Klinički bolnički centar Osijek
Ravnateljstvo
Ur. broj: R1-17715/2018.
Osijek, 26.11.2018.

Na temelju članka 21. Statuta Kliničkog bolničkog centra Osijek, donosi se

Sigurnosna politika informacijskog sustava Kliničkog bolničkog centra Osijek

1. Svrha

Sigurnosna politika informacijskog sustava (u daljnjem tekstu: Sigurnosna politika) Kliničkog bolničkog centra Osijek predstavlja najvišu razinu dokumentacije vezane za sigurnost Informacijskog sustava KBC Osijek, opća pravila kojima se uređuju pitanja povjerljivosti, cjelovitosti i raspoloživosti podataka primjenom propisanih mjera i standarda informacijske sigurnosti kao i organizacijska podrška za poslove planiranja, provedbe, provjere i dorade mjera i standarda.
Informacijski sustav je računalni, komunikacijski ili drugi elektronički sustav u kojem se podaci obrađuju, pohranjuju ili prenose tako da budu dostupni i uporabljivi za korisnike informacijskog sustava, a koji obuhvaća tehničku infrastrukturu, organizaciju, osobe i postupke kojima se podaci obrađuju, pohranjuju ili prenose.
Pravila rada i ponašanja koja definira Sigurnosna politika vrijede prvenstveno za:

- Svu računalnu opremu koja se nalazi u prostorima bolnice
- Administratore informacijskih sustava i djelatnike Službe za informatiku
- Korisnike, među koje spadaju: zaposlenici, vanjski suradnici, specijalizanti iz suradnih KBC Osijek
- Vanjske tvrtke koje po ugovoru rade na održavanju opreme ili softvera

2. Organizacija i načela upravljanja sigurnošću

Sigurnosnom politikom informacijskog sustava se točno definira razdioba poslovnih zaduženja te odgovornost za upravljanje procesima informacijskog sustava KBC Osijek. Isto se postiže kroz

raspodjelu zaduženja, obrazovanje korisnika te preko stručnih tijela za upravljanje sigurnošću. Za efikasnu organizaciju upravljanja sigurnosti nužno je pridržavati se određenih načela. Osnovna načela koja treba poštivati su:

- integralnost: osigurati integritet i cjelovitost sustava
- raspoloživost: osigurati nesmetano i neprekidno odvijanje poslovnih procesa
- povjerljivost: osigurati da informacije budu dostupne samo ovlaštenim osobama
- pouzdanost: osigurati dosljedno, očekivano ponašanje i rezultat
- odgovornost: dužnosti i odgovornosti moraju biti jasno opisane i prihvaćene
- pravovremenost: pravovremeno reagirati na moguće ugrožavanje pružanja informacijske usluge
- provjerljivost: redovna provjera kvalitete informacijske usluge i procjena rizika za informacije i informacijski sustav

3. Korisnici informatičkih usluga

Osobe koje se u radu koriste računalima dijele se na korisnike i davatelje informacijskih usluga. Korisnici su osobe koje se u svom radu služe računalima, proizvode dokumente ili unose podatke ali ne odgovaraju za instalaciju i konfiguraciju sistemskog softvera niti za ispravan i neprekidan rad računala i mreže. Svaki korisnik informacijskog sustava mora znati koja je njegova uloga u poboljšanju sigurnosti ukupnog sustava.
Dužnosti korisnika su:

- Pridržavanje pravila prihvatljivog korištenja, što znači da ne smiju koristiti računala za djelatnosti koje nisu u skladu sa važećim zakonima, etičkim normama i pravilima sigurnosne politike Kliničkog bolničkog centra Osijek.
- Izbor kvalitetne zaporke i njezina povremena promjena
- Prijavljivanje sigurnosnih incidenata kako bi se što prije riješili problemi
- Korisnici koji proizvode podatke i dokumente odgovorni su za njihovo čuvanje. (npr. moraju od davatelja usluga zatražiti da uspostave automatsku pohranu - backup važnih informacija ili u protivnom moraju sami izrađivati sigurnosne kopije)

Korisnicima se zabranjuje korištenje računalne opreme i mrežne infrastrukture bolnice u neprihvatljive svrhe.
U neprihvatljivo korištenje opreme i mrežne infrastrukture između ostalog spada:

- Uporaba nelicenciranog softvera
- Skidanje (download) autorski zaštićenih datoteka bez plaćanja naknade
- Preuzimanje tuđeg identiteta (korištenje opreme s tuđim korisničkim računom, slanje pošte pod tuđim imenom, kupovanje preko interneta s tuđom kreditnom karticom itd.)
- Provaljivanje na druga računala

- Traženje ranjivosti i sigurnosnih propusta. Korisnik ne smije samoinicijativno skenirati računala, probijati zaporke ili na bilo koji način istraživati sigurnosne propuste na računalima, bilo da ona pripadaju Kliničkom bolničkom centru Osijek ili ne.
- Napad uskraćivanjem resursa na druga računala
- Slanje masovnih poruka, bile one komercijalne prirode ili ne, čime se nepotrebno troše mrežni resursi
- Vrijeđanje i ponižavanje ljudi u internetskoj komunikaciji po vjerskoj, rasnoj, nacionalnoj ili nekoj drugoj pripadnosti
- Samovoljna instalacija softvera. Osobe zadužene za instalaciju programa u bolnici su djelatnici Službe za informatiku. Instaliranje softvera koji je licenciran ne smije se instalirati bez odobrenja Službe za informatiku.
- Priključivanje u mrežu KBC Osijek svojih privatnih računala i drugih mrežnih uređaja te samovoljno mijenjanje IP adresa odnosno dodjeljivanje istih nekim drugim uređajima. (IP mrežnu adresu dodjeljuje sistem inženjer bolnice i ona pripada isključivo jednom uređaju)
- Postavljanje web stranica na osobna računala
- Instalacija proxy-ja
- Korištenje P2P programa (peer to peer kao sto su: KaZaA, eDonkey, razni torrenti itd.)
- Ostavljanje uključenih računala u neradno vrijeme (računala se nakon završenog radnog vremena isključuju a ostaju uključena samo ona koja obavljaju specijalne zadaće i moraju biti uključena 24 sata).

