Sigurnosna politika informacijskog sustava Klinike za psihijatriju Vrapče

1. Na koga se odnose odredbe Sigurnosne politika informacijskog sustava Klinike za psihijatriju Vrapče?

Odredbe Sigurnosne politika informacijskog sustava Klinike za psihijatriju Vrapče (u daljnjem tekstu: Sigurnosna politika) odnose se na:

- svu računalnu opremu i pripadajuće programe koji se nalaze u prostorima Klinike za psihijatriju Vrapče (u daljnjem tekstu Klinike);
- administratore informacijskih sustava;
- korisnike, među koje spadaju zaposlenici i vanjski suradnici;
- vanjske tvrtke koje, po ugovoru ili bez ugovora, rade na održavanju opreme ili softvera.

Poštivanje Sigurnosne politike jedna je od važnih točaka u sustavu upravljanja kvalitetom. Zato se u sklopu Sigurnosne politike uspostavljaju kontrolne točke kojima se nastoje spriječiti sigurnosni incidenti.

2. Organizacija upravljanja sigurnošću

Pri provođenju Sigurnosne politike ključno jest da se u svakom trenutku točno znaju odgovornosti i obveze korisnika sustava. Stoga će se raspodijeliti zaduženja i kontinuirano obrazovati korisnike kako bi se postigao zadovoljavajući stupanj sigurnosti (tj. stupanj sigurnosti koji je u skladu sa standardima kvalitete).

3. Korisnici informatičkih usluga

Korisnici informatičkih usluga su osobe koje se u svom radu služe računalima, proizvode dokumente ili unose podatke. Svaki korisnik informacijskog sustava mora znati koja je njegova uloga u poboljšanju sigurnosti ukupnog sustava.

Dužnosti korisnika su najmanje:

- Pridržavanje pravila prihvatljivog korištenja, što znači da ne smiju koristiti računala za djelatnosti koje nisu u skladu s važećim zakonima, etičkim i moralnim normama i pravilima Sigurnosne politike;
- Adekvatno čuvanje zaporki, bez odavanja trećima;
- Pravovremeno prijavljivanje sigurnosnih incidenata kako bi se što prije riješili problemi;
- Korisnik koji unosi podatke u informatički sustav odgovoran je za vjerodostojnost podataka;
- Zabranjuje se pristup pornografskim, pedofilskim i sličnim sadržajima na Internetu;
- Zabranjuje se nelegalno preuzimanje (download), korištenje i širenje zakonom

zaštićenih materijala - softvera, glazbe, e-knjiga, e-časopisa, dokumenata, filmova itd.;

- Zabranjuje se postavljanje, pokretanje i širenje malicioznih programa, kodova, virusa, trojanaca, spyware-a, malware-a, spama, itd.;
- Zabranjuje se korisnicima da samovoljno premještaju pojedine periferne uređaje (tipkovnice, miševe, monitore, itd.) ili da samovoljno vrše „popravak" neispravnih računala. Ako neko računalo (ili neki njegov dio) ne radi ispravno, korisnici su dužni to prijaviti zaposlenim informatičarima;
- Zbog velikog negativnog utjecaja na *throughput,* brzinu i performanse pristupa Internetu, te zbog slučajeva zlouporabe, zabranjuje se korištenje torrent-a i sličnih protokola;
- Zabranjuje se korištenje Tor i sličnih pretraživača za „dark web".

4. Davatelji informatičkih usluga

Davateljima usluga smatraju se profesionalci koji brinu o radu računala, mreže i informacijskih sustava – osiguravaju ispravnost i neprekidnost rada informacijskog sustava. Davatelji informatičkih usluga u Klinici su informatičar – statističar i informatički inženjer (u daljnjem tekstu: zaposleni informatičari).

5. Specijalisti za sigurnost

Klinika će pri rješavanju sigurnosnih incidenata, po potrebi, koristiti pomoć CARNeta i CERT-a. Pored toga, Klinika će, iz redova zaposlenih informatičara, imenovati Voditelja sigurnosti (engl. CSO, Chief Security Officer) čija je prvenstvena briga sigurnost informacijskih sustava. Poželjno je da Voditelj sigurnosti bude stručan, ali da istovremeno posjeduje sposobnost za vođenje ljudi i da je komunikativan.

