnologija i administrator IKT.

6 OPIS PROCEDURE

UDK planira i sprovodi preventivne mere koje obezbeđuju kontinuitet obavljanja posla u predvidljivim vanrednim okolnostima. Takođe, UDK radi na tome da omogući što je veći broj mera i aktivnosti koje bi omogućile da IKT sistem u nepredviđenim vanrednim uslovima u što kraćem roku bude u operativnom stanju.

6.1 Incidenti

Incidenti u IKT sistemu se mogu višestruko klasifikovati. To su unutrašnje ili spoljne okolnosti ili događaji kojima se ugrožava ili narušava informaciona bezbednost.

Mogu se podeliti na nekoliko tipova, i to:

- incidenti koji dovode do prekida kontinuiteta poslovnih procesa i pružanja usluga, odnosno znatnih teškoća u vršenju poslovnih procesa i pružanju usluga UDK;
- incidenti koji utiču na veliki broj korisnika usluga UDK;
- incidenti koji dovode do prekida kontinuiteta, odnosno poteškoća u vršenju poslovnih procesa i pružanja usluga, koji utiču na obavljanje poslovnih procesa i pružanja usluga drugih operatora IKT sistema od posebnog značaja ili utiču na javnu bezbednost;
- incidenti koji dovode do prekida kontinuiteta, odnosno teškoće u vršenju poslovnih procesa i pružanju usluga i imaju uticaj na veći deo teritorije Republike Srbije;
- incidenti koji dovode do neovlašćenog pristupa zaštićenim podacima čije otkrivanje može ugroziti prava i interese onih na koje se podaci odnose.

6.2 Vrste incidenata

Kategorizacija incidenata je zasnovana na sledećoj podeli:

	IZDANJE / IZMENA	VAŽI OD	STRANA	PR.BZB 16
	1/0	01.12.2020.	5 od 9	

1. provaljivanje u IKT sistem – napad na računarsku mrežu i serversku infrastrukturu u okviru koga je, kršenjem mera zaštite, ostvaren pristup koji omogućava neovlašćen uticaj na rad IKT sistema;
2. oticanje podataka – dostupnost zaštićenih podataka van kruga lica ovlašćenih za pristup podacima;
3. neovlašćena izmena podataka (lažiranje ili falsifikovanje podataka);
4. gubitak podataka (neodgovorno ponašanje);
5. prekid u funkcionisanju sistema ili dela sistema iz bilo kog razloga;
6. ograničavanje dostupnosti usluge (*denial of service*);
7. instaliranje zlonamernog softvera u okviru IKT sistema;
8. neovlašćeno prikupljanje podataka putem neovlašćenog nadzora nad komunikacijom ili socijalnim inženjeringom;
9. neprestani napad na određene resurse;
10. zloupotreba ovlašćenja pristupa resursima IKT sistema;
11. ostali incidenti.

6.3 Aktivnosti u slučaju bezbednosnog incidenta

U slučaju bezbednosnog/ih incidenta od izuzetne važnosti je ispravno postupiti, u skladu sa definisanim pravilima. Obično se čitav proces postupaka definiše „Planom kontinuteta poslovanja IKT“ i „Planom oporavka IKT sistema u slučaju incidenata i vanrednih uslova“. UDK će u narednom periodu definisati ove planove i u skladu s tim procedure.

Postupanje u slučaju bezbednosnog incidenta ima nekoliko faza. Prva, početna faza podrazumeva uspostavljanje kontrole (formiranje) pomoću Tima za rešavanje incidenta. U ovom Tmu pored predstavnika top menadžmenta, treba da bude i sistem administrator IKT UDK. Osnovno zaduženje Tima je

- uspostavljanje kontrole primenom definisanih postojećih mera,
- uvođenjem novih mera i
- pribavljanjem potrebnih alata i resursa.

U nastupajućem periodu rukovodilac Odseka informacionih sistema i tehnologija sa drugim odgovornim licima UDK će obaviti pripremne radnje i planirati izradu ovih planova i imenovanje Tima.