4. Glavni korisnik

Kada postoji više korisnika koji rabe određenu aplikaciju za obradu podataka, radi poboljšanja sigurnosti, jedna osoba se imenuje glavnim korisnikom. U slučaju da KBC Osijek za pojedinu aplikaciju nije imenovao glavnog korisnika, glavnim korisnikom se smatra voditelj organizacijske jedinice koja koristi aplikaciju.
Zaposlenici koji unose podatke odgovaraju za vjerodostojnost tih podataka. Glavni je korisnik odgovaran za provjeru ispravnosti podataka, za provjeru ispravnosti i sigurnosti aplikacije, za dodjelu dozvola za pristup podacima i za mjere sprečavanja izmjene podataka od strane neautoriziranih osoba. Glavni korisnik kontaktira proizvođača aplikacije i dogovara isporuku novih verzija, traži ugradnju sigurnosnih mehanizama itd.

5. Davatelji informatičkih usluga

Davateljima usluga smatraju se profesionalci koji brinu o radu računala, mreže i informacijskih sustava. U KBC Osijek to je prvenstveno Služba za informatiku. Ako u bolnici postoje specijalizirani djelatnici za pojedinu djelatnost, oni postaju davateljima usluga za tu djelatnost (primjer: za PACS i RIS sustav su zaduženi tehničari iz Službe za tehničke poslove). Isto se odnosi i na specijalizirane medicinske uređaje. Ugovorom se odgovornost za ispravnost i neprekidnost

rada može prenijeti na vanjskog suradnika. Davatelji usluga odgovaraju za ispravnost i neprekidnost rada informacijskog sustava.

6. Službenik za zaštitu podataka

Temeljem Opće uredbe o zaštiti podataka, KBC Osijek je imenovao „Službenika za zaštitu podataka". Zadaća Službenika za zaštitu podataka je da:

- Vodi brigu o zakonitosti obrade osobnih podataka u smislu poštivanja odredbi Opće uredbe i ostalih propisa koji uređuju pitanja obrade osobnih podataka
- Upozorava voditelja zbirke osobnih podataka na nužnost primjene propisa o zaštiti osobnih podataka u slučajevima planiranja i radnji koje mogu imati utjecaj na pitanja privatnosti i zaštitu osobnih podataka
- Upoznaje sve osobe zaposlene u obradi osobnih podataka s njihovim zakonskim obvezama u svrhu zaštite osobnih podataka
- Omogućava ostvarivanje prava ispitanika sukladno odredbama Opće uredbe o zaštiti podataka
- Surađuje s Agencijom za zaštitu osobnih podataka u vezi s provedbom nadzora nad obradom osobnih podataka

7. Administriranje računala

Davatelji usluga dužni su administrirati računala i mrežnu opremu u skladu s pravilima struke, brinući istovremeno o funkcionalnosti i sigurnosti. Računala se moraju konfigurirati na taj način da budu zaštićena od napada izvana i iznutra što se osigurava instaliranjem softverskih zakrpi po preporukama proizvođača, listama pristupa, filtriranjem prometa i drugim sredstvima. Posebnu pažnju administratori su dužni posvetiti opremi koja obavlja ključne funkcije ili sadrži vrijedne i povjerljive informacije koje treba štititi od neovlaštenog pristupa. Administratori računala svakodnevno prate rad sustava, čitaju dnevničke zapise i provjeravaju rad servisa. Zadaća je administratora i nadgledanje rada korisnika, kako bi se otkrile nedopuštene aktivnosti.
Administratori su dužni prijaviti incidente Službeniku za zaštitu podataka te pomoći pri istrazi i uklanjanju problema. Incidenti se dokumentiraju kako bi se pomoglo u nastojanju da se izbjegnu slične situacije u budućnosti. Ukoliko je incident ozbiljan i uključuje kršenje zakona, prijavljuju se Zavodu za sigurnost informacijskih sustava RH.
Davatelji usluga dužni su u svome radu poštivati privatnost ostalih korisnika i povjerljivost informacija s kojima dolaze u dodir pri obavljanju posla.