Voditelj sigurnosti piše prijedloge internih propisa iz područja informatičke sigurnosti, nadzire rad mreže i servisa, organizira obrazovanje korisnika, komunicira s upravom, sudjeluje u donošenju odluka o nabavi računala i softvera, te sudjeluje u razvoju softvera, kako bi osigurao poštivanje pravila iz sigurnosne politike.

6. Administriranje računala

Davatelji usluga (Klinika, CARNet, ostali davatelji usluga) dužni su administrirati računala i mrežnu opremu u skladu s pravilima struke, brinući istovremeno o funkcionalnosti i sigurnosti. Sva računala u Klinici imaju administratore koji odgovaraju za instalaciju, nadopunu i konfiguraciju softvera.

Računala se moraju konfigurirati na način da budu zaštićena od napada izvana i iznutra, što se osigurava instaliranjem softverskih zakrpi po preporukama proizvođača, listama pristupa, filtriranjem prometa, vatrozidom i drugim prikladnim sredstvima.

Administratori računala svakodnevno prate rad sustava, čitaju dnevničke zapise i provjeravaju rad servisa. Nadalje, zadaća je administratora nadgledanje rada korisnika, kako bi se otkrile nedopuštene aktivnosti. U slučajevima kad administrator treba na sustavu obaviti više poslova istovremeno, prioritet određuje samostalno, u skladu s pravilima struke, brinući istovremeno o

funkcionalnosti i sigurnosti.
Posebnu pažnju administratori su dužni posvetiti opremi koja obavlja ključne funkcije ili sadrži vrijedne i povjerljive informacije koje treba štititi od neovlaštenog pristupa.
Davatelji usluga dužni su u svome radu poštivati privatnost ostalih korisnika i povjerljivost informacija s kojima dolaze u dodir pri obavljanju posla.

7. Upravljanje mrežom

Zaposleni informatičari odgovorni su za upravljanje mrežom, konfiguriranje mrežnih uređaja, dodjeljivanje adresa, kreiranje virtualnih LAN-ova itd.
Svako novo uključivanje u mrežu provodi se pod kontrolom zaposlenog informatičara.
Zaposleni informatičari moraju u svakom trenutku imati točan popis svih mrežnih priključaka i umreženih uređaja, uključujući i prijenosna računala.
Za bežičnu mrežu, Klinika će se osigurati da se ne može bilo tko priključiti na privatnu mrežu i snimati promet. To će se postići metodama enkripcije uređaja i autentikacije korisnika, te odvajanja lokalnih IP adresa od bežične mreže na zaseban segment.
Radi zaštite povjerljivih informacije pri prijenosu mrežom, poželjno je da takav promet bude kriptiran.

8. Nabavka novog softvera i hardvera

Korisnik koji ima potrebu za novim hardverom ili softverom obvezan je sastaviti obrazloženu pisanu zamolbu te ju predati u Urudžbeni zapisnik. Urudžbeni zapisnik zamolbu dostavlja zaposlenom informatičaru koji će dati stručno mišljenje o nabavci hardvera ili softvera. O opravdanosti konačno odlučuje Poslovni kolegij. Iznimno, ako je nabavka hitna ili je manje vrijednosti, o opravdanosti odlučuje ravnatelj Klinike.

9. Fizička sigurnost

Klinika vodi popis osoba koje imaju pravo pristupa u zaštićena područja (server sobu, komunikacijske ormare i sl.). Porta posjeduje i čuva ključeve koji omogućuju ulazak u zaštićena područja te će stoga porta biti obavještena o osobama koje imaju pravo pristupa u zaštićena područja.
Kritična oprema u zaštićenim područjima 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 (UPS), a po potrebi i generatori električne energije.
U zaštićenim područjima i u njihovoj blizini ne smiju se držati zapaljive i eksplozivne tvari.
Povremeno se mora dopustiti pristup zaštićenim područjima osobama iz vanjskih tvrtki ili ustanova radi servisiranja, održavanja, podrške, obuke, zajedničkog poslovanja, konzultacija, itd.
Klinika može zahtijevati da svaka osoba koja pristupa povjerljivoj opremi, zaštićenom području ili osjetljivim informacijama potpiše Izjavu o čuvanju povjerljivih informacija.
Ako u zaštićeno područje, radi potrebe posla, ulaze osobe koje nemaju ovlasti, mora im se osigurati pratnja.