U međuvremenu, zaposleni i rukovodilac Odseka pokušavaju da prepoznaju i ograniče broj potencijalnih bezbednosnih incidenata pravilnim odabirom i primenom niza bezbednosnih mera koje počivaju na rezultatima kontinuirane procene rizika.

Procena rizika i planiranje potrebnih aktivnosti uključuje stalne aktivnosti kao što su:

- otkrivanje opštih pretnji;
- otkrivanje specifičnih pretnji;
- procena adekvatnosti postojećeg nivoa zaštite i otkrivanje bezbednosnih slabosti ili propusta;
- procena potrebnog nivoa zaštite;
- usklađivanje postojećeg sa potrebnim nivoom zaštite.

U slučaju pojave bezbednosnog incidenta, potrebno je:

1. otkrivanje bezbednosnog propusta i
2. prijavljivanje incidenta nadležnim organima i licima i to:
 - o administrator IKT UDK prijavljuje rukovodiocu Odseka informacionih sistema i tehnologija;

	IZDANJE / IZMENA	VAŽI OD	STRANA	PR.BZB 16
	1/0	01.12.2020.	6 od 9	

- o rukovodilac Odseka informacionih sistema i tehnologija prijavljuje događaj Licu zaduženom za bezbednost podataka i Licu zaduženom za zaštitu podataka o ličnosti, kao i direktoru UDK.

Lica zadužena za bezbednost podataka i zaštitu podataka o ličnosti će, ukoliko je potrebno, prijaviti odgovarajućim nadležnim organima u skladu sa svojim odgovornostima i proceni tipa događaja (RATEL ili Poverenik za informacije od javnog značaja).

U zavisnosti od težine, obima i ozbiljnosti incidenta, UDK može preduzeti odgovarajuće mere radi smanjivanja posledica i oporavka od incidenta među kojima je i zamena kredencijala na napadnutim resursima.

Za bezbednosne incidente manjeg obima, nisu nužne opsežne analize, osim incidenata kod kojih su korišćene nove metode napada kako bi se slični napadi izbegli ili brže i efikasnije sanirali u budućnosti.

Incident može biti kategorisan kao:

- incident internog tipa gde se može sprovesti kontinuitet poslovanja;
- i kao incident eksternog tipa gde je potrebno i dodatno uključivanje Vendora.

Svaki incident, bilo kog tipa, bez obzira na težinu potrebno je evidentirati i o njemu obavestiti Lice za bezbednost IKTa UDK.

Administrator IKT UDK i rukovodilac Odseka informacionih sistema i tehnologija vode jedinstvenu evidenciju svih incidenata.

6.4 Kontinuitet poslovanja tokom bezbednosnog incidenta

6.4.1 Incidenti koji uzrokuju prekid u funkcionisanju sistema ili dela sistema

Ukoliko se desi incident koji je definisan kao uzrok otežavanja ili onemogućavanja rada zaposlenih UDK, najpre se sprovodi analiza incidenta. Ukoliko je incident prouzrokovao prekid u funkcionisanju sistema ili dela sistema, u zavisnosti od obima prekida, sprovode se sledeće aktivnosti:

6.4.1.1. Prekid rada jedne radne stanice jednog Korisnika (tj. jedan računar u mreži IKT UDK)

Aktivnost: Administrator IKT UDK proverava, testira mrežu a zatim informatičar na poslovima tehničke podrške vrši popravku identifikovane sporne radne stanice. Ukoliko na toj radnoj stanici postoje vitalni podaci koje je Korisnik čuvao na rezervnim kopijama u skladu sa PR.BZB 12 Procedura za izradu rezervnih kopija (*backup-a*), tada nakon popravke radne stanice informatičar na poslovima tehničke podrške radi i povraćaj podataka. Ukoliko proces rada u kome Korisnik učestvuje ne dozvoljava prekid u radu, tada Administrator IKT UDK kreira Zahtev za zamenski računar koji će se dostaviti Korisniku, dok je njegova radna stanica na servisiranju. Informatičar na poslovima tehničke podrške instalira zamenski računar i prilagođava ga korisniku.