8. Upravljanje mrežom

Za upravljanje mrežom u KBC Osijek je zadužen Odjel za informatičku infrastrukturu Službe za informatiku. Ovaj odjel u svakom trenutku ima točan popis svih mrežnih priključaka i umreženih uređaja, uključujući i prenosiva računala. Ako je podržan rad na daljinu, kada se primjerice djelatnicima dopušta da s kućnoga računala ažuriraju podatke, mora se osigurati da udaljeno računalo ne ugrozi sigurnost mreže KBC Osijek s obzirom na mogućnost da ga koriste neautorizirane osobe, članovi obitelji i slično. Povjerljivi podaci na udaljenom računalu moraju biti jednako sigurni kao da se računalo nalazi unutar kruga bolnice. Spajanje gostujućih računala na mrežu koja donose sa sobom vanjski suradnici, predavači, poslovni partneri i serviseri podrazumijeva poštivanje pravila koja se odnose na sigurnost i zaštitu podataka KBC Osijek. Ne dopušta se da oni po svom nahođenju priključuju računala na mrežu KBC Osijek zbog opasnosti od širenja virusa ili namjernih agresivnih radnji, poput presretanja mrežnoga prometa, prikupljanja informacija itd. KBC Osijek može odrediti priključna mjesta, primjerice u određenim uredima, gdje je dopušteno priključiti gostujuća računala te konfiguracijom mreže spriječiti da se s tog segmenta mreže dopre do ostalih računala u KBC Osijek. Bolnička bežična mreža zaštićena je na način da se ne može bilo tko priključiti i služiti se njome te snimati promet. To se postiže metodama enkripcije i autentifikacije uređaja i korisnika.

9. Instalacija i licenciranje softvera

Korištenje ilegalnog softvera predstavlja povredu autorskog prava i intelektualnog vlasništva. Da bi se zaštitila od moralne i materijalne štete koja time može nastati, KBC Osijek zadužuje jednu ili više odgovornih osoba za instaliranje softvera i njegovo licenciranje. Korisnik koji ima potrebu za nekim programom mora se obratiti ovlaštenoj osobi i zatražiti, uz obrazloženje, nabavu i instalaciju.

Svi korisnici se obvezuju na poštivanje autorskih prava potpisivanjem izjave o tome da su upoznati s Politikom prihvatljivog korištenja i da je prihvaćaju. Na taj način odgovornost za eventualno kršenje zakona prelazi sa KBC Osijek na nesavjesnog korisnika.

10. Povjerenstvo za sigurnost informacijskih sustava

Povjerenstvo za sigurnost informacijskih sustava osigurava sigurno upravljanje bolničkog informacijskog sustava.

Povjerenstvo za sigurnost informacijskih sustava imenuje Ravnatelj KBC Osijek te isto ima najmanje tri člana.

Povjerenstvo prima izvještaje o sigurnosnoj situaciji i predlaže mjere za njeno poboljšanje, uključujući nabavu opreme, organizaciju obrazovanja korisnika i specijalista. Povjerenstvo daje odobrenje za provođenje istrage u slučaju incidenata.

Povjerenstvo podnosi izvještaj o stanju sigurnosti ravnateljstvu KBC Osijek te se zalaže za donošenje konkretnih mjera, nabavu potrebne opreme, ulaganje u obrazovanje specijalista ali i običnih korisnika.

11. Fizička sigurnost i sigurne zone

Prostor u KBC Osijek dijeli se na dio koji je otvoren za javnost, prostor u koji imaju pristup samo zaposleni te prostor u koji pristup imaju samo skupine zaposlenih, ovisno o vrsti posla koji obavljaju.
Računalna oprema koja obavlja kritične funkcije, neophodne za funkcioniranje informacijskog sustava ili sadrži povjerljive informacije, fizički se odvaja u prostor u koji je ulaz dozvoljen samo ovlaštenim osobama.
Zbog vrste posla koje obavljaju to su u pravilu samo zaposlenici koji administriraju mrežnu i komunikacijsku opremu i poslužitelje ključnih servisa. Oni ulaze u sigurne zone samo kada treba ukloniti zastoje ili obaviti servisiranje opreme. Stoga je poželjno administratorima osigurati radni prostor odvojen od prostorija u kojima je smještena kritična oprema.
Kritična oprema treba biti zaštićena od problema s napajanjem električnom energijom što znači da električne instalacije moraju biti izvedene kvalitetno, da se koriste uređaji za neprekidno napajanje a po potrebi i generatori električne energije.
Treba predvidjeti i druge moguće probleme, poput poplava, požara i slično, te poduzeti mjere da se oprema i informacije zaštite i da se osigura što brži oporavak. U sigurnim zonama i u njihovoj blizini ne smiju se držati zapaljive i eksplozivne tvari.

12. Vanjske tvrtke

Povremeno se mora dopustiti pristup osobama iz vanjskih tvrtki ili ustanova radi servisiranja, održavanja, podrške, obuke, zajedničkog poslovanja, konzultacija itd.
KBC Osijek u ugovore s vanjskim tvrtkama ugrađuje odredbe kojima obvezuje poslovne partnere na poštivanje sigurnosnih pravila.
Ugovorom se regulira pristup, čime se podrazumijeva pristup prostorijama, pristup opremi ili logički pristup povjerljivim informacijama. Treću stranu se obvezuje na čuvanje povjerljivih informacija s kojima dođu u dodir pri obavljanju posla.
KBC Osijek može zahtijevati da svaka osoba koja pristupa povjerljivoj opremi, sigurnoj zoni ili osjetljivim informacijama potpiše Izjavu o čuvanju povjerljivih informacija. Ako u sigurnu zonu radi potrebe posla ulaze osobe koje nemaju ovlasti, mora im se osigurati pratnja. Strana osoba može se ostaviti da obavi posao u zaštićenom prostoru samo ako je osiguran video nadzor.
Ukoliko se vanjskoj tvrtki prepušta održavanje opreme i aplikacija s povjerljivim podacima, KBC Osijek može od vanjske tvrtke zatražiti popis osoba koje će dolaziti u prostorije KBC Osijek radi obavljanja posla. U slučaju zamjene izvršitelja, vanjska tvrtka dužna je na vrijeme obavijestiti KBC Osijek.
KBC Osijek zadržava pravo da osobama koje se predstavljaju kao djelatnici vanjskih tvrtki uskrati pristup ukoliko nisu na popisu ovlaštenih djelatnika.