Ako se vanjskoj tvrtki prepušta održavanje opreme i aplikacija s povjerljivim podacima, Klinika može od vanjske tvrtke zatražiti popis osoba koje će dolaziti u prostorije radi obavljanja posla. U slučaju zamjene izvršitelja, vanjska tvrtka dužna je na vrijeme obavijestiti Kliniku. Klinika će osobama koje se predstavljaju kao djelatnici vanjskih tvrtki uskrati pristup ako nisu na popisu ovlaštenih djelatnika.

10. Računalna opreme

U prostorijama Klinike nalazi se i oprema trećih osoba koja je dana na korištenje (npr. oprema CARNeta i sl.). Klinika će trećim osobama dopustiti pristup njihovoj opremi, uz obvezu da poštuju sve odredbe Sigurnosne politike.

Klinika je obavezna održavati popis sve računalne opreme, s opisom ugrađenih komponenti, inventarskim brojevima, itd.

Klinika jednako brine o svoj opremi kojom raspolaže, bez obzira na to tko je njezin vlasnik. Oprema se čuva od oštećivanja i otuđenja pažnjom dobrog vlasnika.

Svaki korisnik odgovara za fizičku sigurnost opreme.

11. Osiguranje neprekidnosti poslovanja

Kako bi se sačuvali podaci u slučaju nezgoda (kvarova na sklopovlju, požara, ljudskih grešaka i sl.), redovito se izrađuju rezervne kopije svih vrijednih informacija, uključujući i konfiguraciju softvera. Preporučuje se izrada više kopija, koje se čuvaju na različitim mjestima.

Povremeno se provjerava upotrebljivost rezervnih kopija podataka te izvode vježbe oporavka sustava.

12. Nadzor nad informacijskim sustavima

Klinika zadržava pravo nadzora nad instaliranim softverom i podacima koji su pohranjeni na umreženim 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 jesu li informacijski sustavi i njihovo korištenje usklađeni s zahtjevima sigurnosne politike

Nadzor smiju obavljati samo osobe koje je Klinika za to ovlastila (administratori). Pri provođenju nadzora ovlaštene osobe dužne su poštivati privatnost i osobnost korisnika te njihovih podataka. Međutim, 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 daljnjem postupku.

Korisnici su dužni pomoći osobama zaduženim za nadzor informacijskih sustava, tako što će im pružiti sve potrebne informacije i omogućiti im pristup prostorijama i opremi radi provođenja nadzora.

Zaposlenik koji uskrati pristup ovlaštenim osobama, u sklopu nadzora, čini povredu obveza iz radnog odnosa.

13. Rukovanje zaporkama

Prosječan korisnik nerijetko smatra kako ne mora brinuti o sigurnosti jer njegovo računalo ne sadrži vrijedne informacije. Međutim, kompromitiranjem jednog osobnog računala u lokalnoj mreži ili jednog korisničkog računa na poslužitelju, napadač je probio obrambenu liniju i otvorio prolaz za napade na važnije sustave i informacije - lanac puca na najslabijoj karici. Stoga je svaki korisnik obvezan, prilikom korištenja i čuvanja lozinke, doprinositi zaštiti ukupnog sustava.

Svi zaposlenici Klinike, te treće ovlaštene osobe koje koriste računala Klinike, dužni su pridržavati se ovih pravila korištenja zaporki, dok su ih administratori dužni tehnički ugraditi u sve sustave koji to omogućavaju.