6.4.1.2. Prekid rada računarske mreže (više računara) ili servera

Aktivnost: Administrator IKT UDK procenjuje situaciju i zavisno od razloga prekida rada mreže ili servera, planira dalje aktivnosti. O novonastaloj situaciji, kao i planiranim aktivnostima obaveštava rukovodioca Odseka informacionih sistema i tehnologija, a on dalje po hijerarhiji navedena lica kao u tački 6.3.

Potrebni koraci:

- ukoliko prekid poslovnog procesa zahteva šalje cirkularne poruke putem eMails;
- ukoliko prekid poslovnog procesa zahteva šalje pisano obaveštenje ili
- ako nema nikakvih drugih mogućnosti to radi usmenim putem. Rukovodilac OJ koja je u direktnoj vezi sa incidentom je dužan da obavesti sve zaposlene svoje OJ o planiranim aktivnostima Administratora IKT i informatičara na tehničkim poslovima.

	IZDANJE / IZMENA	VAŽI OD	STRANA	PR.BZB 16
	1/0	01.12.2020.	7 od 9	

Administrator IKT ili rukovodilac Odseka informacionih sistema i tehnologija, angažuju odgovarajućeg vendedora i u najkraćem roku rade popravku. Ukoliko je došlo do gubitka podataka na serverima, tada se povraćaj podataka sprovodi u skladu sa PR.BZB 12 Procedura za izradu rezervnih kopija (backup-a). Dok su mreža i/ili serveri van funkcije, Korisnici u OJ koji koriste BIS Heliant evidentiraju podatke i medicinsku dokumentaciju u Word-u ili u papirnoj formi. Takođe, zaposleni na šalterima UDK evidentiraju u Word-u ili u papirnoj formi spisak pacijenta (identifikacioni podaci; dijagnoze; usluge koje su sprovedene i ostali relevantni podaci). Nakon osposobljavanja mreže i/ili servera, Administrator IKT, obaveštava nadležne rukovodioce OJ UDK a korisnici unose podatke (sa papira ili iz Word-a) u odgovarajući IS/BIS Heliant ili bazu podataka.

6.4.1.3 Prekid rada BIS Heliant u kome se generiše medicinska dokumentacija

Aktivnost: Administrator IKT UDK procenjuje situaciju i zavisno od razloga prekida rada mreže računara ili BIS Helianta planira dalje aktivnosti. Ukoliko je potrebno, a u skladu sa Ugovorom o saradnji i održavanju BIS Helianta, kontaktira odvlašćena lica. O prekidu poslovnog procesa i o planiranim aktivnostima, obaveštava rukovodioca Odseka informacionih sistema i tehnologija, a on dalje po hijerarhiji navedena lica kao u tački 6.3. postavljanjem odgovarajućeg obaveštenja na glavnu stranu sajta UDK:

- ukoliko prekid poslovnog procesa zahteva šalje cirkularne poruke putem eMaila;
- ukoliko prekid poslovnog procesa zahteva šalje pisano obaveštenje ili
- ako nema nikakvih drugih mogućnosti to radi usmenim putem. Rukovodilac OJ koja je u direktnoj vezi sa incidentom je dužan da obavesti sve zaposlene svoje OJ o planiranim aktivnostima Administratora IKT i informatičara na tehničkim poslovima.

Administrator IKT ili rukovodilac Odseka informacionih sistema i tehnologija, angažuju odgovarajućeg vendedora - Heliant i u najkraćem roku rade na njegovom osposobljavanju. Ukoliko je došlo do gubitka podataka IS/BIS Heliant koji su na serverima UDK, tada se povraćaj podataka sprovodi u skladu sa PR.BZB 12 Procedurom za izradu rezervnih kopija (backup-a). Dok je BIS van funkcije, Korisnici sve podatke i medicinsku dokumentaciju evidentiraju u Word-u ili u papirnoj formi. Takođe, zaposleni na šalterima UDK evidentiraju u Word-u ili u papirnoj formi spisak pacijenta (identifikacioni podaci; dijagnoze; usluge koje su sprovedene i ostali relevantni podaci).