13. Računalna oprema

Računalna oprema u KBC Osijek dijeli se prema zadaćama u sljedeće grupe:

- Zona javnih servisa (tzv. demilitarizirana zona) – oprema koja obavlja javne servise (DNS poslužitelj, HTTP poslužitelj, poslužitelj elektroničke pošte itd.).
- Intranet je privatna mreža KBC Osijek, sačinjavaju je poslužitelji internih servisa, osobna računala zaposlenih, računalne učionice te komunikacijska oprema lokalne mreže.
- Ekstranet je proširenje privatne mreže otvoreno mobilnim korisnicima, poslovnim partnerima ili povezuje izdvojene lokacije. U ovu grupu spadaju na primjer interni modemski ulazi ili veza lokalnih baza podataka s centralnim poslužiteljima (LDAP).

KBC Osijek je obavezan održavati popis sve računalne opreme s opisom ugrađenih komponenti, inventarskim brojevima itd. KBC Osijek brine jednako o svoj opremi kojom raspolaže, bez obzira na to tko je njezin vlasnik. Popis opreme prema zaduženjima nalazi su u računovodstvu osnovnih sredstava i sitnog inventara. Detaljniji popis vodi Odjel za informatičku infrastrukturu unutar Službe za informatiku. Pažnjom dobrog gospodara oprema se čuva od oštećivanja i otuđenja.

14. Osiguranje neprekidnosti poslovanja

Kako bi se sačuvali podaci u slučaju nezgoda, poput kvarova na sklopovlju, požara ili ljudskih grešaka, redovito se izrađuju rezervne kopije svih vrijednih informacija, uključujući i konfiguraciju softvera. Jednom tjedno se kopije pohranjuju u trezoru Službe za sigurnost. Procedura za izradu rezervnih kopija razrađuje se u zasebnom dokumentu. Zadužuju se konkretni djelatnici za izradu i čuvanje kopija informacija. Radi osiguranja neprekinutosti poslovanja, potrebno je razraditi i procedure za oporavak kritičnih sustava te ih čuvati u pismenom obliku, kako bi u slučaju zamjene izvršitelja novozaposleni djelatnici mogli brzo reagirati u slučaju nesreće.
Povremeno se provjerava upotrebljivost rezervnih kopija podataka te izvode vježbe oporavka sustava. Vježbe se ne izvode na produkcijskim računalima već na rezervnoj opremi u laboratorijskim uvjetima.

15. Nadzor nad informacijskim sustavima

KBC Osijek zadržava pravo nadzora nad instaliranim softverom i podacima koji su pohranjeni na računalima te nad načinom korištenja računala.

Nadzor se smije provoditi radi:

- Osiguranja integriteta, povjerljivosti i dostupnosti informacija i resursa.
- Provođenja istrage u slučaju sumnje da se dogodio sigurnosni incident.

- Provjere da li su informacijski sustavi i njihovo korištenje usklađeni sa zahtjevima sigurnosne politike.

Nadzor smiju obavljati samo osobe koje je ravnatelj za to ovlastio. Pri provođenju nadzora, ovlaštene osobe dužne su poštivati privatnost i osobnost korisnika i njihovih podataka. No u slučaju da je korisnik prekršio pravila sigurnosne politike, ne može se više osigurati povjerljivost informacija otkrivenih u istrazi te se one mogu koristiti u stegovnom ili sudskom postupku.

16. Doseg

Ova se pravila odnose na svu računalnu opremu koja se nalazi u prostorijama KBC Osijek, na sav instalirani softver, te na sve mrežne servise. Pravila su dužni poštivati i provoditi svi zaposleni i vanjski suradnici koji po ugovoru obavljaju određene poslove.

17. Provođenje

Korisnici su dužni pomoći osobama zaduženim za nadzor informacijskih sustava na taj način što će im pružiti sve potrebne informacije i omogućiti im pristup prostorijama i opremi radi provođenja nadzora.
Isto vrijedi i za administratore računala i pojedinih servisa koji su dužni osobama zaduženim za nadzor informacijskih sustava pomagati pri istrazi.

Pristup uključuje:

- Pristup na razini korisnika ili sustava svoj računalnoj opremi
- Pristup svakoj informaciji u elektroničkom ili tiskanom obliku koja je proizvedena ili spremljena na opremi KBC Osijek ili oprema KBC Osijek služi za njezin prijenos.
- Pristup radnom prostoru (uredu, laboratoriju, sigurnoj zoni itd.)
- Pravo na interaktivno nadgledanje i bilježenje prometa na mreži KBC Osijek

18. Nepridržavanje

Zaposlenika koji se ogluši na pravila o nadzoru može se disciplinski kazniti ili mu uskratiti prava korištenja mreže KBC Osijek i njezinih servisa.

19. Prateći dokumenti

Procedure koje čine sastavni dio sigurnosne politike informacijskog sustava su:

- Procedura za rukovanje zaporkama
- Procedura i upute za korištenje elektroničke pošte
- Procedura i upute za korištenje antivirusne zaštite

- Procedura za rješavanje sigurnosnih incidenata
- Procedura i upute za zaštitu od spama
- Procedura i upute za zaštitu od špijunskih programa (spyware)
- Procedura i upute za izradu kopija podataka
- Procedura za zbrinjavanje rashodovane informatičke opreme i ispisane dokumentacije
- Procedura za upravljanje rizicima

19.1. Procedura za rukovanje zaporkama

19.1.1. Odgovornost

Korisnik je odgovoran za sve računalne transakcije učinjene korištenjem dodijeljenog mu prijavnog imena i zaporke.

