

	UNIVERZITETSKA DEČJA KLINIKA, BEOGRAD TIRŠOVA 10			PR.BZB 17
	IZDANJE/IZMENA 1/0	VAŽI OD 01.12.2020.	STRANA 1 od 8	

PROCEDURA O BEZBEDNOSTI RAZMENE ePORUKA (eMail-a)

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 17
	1/0	01.12.2020.	2 od 8	

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 Dostupnost službene elektronske pošte	4
	6.2 Odgovornost Korisnika.....	5
	6.3 Upotreba službene elektronske pošte	5
	6.4 Slanje internih i/ili poslovnih podataka	6
	6.5 Slanje poruka svim ili većem broju korisnika IKT sistema (cirkularni mejl)	7
	6.6 Poštovanje prava privatnosti	7
	6.7 Brisanje elektronskih poruka	7
7	PRAVNI OSNOV	8

	IZDANJE / IZMENA	VAŽI OD	STRANA	PR.BZB 17
	1/0	01.12.2020.	3 od 8	

1 SVRHA

Svrha procedure je da definiše poslovne aktivnosti u procesu nastanka, razmene i čuvanja elektronskih poruka, s ciljem da se unapredi bezbednost ovakve poslovne komunikacije.

2 PREDMET I PODRUČJE PRIMENE

Ovom procedurom utvrđuju se aktivnosti, nosioci aktivnosti i odgovornosti prilikom razmene elektronskih poruka u cilju zaštite informacija i informacionih dobara UDK od zloupotrebe ili nepažnjom izazvane štete.

Primenjuje se na sve zaposlene koji koriste radne stanice IKT sistema i mobilne uređaje UDK za potrebe elektronske komunikacije.

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 02 Procedurom o instalaciji i konfiguraciji sistema;
- PR.BZB 05 Procedurom o pravima pristupa IKT sistemu.

4 DEFINICIJE I SKRAĆENICE

UDK - Univerzitetska dečja klinika;

OJ - Organizaciona jedinica UDK;

Odsek za informacione sisteme i tehnologije – 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;
4. organizacionu strukturu putem koje se upravlja IKT sistemom.

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;

Administrator IKT - zaposleni Odseka informacionih sistema i tehnologija kome je dozvoljeno administriranje IKT i/ili IS sistema.

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

Mobilni uređaji IKT – svi pokretni uređaji: prenosivi računar, tablet, SMART mobilni telefon, PDA, i sl. koji se povezuje sa mrežom UDKa

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

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

	IZDANJE / IZMENA	VAŽI OD	STRANA	PR.BZB 17
	1/0	01.12.2020.	4 od 8	

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

Usluga Odseka informacionih sistema i tehnologija - stručna usluga koju sprovodi jedan ili više zaposlenih iz Odseka informacionih sistema i tehnologija.

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;

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

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 osoba čiji se podaci obrađuju ili čuvaju;

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).

ePošta – elektronska poruka eMail.

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 podataka – eksterna, 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 je ustanova koja ima implementiranu savremenu IKT opremu u obimu koji je u skladu sa mogućnostima. Menadžment UDK u kontinuitetu razvija primenu novih tehnologija kroz savremene vidove poslovne komunikacije, kao što su: upotreba internet tehnologija, elektronska pošta, video-konferencije, webinar, portal za učenje na daljinu KME itd. U sklopu ovih aktivnosti se neprekidno obavlja poslovna komunikacija elektronskim putem, putem različitih pristupa i aplikacija.

6.1 Dostupnost službene elektronske pošte

Osnovno pravo Korisnika koji ima potrebu za poslovnom komunikacijom, u skladu sa svojim opisom radnog mesta je da može dobiti službenu eMail adresu. Međutim, to je moguće isključivo ukoliko je potpisao Izjavu o obavezi bezbednog korišćenja resursa IKT sistema UDK.

Zahtev za dodelu, izmenu, blokiranje, deblokiranje ili ukidanje eMail adrese Korisnika, kao i dodeljivanje njegovih kredencijala za pristup ePošti, vrši se u skladu sa PR.BZB 05 Procedurom o pravima pristupa IKT sistemu.