Nakon osposobljavanja BIS Heliant, Administrator IKT, obaveštava nadležne rukovodioce OJ UDK, a korisnici unose podatke u BIS.

6.4.1.4 Prekid rada usled nestanka električne energije

Ukoliko je najavljen prekid električne energije, ili se planira prekid električne energije iz nekih drugih razloga (radovi unutar UDK) ili prekid nastane neplanirano, usled havarije (poplava; požar; zemljotres ili druge elementarne nepogode; kvar klima uređaja; itd), neophodno je da zaposleni ili odgovorno lice Odseka za održavanje objekta u najkraćem roku obaveste rukovodioca Odseka informacionih sistema i tehnologija i/ili administratora IKT.

A) Planiran nestanak električne energije u Odseku informacionih sistema i tehnologija ili u celom UDKu

Aktivnost: Planiran prekid u isporuci električne energije podrazumeva pravovremeno obaveštenje odgovornog lica – rukovodioca Odseka. Nakon dobijanja obaveštenja, Administrator IKT procenjuje potrebne aktivnosti, kao i vreme na koliko je potrebno isključiti servere u prostorijama Odseka. O planiranim aktivnostima obaveštava rukovodioca Odseka, a on dalje po hijerarhiji navedena lica kao u tački 6.3.

Potrebni koraci:

- ukoliko prekid poslovnog procesa zahteva šalje cirkularne poruke putem eMaila;
- ukoliko prekid poslovnog procesa zahteva šalje pisano obaveštenje ili

	IZDANJE / IZMENA	VAŽI OD	STRANA	PR.BZB 16
	1/0	01.12.2020.	8 od 9	

- ako nema nikakvih drugih mogućnosti to radi usmenim putem. Rukovodilac OJ koja je u direktnoj vezi sa incidentom je dužan da obavesti sve zaposlene svoje OJ o planiranim aktivnostima Administratora IKT i informatičara na tehničkim poslovima.

Ukoliko planirane aktivnosti to zahtevaju, Administrator IKT UDK isključuje servere u skladu sa PR.BZB 14 Procedura uključivanja i isključivanja servera. Dok su serveri isključeni, u prostorijama Odseka (u trajanju dužem od 60 minuta), zaposleni potrebne podatke beleže na papiru ili u Word-u ukoliko postoje radne jedinice sa sopstvenim napajanjem.

Po dolasku električne energije, administrator IKT uključuje servere u skladu sa PR.BZB 14 Procedura uključivanja i isključivanja servera, obaveštava rukovodioca Odseka, a on dalje po hijerarhiji navedena lica kao u tački 6.3. a korisnici unose podatke u odgovarajući IS/BIS nakon njegovog osposobljavanja.

B) Havarija ili neplaniran nestanak električne energije u Odseku informacionih sistema i tehnologija ili u celom UDK

Aktivnost: U slučaju neplaniranog isključenja električne energije ili havarije, Administrator IKT UDK što je brže moguće procenjuje situaciju i zavisno od trajanja nestanka električne energije ili obima havarije, planira dalje aktivnosti. O tome obaveštava najpre rukovodioca Odseka, a on dalje po hijerarhiji navedena lica kao u tački 6.3.

Potrebni koraci:

- ukoliko prekid poslovnog procesa zahteva šalje cirkularne poruke putem eMaila;
- ukoliko prekid poslovnog procesa zahteva šalje pisano obaveštenje ili
- ako nema nikakvih drugih mogućnosti to radi usmenim putem. Rukovodilac OJ koja je u direktnoj vezi sa incidentom je dužan da obavesti sve zaposlene svoje OJ o planiranim aktivnostima Administratora IKT i informatičara na tehničkim poslovima.