19.1.2. Minimalna dužina zaporke

Minimalna dužina zaporke za korištenje informatičkih resursa je osam znakova. Preporuča se korištenje kombinacija brojki i slova te korištenje i dužih zaporki od osam znakova.

19.1.3. Ne služiti se riječima iz rječnika

Prilikom odabira zaporke treba izbjegavati korištenje riječi iz domaćih i stranih rječnika jer se time otežava probijanje zaporki.

19.1.4. Koristiti složene zaporke

Preporuča se koristiti složene zaporke koja se sastoji iz kombinacije velikih i malih slova, brojeva i specijalnih znakova.

19.1.5. Ne koristiti imena bliskih osoba, ljubimaca, datume

Prilikom odabira zaporke treba izbjegavati korištenje imena bliskih osoba, ljubimaca, datume jer se takve zaporke lako otkriju socijalnim inženjeringom.

19.1.6. Trajanje zaporke

Zaporka za pristup mrežnim resursima je vremenski ograničena te ju je nužno mijenjati svaka 3 mjeseca. Dužina vremenskog trajanja zaporke je definirana na serverima bolnice.

19.1.7. Tajnost zaporke

Korisnici su odgovorni za svoju zaporku i ni u kom je slučaju ne smiju otkriti, čak ni administratorima sustava. Korisnik se treba odjaviti iz informacijskog sustava kada napušta radno mjesto.

19.1.8. Čuvanje zaporke

Zabranjeno je zaporke ostavljati na papirićima zalijepljenim na ekran, ostavljenim na stolovima, u nezaključanim ladicama i na drugim dostupnim mjestima. Korisnik je odgovoran za tajnost svoje zaporke te mora naći način da je sakrije. Ukoliko korisnik zaboravi zaporku, administrator će mu omogućiti da unese novu.

19.1.9. Administriranje zaporki

Posebnu pažnju treba obratiti zaporkama za prijavu na računala koja spadaju u zonu visokog rizika. Isto se odnosi na korisnička imena sa administratorskim pravima. Administratori su dužni konfigurirati ovjeru autentičnosti tako da zaporke zastare nakon 90 dana te onemogućiti korištenje zaporki koje su već potrošene ako sustav to dozvoljava. Prilikom provjere sustava, sigurnosni tim može ispitati da li su korisničke zaporke u skladu s navedenim pravilima.

19.1.10. Nepridržavanje

Svi zaposlenici KBC Osijek i suradnici koji u svome radu koriste računala, dužni su pridržavati se ovih pravila korištenja zaporki, dok su ih administratori dužni tehnički ugraditi u sve sustave koji to omogućavaju.
Korisnici koji se ne pridržavaju navedenih pravila ugrožavaju sigurnost informacijskog sustava. KBC Osijek je obavezan upoznati korisnike sa pravilima za kreiranje sigurnih zaporki. U slučaju ponovljenog ignoriranja ovih pravila, KBC Osijek može stegovno djelovati ili postaviti zaposlenika na radno mjesto na kojem je manja mogućnost ugrožavanja integriteta i sigurnosti sustava i podataka.

19.2. Procedura i upute za korištenje elektroničke pošte

19.2.1. Svrha

Elektronička pošta dio je svakodnevne komunikacije, poslovne i privatne. Komuniciranje elektronskom poštom u KBC Osijek zahtijeva da se razmotre svi aspekti elektroničke komunikacije s obzirom na moguće posljedice. Protokol koji se koristi za prijenos elektroničke pošte, SMTP ili Simple Mail Transport Protocol, nije potpuno siguran.
Korištenje elektroničke pošte se stoga smatra rizičnom djelatnošću, te se korisnici obavezuju na pridržavanje određenih pravila:

- Služba za informatiku postavlja i održava mail server KBC Osijek.
- Zaposlenicima se otvara korisnički račun radi obavljanja posla.
- Privatne poruke dozvoljene su u umjerenoj količini, ukoliko to ne ometa rad. Za privatne potrebe mogu se koristiti za to namijenjene HR-F domene.
- Zabranjeno je korištenje službene e-mail adrese za slanje uvredljivih, omalovažavajućih poruka ili za seksualno uznemiravanje.
- Nije dozvoljeno slanje lančanih poruka kojima se opterećuju mrežni resursi i ljudima oduzima radno vrijeme.
- Svaka napisana poruka smatra se dokumentom te na taj način podliježe propisima o autorskom pravu i intelektualnom vlasništvu. Zabranjeno je prosljeđivanje poruka dalje bez dozvole autora, odnosno pošiljatelja.
- Prilozi koji se šalju uz elektroničke poruke mogu sadržavati autorski zaštićene informacije, na primjer glazbu, filmove, članke itd. Primanje i slanje takvih sadržaja je strogo zabranjeno.
- Sve poruke pregledati će automatski aplikacija koja otkriva viruse. Ako poruka sadrži virus, neće biti isporučena a pošiljatelj i primatelj će biti o tome obaviješteni. Poruka će provesti određeno vrijeme u karanteni odakle ju je moguće na zahtjev primatelja izvući. Nakon određenog vremena, poruka se briše iz karantene kako bi se oslobodio prostor na disku.
- KBC Osijek zadržava pravo filtriranja poruka s namjerom da se zaustavi spam.
- U slučaju istrage uzrokovane mogućim sigurnosnim incidentom, sigurnosni tim može pregledavati kompletan sadržaj diska, pa time i e-mail poruke.
- Poruke putuju kao običan tekst te ih je lako presresti i pročitati ili čak izmijeniti sadržaj. POP i IMAP protokol koji se koriste za čitanje poruke je moguće presresti i pročitati na

putu od mail servera do korisnika. Stoga je, ako je sadržaj poruke povjerljive prirode, neophodno koristiti kriptografiju, na primjer SSL za prijenos i PGP za skrivanje sadržaja.

