PROCEDURA ZA VPN PRISTUP
(Virtual Private Network)

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 način funkcionisanja poslovnih procesa koji se obavljaju „na daljinu“ odnosno sve daljinske pristupe IKT sistemu UDK s ciljem povećanja bezbednosti podataka.

2 PREDMET I PODRUČJE PRIMENE

Ovom procedurom utvrđuju se aktivnosti, nosioci aktivnosti i odgovornosti prilikom omogućavanja obavljanja poslova zaposlenih u UDK i saradnika koji koriste fizički udaljene računare ili mobilne uređaje za bezbedno povezivanje na mrežu UDK kao i način pristupa mreži UDK sa udaljenih lokacija.

Primenjuje se za daljinske pristupe IKT sistemu UDK.

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 02 Procedura o instalaciji i konfiguraciji sistema;
- PR.BZB 03 Procedura pristupa mreži i mrežnim uređajima;
- PR.BZB 05 Procedura o pravima pristupa IKT sistemu;
- Ugovorima između Vendora i UDK.

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;
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 BIS sistema;

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;

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

VPN *(Virtual Private Network)* pristup - sigurna kriptovana internet veza koja fizički udaljenom računaru omogućava pristup mreži UDK pa samim tim i IKT sistemu i IS sistemima UDK, kao da se računar nalazi u UDK;

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

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.

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 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 i rukovodioci organizacionih jedinica.

6 OPIS PROCEDURE

VPN pristup BIS Heliantu ili bilo kom samostalnom IS koji je implementiran u UDK je dozvoljen isključivo za potrebe obavljanja radnih zadataka. VPN pristup BIS Heliantu mogu imati sledeći korisnici IKT sistema:

1. korisnici sa radne stanice koji su u vlasništvu UDK;
2. zaposleni radnici vendora koji održava informacioni sistem UDK koji koriste radne stanice u vlasništvu vendora;
3. spoljni saradnici na osnovu ugovora kao i Vendori.

VPN konekcija može biti uspostavljena i između UDK i određenih državnih institucija sa kojima UDK sarađuje ili ima zakonsku obavezu dostavljanja izveštaja, podataka i sl.

6.1 Radne stanice u vlasništvu UDK

Radna stanica koja ima VPN pristup, mora da bude konfigurisana u skladu sa PR.BZB 02 Procedura o instalaciji i konfiguraciji sistema. Korisnik koji traži takvu vrstu konekcije - VPN pristup mora da obezbedi pravo pristupa mreži u skladu sa procedurom PR.BZB 05 Procedura o pravima pristupa IKT sistemu.

Korisnik podnosi rukovodiocu Odseka informacionih sistema i tehnologija zahtev za omogućavanje VPN pristupa IS UDK sa daljine, preko servera UDK.

Zahtev treba da bude potpisan od strane Korisnika i njegovog neposrednog rukovodioca i treba da sadrži sledeće informacije:

1. obrazloženje poslovne potrebe za rad na daljinu;
2. garancija tj. potvrda Korisnika da će koristiti rad na daljinu isključivo za potrebe obavljanja radnih zadataka;
3. potvrda da će Korisnik sa takvim pristupom IKT sistemu UDK, isključiti radnu stanicu sa VPN veze kada je:
   - ne koristi, odnosno završi poslove koji se od njega traže,
   - ako se koristi za druge potrebe za koje nije potreban pristup mreži UDK (npr. pretraživanje interneta ili eMail pošta);

4. potvrda da Korisnik na radnoj stanici neće čuvati fajlove koji sadrže poslovne i interne podatke UDK;
5. garanciju Korisnika da će radnu stanicu na kojoj će raditi na daljinu smestiti u bezbedan prostor (zasebna soba, položaj displeja takav da se onemogući posmatranje od strane neovlašćenih osoba i slično);
6. potvrdu da će se Korisnik ponašati u skladu sa pravnim aktima UDK.

Odgovorno lice Odseka razmatra zahtev i ukoliko ga odobri, Administrator IKT u saradnji sa vendorom za mrežu, sprovodi proveru usklađenosti radne stanice sa bezbednosnim merama, proveru tehničkih mogućnosti uspostavljanja VPN veze i upoznaje Korisnika sa bezbednosnim rizicima.

Ukoliko postoje tehničke mogućnosti, vendor za mrežu i Administrator IKT uspostavljaju VPN vezu koja je zaštićena korišćenjem kriptografskih algoritama (Sophos antivirus).

Ukoliko radna stanica nije usklađena sa bezbednosnim merama i ne postoje tehničke mogućnosti za realizaciju VPN veze, Odsek informacionih sistema i tehnologija o tome informiše Korisnika i Lice za bezbednost podataka. Unosi u evidenciju pristupa razloge i evidentira zahtev Korisnika.

Evidenciju pristupa VPN korisnika vodi Administrator IKT UDK.

6.2 Radne stanice Vendora koji održava IS, BIS i servere

Ukoliko je radna stanica za koju se traži VPN pristup u vlasništvu vendora koji održava BIS i servere, tada se VPN pristup definiše ugovorom u kome se navodi da vendor ima sopstveni Akt o bezbednosti informaciono-komunikacionog sistema i postupa po njemu tokom svog procesa rada. Odgovornost je na strani vendora.

6.3 VPN konekcija UDK sa državnim institucijama

VPN konekcija može biti uspostavljena između UDK i državnih institucija (npr. Ministarstvo zdravlja, IZIS, RFZO, Trezor Narodne banke, Institut za transfuziju krvi, Institut Batut i sl.) i tada je informaciona bezbednost VPN pristupa u ingerenciji imenovane državne institucije.

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).