Za vreme dok su serveri isključeni u prostorijama Odseka informacionih sistema i tehnologija, u trajanju dužem od 60 minuta, Korisnici evidentiraju sve podatke i dokumentaciju, ukoliko je to moguće, u odgovarajućem IS, u Word-u ili u papirnoj formi Zaposleni na šalterima UDK podatke beleže u Word-u ili u papirnoj formi (identifikacioni podaci; dijagnoze; usluge koje su sprovedene i ostale relevantne podatke). Po dolasku električne energije ili posle saniranja havarije, kada je uspostavljena potrebna sigurnost i bezbednost prostora u kom se nalaze, u okviru Odseka i opreme u njoj, uključuje servere u skladu sa PR.BZB14 Procedurom uključivanja i isključivanja servera. Odmah zatim obaveštava rukovodioca Odseka, a on dalje po hijerarhiji navedena lica kao u tački 6.3. Obaveza korisnika je da što je moguće pre unesu podatke u odgovarajući IS/BIS nakon njegovog osposobljavanja.

6.4.2 Incidenti u vezi neovlašćenog pristupa, gubitka, izmene ili oticanja podatka

U slučaju neovlašćenog pristupa, odnosno ako dođe do provaljivanja u IKT sistem, gubitka, izmene ili oticanja podataka, obavezno se u dokumentovanoj formi (eFormi ili papiru) kao i usmeno obaveštava rukovodilac Odseka informacionih sistema i tehnologija, a on dalje po hijerarhiji navedena lica kao u tački 6.3. Ova imenovana lica će reagovati u skladu sa svojim pravima i obavezama i obavestiti potrebna tela i lica (RATEL i Poverenik za informacije od javnog značaja).

Ukoliko je poznato ko je „napadač“ i ako je on prepoznat kao korisnik IKT sistema, tada se u najkraćem mogućem roku menjaju svi kredencijali i inicira disciplinski postupak.

6.4.3 Incidenti u vezi provaljivanja u IKT sistem

Ako je incident prepoznat kao provala u IKT sistem UDK i to zbog kršenja mera zaštite, i na taj način ostvaren pristup koji omogućava neovlašćen uticaj na rad IKT sistema, tada je neophodno da se u dokumentovanoj formi (eFormi ili papiru) kao i usmeno obavesti rukovodilac Odseka informacionih sistema i tehnologija, a on dalje po hijerarhiji obaveštava navedena lica kao u tački

	IZDANJE / IZMENA	VAŽI OD	STRANA	PR.BZB 16
	1/0	01.12.2020.	9 od 9	

6.3. Ova imenovana lica će reagovati u skladu sa svojim pravima i obavezama i obavestiti potrebna tela i lica (RATEL i Poverenik za informacije od javnog značaja).

6.5 Aktivnosti nakon incidenta

Posle saniranja i rešavanja incidentne situacije treba izvršiti analizu pre, za vreme i neposredno posle incidenta. Iz svake incidentne situacije treba izvući faktore rizika i iskoristiti situaciju za poboljšavanje i unapređenje IKT sistema. Ovo je važno zbog budućih mera i Planova u vezi mogućih ponovljenih pretnji.

Nakon incidenta, Lice za bezbednost podataka, Lice za zaštitu podataka o ličnosti, rukovodilac Odseka informacionih sistema i tehnologija, administrator IKTa UDK timski razmatraju uzroke i posledice incidenta.

- Šta se tačno dogodilo i u koje vreme?
- Da li su odgovorna lica adekvatno i odgovorno rešila zadatak i nosili se s incidentom?
- Da li su procedure bile jasne i dobro dokumentovane i jesu li bile odgovarajuće?
- Koje je informacije trebalo doznati ranije?
- Jesu li preduzeti svi koraci ili akcije koje mogu ubrzati oporavak?
- Koje je mere potrebno preduzeti za sprečavanje sličnih incidenata u budućnosti?
- Koji su dodatni resursi i alati potrebni za otkrivanje, analizu i ublažavanje posledica budućih incidenata?
- Što bi trebalo zaposleni i menadžment da učine drugačije idući put kada se dogodi sličan incident?

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).