- Spam, slanje neželjenih komercijalnih poruka, sve više opterećuje promet na Internetu te oduzima vrijeme čak i ukoliko se takva poruka obriše bez čitanja. KBC Osijek će filtrirati spam na poslužitelju elektroničke pošte ali je obaveza korisnika da sami ne šalju takve poruke.
- Slanje poruka sa mreže KBC Osijek trebalo bi se prvenstveno vršiti sa mail adresom dodijeljenom od strane bolnice, npr. prezime.ime@kbo.hr ili prezime.ime@kbco.hr ili ime.prezime@kbo.hr ili ime.prezime@kbco.hr.

Mail server KBC Osijek ima ograničene resurse te stoga ne služi trajnom čuvanju elektronske pošte te se ne radi redoviti backup sadržaja elektronske pošte. Veličina poštanskog sandučića je ograničena. Korisnici se obavezuju redovito skidati poruke sa servera. Poruke se na serveru mogu ostaviti do 7 dana (godišnji odmor, dulje opravdano odsustvo). U slučaju duljeg perioda nemogućnosti skidanja poruka sa servera korisnik je dužan obavijestiti administratora sustava. U suprotnom administrator sustava ima pravo obrisati poruke sa servera starije od 30 dana, bez prethodne najave i upozorenja.

19.2.2. Procedura za dodjelu e-mail adrese

Pri zapošljavanju novog djelatnika, rukovodilac Klinike/Službe/Odjela popunjava propisani obrazac koji prosljeđuje Odjelu za kadrovske poslove KBC Osijek, koji od administratora poslužitelja elektroničke pošte traži otvaranje korisničkog računa. Djelatnik Odjela za kadrovske poslove ovjerava ispravnost podataka o djelatniku te ovjereni zahtjev prosljeđuje u Službu za informatiku.

Pri prestanku radnog odnosa, Odjel za kadrovske poslove KBC Osijek je dužna najkasnije u roku od sedam dana zatražiti zatvaranje korisničkog računa. Nakon odlaska iz KBC Osijek, korisnički se račun zatvara. Na mail serverima KBC Osijek otvara se elektronski sandučić isključivo djelatnicima KBC Osijek.

19.2.3. Nepridržavanje

Protiv korisnika koji ne poštuju ova pravila, KBC Osijek može pokrenuti disciplinski postupak. U slučaju ponovljenih težih prekršaja, korisniku se može zatvoriti korisnički račun i uskratiti pravo korištenja servisa elektroničke pošte.

19.3. Procedura i upute za korištenje antivirusne zaštite

19.3.1. Svrha

Virusi i crvi predstavljaju opasnost za informacijske sustave, ugrožavajući funkcioniranje mreže i povjerljivost podataka. Nove generacije virusa su izuzetno složene i opasne, sposobne da prikriju svoje prisustvo, presreću unos podataka na tipkovnici. Informacije poput zaporki ili povjerljivih dokumenata mogu slati svome tvorcu nekamo na Internet te otvoriti kriptiran kanal do „zaraženog" računala kako bi hakeri preuzeli kontrolu nad njim.

Stoga je zaštita od virusa obaveza KBC Osijek, administratora računala i svakog korisnika.

Zaštita od virusa u KBC Osijek obavezna je i provodi se na nekoliko razina:

- na poslužiteljima elektroničke pošte
- na internim poslužiteljima gdje se stavlja centralna instalacija
- na bolničkom vatrozidu
- na svakom osobnom računalu korisnika

Administratori su dužni instalirati protuvirusne programe na sva korisnička računala i konfigurirati ih tako da se izmjene u bazi virusa i u konfiguraciji automatski propagiraju sa centralne instalacije na korisnička računala u lokalnoj mreži, bez aktivnog sudjelovanja korisnika. Korisnici ne smiju samovoljno isključiti protuvirusnu zaštitu na svome računalu. Ukoliko iz nekog razloga moraju privremeno zaustaviti protuvirusni program, korisnici moraju obavijestiti sistem inženjera.

19.3.2. Nepridržavanje

Korisnik koji samovoljno isključi protuvirusnu zaštitu na svom računalu te na taj način izazove štetu, odgovarat će zbog povrede radne obveze te odgovara za svu štetu koja pri tome nastane KBC Osijek ili nekom trećem.

19.4. Procedura za rješavanje sigurnosnih incidenata

19.4.1. Svrha

Svrha ove procedure je da KBC Osijek obavezu prijavljivanja sigurnosnih incidenata te da razradi procedure za provođenje istrage.

