

	UNIVERZITETSKA DEČJA KLINIKA, BEOGRAD TIRŠOVA 10			PR.BZB 10
	IZDANJE/IZMENA 1/0	VAŽI OD 01.12.2020.	STRANA 1 od 6	

PROCEDURA ZA BEZBEDNO UPRAVLJANJE PRENOSNIM NOSAČIMA PODATAKA

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 10
	1/0	01.12.2020.	2 od 6	

S a d r Ź 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 Čuvanje poslovnih ili internih podataka na prenosnim nosačima podataka	4
	6.2 Iznošenje poslovnih ili internih podataka na prenosnim nosačima podataka	5
	6.3 Čuvanje i iznošenje javnih podataka na prenosnim nosačima podataka	6
7	PRAVNI OSNOV	6

	IZDANJE / IZMENA	VAŽI OD	STRANA	PR.BZB 10
	1/0	01.12.2020.	3 od 6	

1 SVRHA

Svrha procedure je da precizira način upravljanja prenosnim nosačima podataka koje UDK koristi u svojim poslovnim aktivnostima, s ciljem da se unapredi bezbednost podataka.

2 PREDMET I PODRUČJE PRIMENE

Ovom procedurom utvrđuju se aktivnosti, nosioci aktivnosti i odgovornosti pri upravljanju prenosnim nosačima podataka. Pravilnom primenom utvrđenog postupka, svodi na minimum potencijalnu izloženost šteti koja može nastati usled nedozvoljenog pristupa podacima.

Primenjuje se na sve nosače podataka na kojima se nalaze poslovni ili interni podaci UDK.

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 11 Procedura za bezbedno rashodovanje nosača podataka;
- PR.BZB 12 Procedura za izradu rezervnih kopija (*backup-a*);
- Ugovori s vendorima.

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 - 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;

organizacionu strukturu putem koje se upravlja IKT sistemom;

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

Radna stanica - 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;

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

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

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

	IZDANJE / IZMENA	VAŽI OD	STRANA	PR.BZB 10
	1/0	01.12.2020.	4 od 6	

tajnost, integritet, raspoloživost, autentičnost i neporecivost tih podataka, da bi IKT sistem funkcionisao kako je predviđeno, kada je predviđeno i pod kontrolom ovlašćenih lica;

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

Poslovni podaci su podaci na koje se odnosi Zakon o zaštiti poslovne tajne („Sl.glasnik RS", br. 72/2011);

Interni podaci su podaci medicinske dokumentacije pacijenata UDK kao i podaci na koje se odnosi Zakon o zaštiti podataka o ličnosti („Sl. glasnik RS", br. 87/2018);

Anonimizacija podataka predstavlja postupak konverzije podataka o ličnosti u oblik koji onemogućava identifikaciju ličnosti;

Anonimizirani podaci su podaci o ličnosti na osnovu kojih se ne može identifikovati o kojoj osobi je reč;

Agregarni podaci su podaci koji nisu izvorni (podaci na kojima je sprovedena obrada podataka) i iz kojih se ne može identifikovati osoba/ličnost (npr. sumarne tabele, grafikoni).

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.

Vendori ili drugi saradnici UDK su dužni da se ponašaju u skladu sa ugovorom i u skladu sa njim snose odgovornost.

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

Za kontrolu sprovođenja procedure odgovorni su odgovarajući rukovodioci organizacionih jedinica.

6 OPIS PROCEDURE

Na prenosnim nosačima podataka mogu se nalaziti samo određeni tipovi podataka. Poverljivi podaci se ne smeju nalaziti na prenosnim nosačima podataka, već samo poslovni, interni ili javni podaci.

Poslovni i interni podaci se mogu nalaziti na prenosnim nosačima podataka samo ukoliko su namenjeni Korisnicima tj. zaposlenima UDK, koji svojim korisničkim naložima imaju pristup takvim podacima. Potrebno je voditi evidenciju o prenosu ovog tipa podataka. Odgovorna lica za prenos su rukovodioci odgovarajućih organizacionih jedinica koji koordiniraju i nadgledaju ovaj proces.

6.1 Čuvanje poslovnih ili internih podataka na prenosnim nosačima podataka

Poslovni i interni podaci UDK se čuvaju na serverima ili radnim stanicama. Odgovornost za čuvanje ovih i svih podataka na serverima je na Administratoru IKT. Pristup serverima je strogo kontrolisan, jer se pristupom serverima pristupa i svim podacima. Sem administratora pristup je omogućen i rukovodiocu Odseka za informacione sisteme i tehnologije.

Poslovni i interni podaci se mogu nalaziti i čuvati na posebnoj radnoj stanici mimo servera. Svaki Korisnik, koji na radnoj stanici čuva poslovne ili interne podatke je lično odgovoran za njih. Razlog za čuvanje podataka na ovakav način može biti specifičnost poslovnih procesa, ali je poželjno da radna stanica na kojoj se nalaze ovi podaci bude mimo mreže računara iz bezbednosnih razloga. Za bezbednost ovih radnih stanica odgovoran je Korisnik, odnosno zaposleni koji radi na ovoj radnoj stanici. Zato je potrebno da preduzme sledeće korake:

- 1) da napravi više od jedne kopije podataka na prenosnim nosačima podataka;
- 2) kopije podataka treba čuvati na posebnim medijumima kako bi se smanjio rizik od slučajnog oštećenja ili eventualnog gubitka podataka;