Podešavanja parametara za pristup elektronskoj pošti zaposlenog na radnoj stanici koju koristi, vrši Administrator IKT UDK ili informatičar za podršku u Odseku informacionih sistema i tehnologija, u skladu sa PR.BZB 02 Procedurom o instalaciji i konfiguraciji sistema.

Pristup elektronskoj pošti UDK Korisnik može se ostvariti na dva načina:

1. korišćenjem interneta preko <https://webmail.udk.bg.ac.rs/webmail>).

	IZDANJE / IZMENA	VAŽI OD	STRANA	PR.BZB 17
	1/0	01.12.2020.	5 od 8	

Pročitana, započeta ili poslata ePošta pristupom web mejla ostaje dostupna zaposlenom na odgovarajućem serveru Odseka nformacionih sistema i tehnologija. Korisnik može sačuvati svoju ePoštu samostalno na svojoj radnoj stanici, ali ona ostaje na mejl serveru UDK.

2. korišćenjem Outlook aplikacije na radnoj stanici, računaru;

Iako se u malom broju koristi ova aplikacija, postoji određen manji broj korisnika koji je zahtevao Outlook. Stoga je aktivan IMAP. Ovim korisnicima je instaliran klijent i uglavnom koriste za čitanje službene pošte na svom telefonu.

Pristup i slanje elektronske pošte je enkriptovano, zahteva autentikaciju i konfiguraciju zasebnih mail klijenata na desktop računarima i mobilnim telefonima.

U tom slučaju pročitana, započeta ili poslata elektronska pošta ostaje dostupna zaposlenom isključivo na njegovoj radnoj stanici.

6.2 Odgovornost Korisnika

- Službenu eMail adresu, treba koristiti u skladu sa namenom, odnosno u poslovne svrhe u skladu sa radnim zaduženjima;
- svaki Korisnik lično je odgovoran za sadržaj, arhiviranje i brisanje elektronskih poruka koje šalje putem svoje službene eMail adrese;
- Korisnik je u obavezi da čuva integritet - tajnost lozinke, odnosno lično je odgovoran za svoje kredencije. Ne sme ih otkrivati drugim osobama, kako treće lice ne bi zloupotrebilo njegove eMail adresu i sa nje slalo mejlove u ime Korisnika, čitao poštu ili pak distribuirao Korisnikovu ePoštu bez njegovog znanja. Ukoliko posumnja da je njegova lozinka kompromitovana na bilo koji način, Korisnik treba odmah da obavesti Administratora IKT ili rukovodioca Odseka informacionih sistema i tehnologija, radi njene izmene. Otkrivanje lozinke drugoj osobi povlači sa sobom odgovornost Korisnika za goren navedene i druge aktivnosti koje ta osoba može preduzeti korišćenjem njegove lozinke. U tim slučajevima odgovornost je isključivo na Korisniku;
- Takođe, zabranjeno je slanje poverljivih podataka (kredencijala i lozinki) putem elektronske pošte;
- Zabranjeno je ustupanje eMail adresa trećim licima, osim ukoliko ne postoji ugovor između UDK i trećih lica koji sadrži klauzulu o poverljivosti podataka.

6.3 Upotreba službene elektronske pošte

Svaka poruka elektronske pošte kreirana od strane Korisnika je autorska, odnosno pripada osobi koja je poslala. Takođe, prilozi koji se šalju uz elektronske poruke mogu sadržati autorski zaštićene informacije. S obzirom na ove karakteristike, svaki ovaj element ePošte generiše posebne obaveze i prava.

Takođe, razmenom službene elektronske pošte, korisnici moraju znati da vode komunikaciju ne samo u svoje ime, već da predstavljaju i UDK. Odnosno, imaju dvostruku odgovornost: ličnu i kolektivnu.

Pri slanju elektronske pošte koristeći službenu eMail adresu, Korisnik mora da se pridržava sledećeg:

- Poslovna tj. Službena elektronska pošta UDK se koristi samo radi obavljanja poslova za potrebe UDK, odnosno za poslovne i druge slične potrebe vezano za poslovne aktivnosti UDK (naučne, istraživačke ili nastavne potrebe). Privatne poruke su dozvoljene, ali u umerenoj količini, samo ukoliko ne ometaju poslovnu komunikaciju i ukoliko se pridržavaju pravila pristojne komunikacije na internetu;
- svaka napisana ePoruka se tretira kao eDokument, pa stoga podleže propisima o autorskom pravu i intelektualnom vlasništvu. Poruke koje su poslate lično jednom Korisniku, taj Korisnik nema pravo da prosleđuje dalje bez dozvole pošiljaoca;