19.4.2. Prijava incidenta

Svaki zaposlenik ili suradnik KBC Osijek, dužan je prijavljivati sigurnosne incidente poput usporenog rada servisa i aplikacija, nemogućnosti pristupa, gubitka ili neovlaštene izmjene podataka, pojave virusa itd.
Incidenti se prijavljuju „Službeniku za zaštitu podataka". Svaki incident se dokumentira. Ozbiljniji incidenti prijavljuju se prema naputku Ministarstva zdravstva RH, Zavodu za sigurnost informacijskih sustava (ZSIS) na mail adresu cert@zsis.hr.
S druge strane, uspostavljen je i obrnuti komunikacijski kanal između Zavoda za sigurnost informacijskih sustava i Kliničkog bolničkog centra Osijek. U tu svrhu, u KBC Osijek, otvorena je nova mail adresa cert@kbco.hr na koju stižu informacije o pojavi potencijalnih prijetnji. Poruke sa ove mail adrese primaju Službenik za zaštitu podataka KBC Osijek, Voditelj Službe za informatiku, Voditelj odjela za informatičku infrastrukturu i Voditelj odjela za poslovnu informatiku. Ozbiljnije prijetnje objavljuju se na intranet stranicama KBC Osijek.

19.4.3. Procedure za rješavanje sigurnosnih incidenata

Administratori informatičkog sustava KBC Osijek, smiju pratiti korisničke procese. Ako sumnjaju da se računalo koristi na nedozvoljen način, mogu ispisati sadržaj korisničkog direktorija ali ne smiju provjeravati sadržaj korisničkih podatkovnih datoteka (npr. dokumenata ili e-mail poruka).
Daljnja istraga može se provesti samo ako je prijavljena Povjerenstvu za sigurnost koje je uspostavljeno sigurnosnom politikom KBC Osijek, uz poštivanje slijedećih pravila:

- Istragu provodi jedna osoba ali uz prisustvo svjedoka kako bi se omogućilo svjedočenje o poduzetim radnjama.
- Prvo pravilo forenzičke istrage jest da se informacijski sustav sačuva u zatečenom stanju, odnosno da se ne učine izmjene koje bi otežale ili onemogućile dijagnosticiranje.
- Najprije se napravi kopija zatečenog stanja (npr. na traku, CD ili dr.), po mogućnosti na takav način da se ne izmijene atributi datoteka.
- Dokumentira se svaka radnja, tako da se ponavljanjem zabilježenih akcija može rekonstruirati tijek istrage.
- istrazi se piše izvještaj, kako bi u slučaju potrebe mogli poslužili kao dokaz u eventualnim disciplinskim ili sudskim procesima.
- Izvještaji o incidentu smatraju se povjerljivim dokumentima i čuvaju se na taj način da im pristup imaju samo ovlaštene osobe.

KBC Osijek može objavljivati statističke podatke o sigurnosnim incidentima, bez otkrivanja povjerljivih i osobnih informacija.

19.4.4. Sankcije

Svrha je istrage da se odredi uzrok nastanka problema kako bi se spriječilo ponavljanje incidenta. Ako je uzrok sigurnosnom incidentu bio ljudski faktor, protiv odgovornih osoba se mogu poduzeti odgovarajuće sankcije.
KBC Osijek može osobama odgovornim za sigurnosni incident zabraniti fizički pristup prostorijama ili logički pristup podacima.
Ukoliko je incident izazvao zaposlenik vanjske tvrtke, KBC Osijek može zatražiti od vanjske tvrtke da ga ukloni sa liste osoba ovlaštenih za obavljanje posla u KBC Osijek. U slučaju teže povrede pravila sigurnosne politike, KBC Osijek može raskinuti ugovor s vanjskom tvrtkom.

19.5. Procedura i upute za zaštitu od spama

19.5.1. Svrha

Internetom putuje sve više neželjenih komercijalnih poruka, tzv. spam. Masovne poruke elektroničke pošte najjeftiniji su način reklamiranja. Cijenu plaćaju korisnici i tvrtke jer čitanje i brisanje neželjenih poruka troši radno vrijeme i umanjuje produktivnost. Dio neželjenih poruka nastoji uvući primatelja u kriminalne aktivnosti kao na primjer otvaranje računa za pranje novca ili su prijevara.

19.5.2. Pravila za administratore

Administratori poslužitelja elektroničke pošte dužni su konfigurirati računala na taj način da se što više neželjenih poruka zaustavi.
Prva mogućnost jest da se definira ulazni filter koji će prilikom primanja poruke konzultirati baze podataka koje sadrže popise poslužitelja koji su otvoreni za odašiljanje (open relay), te baza s adresama poznatih spam-era. Pošta koja dolazi s tako pronađenih adresa neće se primati.

Druga razina zaštite je automatska provjera sadržaja. Poslužitelj može poruke koje su obilježene kao spam spremati na određeno vrijeme u karantenu.
Treću razinu zaštite određuju sami korisnici. Poruke dobivaju bodove koji ukazuju na vjerojatnost da se radi o spam-u. Kako nije uvijek moguće pouzdano definirati što je spam, ovakva zaštita mora biti uvjetna, odnosno krajnjem korisniku se prepušta uključivanje bodovanja i konfiguriranje preusmjeravanja označenih poruka.

19.5.3. Pravila za korisnike

Korisnici ne smiju slati masovne poruke bez obzira na njihov sadržaj. Upozorenja na viruse su često lažna i šire zablude. Korisnici ne smiju radi stjecanja dobiti odašiljati propagandne poruke koristeći računalnu opremu koja pripada KBC Osijek.

19.5.4. Nepridržavanje

Protiv korisnika koji se ponašaju suprotno pravilima prihvatljivog korištenja i šalju masovne neželjene poruke, biti će pokrenut disciplinski postupak.