	IZDANJE / IZMENA	VAŽI OD	STRANA	PR.BZB 10
	1/0	01.12.2020.	5 od 6	

- 3) potrebna su najmanje dva medijuma (odnosno lokacija za skladištenje, a preporuka je da to bude više;
- 4) poželjno je da lokacije na kojima se čuvaju medijumi sa podacima budu različite (misli se na različite lokacije u okviru UDK) kako bi podaci bili sigurni u slučaju požara ili sličnih nepogoda;
- 5) potrebno je napraviti evidenciju / registar ovih medijuma, za koje su odgovorni rukovodioci OJ i Korisnik;
- 6) pri odabiru lokacija na kojima će se čuvati ovi medijumi, treba voditi računa o tome da to budu bezbedna i zaštićena mesta, u skladu sa preporukama proizvođača;
- 7) takođe, potrebno je kontrolisati vreme tj. voditi računa o roku koji garantuje ispravnost medijuma - prenosnog nosača podataka, u skladu sa preporukama proizvođača;
- 8) kada je blizu isticanje roka trajanja nosača podataka, potrebno je podatke prebaciti na novi medijum da ne bi postali nečitljivi;
- 9) svaki neispravan ili dotrajaao nosač podataka na kom se nalaze poslovni ili interni podaci, treba uništiti u skladu sa PR.BZB 11 Procedura za bezbedno rashodovanja nosača podataka.

Svaki korisnik može podneti zahtev Odseku informacionih sistema i tehnologija, ukoliko smatra da podaci koji se nalaze na njegovoj radnoj stanici treba da se skladište na serverima UDK (obrazac O.BZB.01 Zahtev za uslugu Odseka)

Eventualnu upotrebu privatnih nosača podataka u svrhu čuvanja poslovnih ili internih podataka odobrava i evidentira rukovodilac odgovarajuće OJ.

U planu je nabavka službenih mobilnih nosača podataka (USB, eksterne memorije, diskovi) koji će imati implementiranu zaštitu.

6.2 Iznošenje poslovnih ili internih podataka na prenosnim nosačima podataka

Svako iznošenje internih ili poslovnih podataka podleže propisima o zaštiti podataka o ličnosti i o poslovnoj tajni. Zato, iznošenje ovih podataka fizički, van zgrade UDK je moguće samo za potrebe obavljanja redovnih radnih zadataka (svaki zaposleni je odgovoran na osnovu potpisane Izjave o poverljivosti korišćenja resursa i IKT podataka UDK).

Ukoliko je neophodno izneti poslovne ili interne podatke na bilo kom medijumu, od strane Korisnika na prenosnim nosačima podataka, potrebno je pridržavati se sledećih uputstava:

- 1) Kada god je moguće Korisnik za sve medijume koji se iznose iz UDK traži odobrenje rukovodioca odgovarajuće OJ;
- 2) Davanjem saglasnosti rukovodilac OJ preuzima odgovornost i donosi odluku o tome da li treba pratiti prenos informacija na takve medijume;
- 3) rukovodilac odgovarajuće OJ, ukoliko je to potrebno vodi evidenciju o prenosnom nosaču podataka, njegovom sadržaju i Korisniku. Ovo je neophodno kako bi bilo moguće pratiti put kretanja podataka u slučaju potrebe;
- 4) korisnik je obavezan da sve prenosne nosače podataka čuva na bezbednom i zaštićenom mestu, u skladu sa preporukama proizvođača;
- 5) sadržaj svakog medijuma treba nepovratno izbrisati kada više nije potreban. Brisanje podataka vrši Administrator IKT ili informatičar na poslovima tehničke podrške pomoću namenskog softvera;
- 6) sve neupotrebljive ili oštećene prenosne nosače podataka na kojima se nalaze poslovni ili interni podaci, treba uništiti u skladu sa PR.BZB 11 Procedura za bezbedno rashodovanje nosača podataka.

Ukoliko se iznošenje podataka vrši za potrebe trećih lica, odnosno trećim licima se daje prenosni nosač podataka na kome se oni nalaze, potrebno je da:

	IZDANJE / IZMENA	VAŽI OD	STRANA	PR.BZB 10
	1/0	01.12.2020.	6 od 6	

- UDK ima ugovor sa trećim licima koji u sebi ima klauzulu o poverljivosti podataka kao i potpisanu izjavu o poverljivosti podataka - eksternu;
- podaci budu agregarni ili bar anonimizirani. Ukoliko depersonalizacija onemogućava traženu analizu podataka sa medicinskog aspekta, onda treba nekom drugom metodom zaštititi podatke i dostaviti ih na takav način (npr. šifrovano otvaranje dokumenta ili kriptazaštita). U slučaju da Korisnik ne može samostalno da obezbedi zaštitu podataka, može se obratiti Administratoru IKT ili rukovodiocu Odseka inormacionih sistema i tehnologija.

6.3 Čuvanje i iznošenje javnih podataka na prenosnim nosačima podataka

Čuvanje i iznošenje javnih podataka je dozvoljeno svim zaposlenima UDK. Za čuvanje ove vrste podataka ako se nalaze na serverima Odseka zadužen je Administrator IKT. Za čuvanje javnih podataka koji se nalaze na radnim stanicama, mobilnim uređajima ili prenosnim nosačima podataka zadužen je Korisnik.

Čuvanje podataka se razlikuje u skladu sa tipom podataka koji se čuvaju. Odgovornost čuvanja podataka podrazumeva i odgovornost rashodovanja nosača podataka. Rashodovanje nosača podataka se vrši u skladu sa PR.BZB 11 Procedura za bezbedno rashodovanje nosača podataka

Svaku eventualnu nepravilnost pri rashodovanju i odlaganju nosača podataka neophodno je prijaviti **Licu zaduženom za bezbednost podataka** koje će na osnovu svojih ovlašćenja obavestiti druga nadležna lica i odgovarajuću agenciju (Lice za zaštitu podataka o ličnosti ili RATEL).

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).