	IZDANJE / IZMENA	VAŽI OD	STRANA	PR.BZB 17
	1/0	01.12.2020.	6 od 8	

- pridržavajući se pravila pristojne komunikacije na internetu, korisnici službeni eMail adresu ne smeju koristiti za slanje uvredljivih, rasnih ili na bilo koji drugi način omalovažavajućih poruka, nije dozvoljeno seksualno ili bilo kakvo drugo uznemiravanje;
- takođe, nije dozvoljeno slanje lančanih tj. cirkularnih poruka kojima se opterećuju mrežni resursi;
- sve ePoruke automatski kontroliše aplikacija za zaštitu elektronske pošte (eMail sistem). Ako mejl sadrži virus, kao i nedozvoljene i sumnjive elemente, neće biti isporučena. O postupku sa sumnjivom porukom odlučuje Administrator IKT na osnovu svojih prava i obaveza;
- mejlove koji su deo poslovnog procesa treba arhivirati i čuvati propisani vremenski period, odnosno prema njima treba imati odnos kao i prema dokumentima u papiru u skladu sa internim dogovorom ili prema Registratorskoj listi ako je definisan status ePoruka (Zakon o med.dokumentaciji ravnopravno tretira elektronski i papirni dokument);
- korisnicima nije dopušteno da bez saglasnosti drugog Korisnika pregledaju, čitaju i prosleđuju njegovu eMail poštu;
- korisnik treba da vodi računa o ispravnom adresiranju elektronske pošte, koji podrazumeva popunjena tzv. obavezna polja. Na taj način razmena poruka je kvalitetnija, a broj vraćenih poruka se svodi na minimum (obavezno popuniti polje TEMA/**subject** engl. kako poruka ne bi bila vraćena ili poslata u Nepoželjne poruke/**Spam** engl. Takođe, poruka mora imati potpis pošiljaoca, sa punim zvanjem i pozicijom, kao i kontakt podatke).

6.4 Slanje internih ili poslovnih podataka

Slanje internih ili poslovnih podataka putem poruka elektronske pošte podleže Zakonu o zaštiti podataka o ličnosti ili poslovnoj tajni. Otuda proizilazi da Korisnik može slati ove podatke samo u slučaju da ima :

- saglasnost neposrednog rukovodioca i
- da to radi isključivo sa službene eMail adrese.

Interne ili poslovne podatke putem poruka elektronske pošte, Korisnik može uputiti na:

- službeni eMail adresu primaoca koji je zaposlen u UDK;
- službeni eMail adresu primaocu u mreži zdravstvenih ustanova;
- službeni eMail adresu nadležnih državnih organa;
- na službeni eMail vendora, koji je prethodno potpisao Izjavu o poverljivosti (eksternu) ili Ugovor u kome je definisan aspekt poverljivosti informacija/podataka;
- na službeni mail službenih, ovlašćenih lica ili ustanova, kada je neophodno dostaviti podatke u procesu digitalizacije medicinske dokumentacije / podataka (u početnoj fazi ovog procesa, podaci se dostavljaju sa službenog maila na službeni mail, i na ovaj način bezbednost razmene podataka je dvosmerna, odnosno druga ustanova preuzima deo odgovornosti – bezbednost IKT mreže date ustanove).

Anonimizacija podataka se primenjuje kad god je to moguće i odgovornost snosi Korisnik koji dostavlja podatke. Ukoliko nije primenio anonimizaciju potrebno je da podaci imaju zaštićenu formu (npr. razmena podataka za izradu statističkih izveštaja, kada podatak pacijenta podrazumeva samo podatke o bolesti, a ne identifikacione podatke o pacijentu).

Kada je potrebno dostaviti podatke o pacijentu u celosti (identifikacione podatke zajedno sa podacima o bolesti, odnosno kompletan eKarton ili elstoriju bolesti), tada je potrebno sprovoditi neke od drugih metoda zaštite (npr. šifrovano otvaranje dokumenta koji je u prilogu elektronske pošte) ili koristiti razmenu podataka sa kriptozastitom. U takvim situacijama se korisnici mogu obratiti za pomoć Administratoru IKT ili nekom od zaposlenih Odseka informacionih sistema i tehnologija.