19.6. Procedura i upute za zaštitu od špijunskih programa (spyware)

19.6.1. Svrha

Internetom se širi sve više neželjenih, skrivenih, tzv. špijunskih programa (spyware) koji mogu biti veoma opasni. To su programi koji se često instaliraju na računalo bez znanja korisnika te na računalu čine razne, štetne radnje.
Posljedice mogu biti:

- usporeni rad računala
- promijenjena početna mrežna stranica
- neprekidna aktivnost na Internetu
- otvaranje drugog prozora iz čista mira

Najčešće dolaze skriveni uz neke besplatne programe.

19.6.2. Pravila za administratore

Administratori osobnih računala dužni su na računala instalirati odgovarajuću zaštitu od špijunskih programa (obično dolaze u sklopu antivirusnih programa) koji omogućava uklanjanje špijunskih programa s računala. Program je potrebno konfigurirati tako da ga može pokrenuti i svaki korisnik računala.

19.6.3. Pravila za korisnike

Ako korisnici instaliraju besplatni software, dužni su obratiti pozornost da uz njega ne instaliraju i neki od skrivenih programa.
Korisnici su dužni povremeno pokrenuti programe za zaštitu kako bi uklonili ove maliciozne programe.

19.6.4. Nepridržavanje

Korisnici su dužni obratiti pozornost da na računalo ne instaliraju skriveni programi, a protiv onih koji namjerno instaliraju špijunske programe, bit će pokrenut disciplinski postupak.

19.7. Procedura i upute za izradu kopija podataka

Ravnatelj KBC Osijek, u dogovoru sa Voditeljem Službe za informatiku, određuje tko je od zaposlenika zadužen za izradu kopija pojedine vrste podataka. Veću pozornost treba obratiti na spremanje važnijih podataka (baza podataka, elektronski karton pacijenta, kadrovska evidencija, poslovni podaci, itd.).
Izrada kopija podataka prilagođena je postojećoj tehnološkoj osnovi kojom raspolaže KBC Osijek.

Osnovna strategija izrade kopija je sljedeća:
Kopija podataka iz baze podataka glavnih servera se izrađuje minimalno jednom dnevno na fizički odvojenom mediju (drugi disk, optički medij). Također, tri ili četiri puta godišnje radi se potpuna kopija (svi podaci i kod).
Za navedeno je zadužen sistem inženjer ili osoba kojoj on povjeri obavljanje toga zadatka.
Kopija podataka ključnih servisa (mail, mrežne stranice, DNS, itd.), kao i osobnih podataka s poslužitelja, izrađuje se nekoliko puta godišnje, po potrebi i češće (veće izmjene na sustavu).
Za izradu kopije podataka s osobnih računala zadužen je sam korisnik računala.

Podatke s osobnih računala spremaju korisnici (zaposlenici) pojedinačno. Ukoliko im je u tome potrebna pomoć, obraćaju se sistem inženjeru.
Zaposlenici i vanjski suradnici za izradu sigurnosnih kopija i pohranu podataka mogu koristiti ili medije dobivene od strane KBC Osijek ili vlastite medije. U bilo kojem slučaju, svaki pojedinac je sam odgovoran za sigurnost istih.

19.8. Procedura za zbrinjavanje rashodovane informatičke opreme i ispisane dokumentacije

Mediji koji sadrže povjerljive informacije (posebnu pažnju treba obratiti na osobne podatke pacijenata i zaposlenika te poslovne podatke), ne bacaju se već se uništavaju metodom koja osigurava da se trajno i pouzdano uništi sadržaj (spaljivanjem, usitnjavanjem, prešanjem). Ukoliko se zastarjela i rashodovana računalna oprema daje na korištenje trećoj strani, obavezno je uništavanje podataka sa diskova posebnim programom koji nepovratno prebriše sadržaj diska. Isto vrijedi i prilikom rashodovanja računala. Poslije toga, diskovi se mogu predati u Odjel za strukturno održavanje i zaštitu okoliša u svrhu fizičkog uništenja.

19.9. Procedura za upravljanje rizicima

Upravljanje sigurnosnim rizicima sastavni je dio Sigurnosne politike koja se provodi s ciljem prepoznavanja specifičnih prijetnji i ranjivosti informacijskog sustava.

Procjena sigurnosnog rizika informacijskog sustava u Kliničkom bolničkom centru Osijek obavlja se najmanje jednom godišnje od strane Službenika za zaštitu podataka u suradnji sa stručnim i kompetentnim osobama za pojedinu djelatnost, kako bi se ustanovile promjene u oblicima prijetnji informacijskom sustavu te izvršile izmjene Sigurnosne politike.
Službenik za zaštitu podataka u suradnji sa stručnim službama KBC Osijek vrši procjenu učinka (Data protection impact assessment) za obrade koje će prouzročiti visok rizik za prava i slobode ispitanika.

20. Izmjene sigurnosne politike

Povjerenstvo za sigurnost informacijskih sustava po potrebi usklađuje i predlaže Ravnatelju KBC Osijek promjenu Sigurnosne politike i svih ostalih mjera, uputa i procedura donesenih na temelju Sigurnosne politike.

21. Stupanje na snagu

Ova Sigurnosna politika stupa na snagu danom donošenja.

Ravnatelj
Kliničkog bolničkog centra Osijek

doc.dr.sc. Željko Zubčić, dr.med.

KLINIČKI BOLNIČKI CENTAR OSIJEK
RAVNATELJSTVO
2
OSIJEK, J. Huttlera 4