	IZDANJE / IZMENA	VAŽI OD	STRANA	PR.BZB 17
	1/0	01.12.2020.	7 od 8	

6.5 Slanje poruka svima ili većem broju korisnika IKT sistema UDK (cirkularni mejl)

Cirkularni mejlovi su specifični jer se dostavljaju svim korisnicima u isto vreme i mogu negativno uticati na protok mreže i na rad servera. Zato, upotreba ovog tipa mejla ima ograničenja.

Direktor UDK, pomoćnici direktora, rukovodioci OJ ili samostalnih službi mogu poslati cirkularni eMail sa obaveštenjem koje se tiče svih zaposlenih.

Odgovorna lica Odseka informacionih sistema i tehnologija, kao i Lica za zaštitu podataka o ličnosti i Lica zaduženo za bezbednost IKTa UDK, mogu poslati cirkularni mejl, s nalogom za postupanje u situaciji koja ugrožava bezbednost IKT UDK ili predstavlja obaveštenje o novonastalim merama povodom bezbednosti IKTa UDK, svim Korisnicima UDK.

Ostali Korisnici mogu da pošalju cirkularni eMejl samo uz prethodno odobrenje rukovodioca OJ.

6.6 Poštovanje prava privatnosti

Bez obzira što je službena mejl adresa namenjena komunikaciji u poslovne svrhe, službena mejl adresa se mora tretirati kao deo privatnosti svakog Korisnika tj. Zaposlenog kome je dodeljena. UDK poštuje prava svojih Korisnika u sistemu IKT uključujući i pravo privatnosti u procesu slanja i primanja ePošte na sledeće načine:

- Administrator IKT UDK ne sme pregledati sadržaj elektronske pošte drugih Korisnika iz lične radoznalosti, niti dopustiti uvid u sadržaj elektronske pošte trećim licima koje za to nemaju potrebna ovlašćenja Korisnika;
- Uz saglasnost Korisnika i samo u slučaju rešavanja problema komunikacije, Administrator IKT može imati pravo na uvid u sadržaj poruka elektronske pošte pojedinog Korisnika;
- UDK zadržava pravo filtriranja poruka s namerom da se zaštiti bezbednost IKT sistema UDK, odnosno stopira nepoželjna ePošta (tzv. Spam);
- U posebnim slučajevima, kada postoji opravdana sumnja u kršenje odredbi ove procedure, radi zaštite elektronske pošte i po zahtevu ovlašćenih državnih ustanova ili Direktora UDK, a uz saglasnost Lica zaduženog za zaštitu podataka o ličnosti, UDK može dopustiti povremeno presretanje i pregledanje sadržaja elektronske pošte svojih Korisnika.

Pored mera zaštite koje UDK sprovodi, a zbog prethodno navedenih razloga, UDK ne može u potpunosti garantovati privatnost sadržaja ePošte. Stoga, Korisnici jednim delom preuzimaju rizik u eKomunikaciji.

6.7 Brisanje elektronskih poruka

Korisnik je lično odgovoran za arhiviranje i brisanje elektronskih poruka svog službenog mejla. Odgovornost se ogleda i u tome da je potrebno povremeno čistiti „sanduče“. To podrazumeva da Korisnik treba da obriše poruke koje više nisu bitne za poslovne potrebe. Takođe, Korisnik treba da arhivira poslovne poruke koje su važne, ali nisu trenutno aktuelne. Dinamiku održavanja „sandučeta“ definiše sam Korisnik.

Ukoliko su pokrenute neke istražne aktivnosti (koje mogu biti izazvane mogućim bezbednosnim incidentom), sve poruke elektronske pošte relevantne za tu istražnu aktivnost neće biti brisane do izričite naredbe rukovodstva UDK.

Ove istražne aktivnosti mogu biti inicirane od strane:

- rukovodstva UDK;
- Lica zaduženog za bezbednost podataka IKT UDK;
- Lica zaduženog za zaštitu podataka o ličnosti ili
- od strane ovlašćenih državnih ustanova.

	IZDANJE / IZMENA	VAŽI OD	STRANA	PR.BZB 17
	1/0	01.12.2020.	8 od 8	

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).