Pravila za korištenje zaporki su sljedeća:

1. Minimalna dužina zaporke - Kratku zaporku lakše je probiti te je stoga minimalna dužina zaporke 8 znakova.
2. Ne koristiti riječi iz rječnika - Hackeri posjeduju zbirke rječnika, što im olakšava probijanje ovakvih zaporki (tzv. Dictionary attack).
3. Izmiješati mala i velika slova s brojevima - Na primjer: h0bo3niCa. Na prvi pogled besmislena i teška za pamćenje, ova je zaporka izvedena iz riječi hobotnica. Polazište je pojam koji lako pamtimo, ali onda po nekom algoritmu vršimo zamjenu znakova.
4. Ne koristiti imena bliskih osoba, ljubimaca i datume - Takve se zaporke lako otkriju socijalnim inženjeringom.
5. Periodičke promjene zaporke - Promjena zaporke smanjuje vjerojatnost njezina otkrivanja.
6. Tajnost zaporke - Korisnici su odgovorni za svoju zaporku te ju ne smiju nikome otkriti, uključujući administratore. Hackeri nastoje izmamiti zaporke lažno se predstavljajući kao administratori. Pravi administratori imaju mogućnost rješavanja probleme i bez poznavanja korisničkih zaporki.
7. Čuvanje zaporke - Zaporke se ne ostavljaju na papirićima koji su zalijepljeni na ekran ili ostavljeni na stolovima, u nezaključanim ladicama, itd. Korisnik je odgovoran za tajnost svoje zaporke, te mora naći način da je sakrije. Ako korisnik zaboravi zaporku, administrator će mu omogućiti da unese novu.
8. Administriranje zaporki - Na računalima koja spadaju u zonu visokog rizika administratori će konfigurirati sustav tako da se korisnički račun zaključa nakon tri ili više neuspjelih pokušaja prijave. Prilikom provjere sustava, sigurnosni tim može ispitati jesu li korisničke zaporke u skladu s navedenim pravilima.

Korisnici koji se ne pridržavaju navedenih pravila ugrožavaju sigurnost informacijskog sustava. Klinika će obrazovati korisnike oko upravljanja i čuvanja zaporki.

14. Uporaba elektroničke pošte

Elektronička pošta dio je svakodnevne komunikacije. Komuniciranje e-mailom zahtijeva da se

razmotre svi aspekti elektroničke komunikacije s obzirom na moguće posljedice.
Protokol koji se koristi za prijenos elektroničke pošte, SMTP (eng. Simple Mail Transport Protocol), nije od samog početka dizajniran da bude siguran. Dodatne probleme ponekad izazivaju i korisnici, koji nisu posve svjesni zamki pri korištenju e-maila.
Problemi koji mogu nastati pri korištenju elektroničke pošte:

- Nesigurnost protokola
  - o Poruke putuju kao običan tekst te ih je zato lako presresti i pročitati ili čak izmijeniti sadržaj.
  - o Lako je krivotvoriti adresu pošiljatelja, tako da nikada niste sigurni tko vam je zapravo poslao poruku.
  - o Protokoli za čitanje elektroničke pošte, POP i IMAP, u svom osnovnom obliku šalju korisničko ime i zaporku kao običan tekst, pa ih je moguće presresti i pročitati. Stoga je potrebno, kad god je to moguće, koristiti kriptografiju, na primjer SSL za prijenos i PGP za skrivanje sadržaja.
- Nezgode
  - o Uvijek je moguće pritisnuti pogrešnu tipku ili kliknuti mišem na susjednu ikonu. Time može nastati nepopravljiva šteta - ne možete zaustaviti poruku koja je već otišla.
  - o Česta je pogreška i kada se pokupi pogrešna adresa iz adresara.
  - o Neki e-mail klijenti sami dovršavaju e-mail adresu koju tipkate. U žurbi se može prihvatiti pogrešna adresa, slična onoj koju zapravo želite.
- Nesporazumi
  - o Ljudi su skloni pisati e-mail poruke na opušteniji način. To može dovesti do nesporazuma ako druga strana ne shvaća poruku na isti način. Stoga službene dopise pišite u službenom tonu.
  - o Iza vašeg imena u e-mail adresi nalazi se ime ustanove. Pišući, budite svjesni kako netko može shvatiti vašu privatnu prepisku kao službeni dopis, odnosno vaše privatno mišljenje kao službeni stav ustanove. Stoga u raspravi uvijek jasno naznačite kada je izneseni stav vaše privatno uvjerenje.
- Otkrivanje informacija
  - o Poruke namijenjene jednoj osobi, greškom se mogu proslijediti drugima, na primjer na mailing listu. To se može dogoditi: - (zlo)namjerno, s ciljem da se naškodi drugoj osobi ili tvrtki - nemarom sudionika, koji ne traži dozvolu za prosljeđivanje poruke - slučajnom pogreškom, na primjer nehotičnim klikom mišem na pogrešnu ikonu (Reply All umjesto Reply).
- Radna etika
  - o Lančane poruke koje ljudi šalju poznanicima mogu sadržavati lažne informacije ili biti dio prijevare, s namjerom da se ljudima izvuče novac ("pomozite nesretniku kojem treba operacija", "otvorite račun kako bi svrgnuti diktator mogao izvući novac iz nestabilne afričke države"...). Za provjeru ovakvih poruka (engl. hoax) može se koristiti servis CARNet CERT-a "Hoax recognizer".
  - o Spam, slanje neželjenih komercijalnih poruka, sve više opterećuje promet na Internetu, te oduzima vrijeme, čak i ako brišete takve poruka bez čitanja. Klinika će, kada je moguće, filtrirati spam na poslužitelju elektroničke pošte, ali je obveza korisnika da sami ne šalju takve poruke.

- Povreda autorskih prava
  - Prilozi koji se šalju uz elektroničke poruke mogu sadržavati autorski zaštićene informacije, na primjer glazbu, filmove, članke, itd.

Zbog svega nabrojanog korištenje elektroničke pošte smatra se rizičnom djelatnošću, te se korisnici obavezuju na pridržavanje određenih pravila:

- Zaposlenicima se otvara korisnički račun radi obavljanja posla. U službenoj komunikaciju korisnici su obvezni koristiti dobivenu službenu e-mail adresu. Zabranjuje se korištenje privatne e-mail adrese za službene svrhe.
- Zabranjeno je službenu e-mail adresu koristiti za privatne svrhe.
- Korisnici su obvezni pridržavati se pravila pristojnog ponašanja na Internetu te se službenu e-mail adresu ne smije koristiti za slanje uvredljivih, omalovažavajućih poruka ili za seksualno uznemiravanje i sl.
- Sve poruke može automatski pregledati aplikacija koja otkriva viruse - ako poruka sadrži virus, antivirusni program uklanja virus i upozorava korisnika. Korisnik ne smije ugasiti antivirusni program te time spriječiti otkrivanje virusa.
- U slučaju istrage uzrokovane mogućim sigurnosnim incidentom, ovlaštena osoba može pregledavati kompletan sadržaj diska, pa time i e-mail poruke. Korisnik je obvezan omogućiti pristup ovlaštenoj osobi.

Pri zapošljavanju novog djelatnika, voditelj ustrojstvene jedinice će zatražiti od zaposlenog informatičara otvaranje nove e-mail adrese.
Pri prestanku radnog odnosa, voditelj ustrojstvene jedinice je obvezan, najkasnije u roku od sedam dana, zatražiti od zaposlenog informatičara zatvaranje e-mail adrese.

15. Zaštita od virusa

Virusi i crvi predstavljaju opasnost za informacijske sustave, ugrožavajući funkcioniranje mreže i povjerljivost podataka.
Nove generacije virusa izuzetno su složene i opasne, sposobne da prikriju svoje prisustvo. Informacije poput zaporki ili povjerljivih dokumenata mogu slati hackeru, te otvoriti kriptiran kanal do vašeg računala, kako bi hacker preuzeo kontrolu nad njim.
Također je bitno napomenuti pojavu Crypto virusa. To je vrsta virusa koja zaključava dokumente složenim kriptografskim algoritmom u svrhu iznude novca od korisnika dokumenata. Jedina zaštita je pravovremena izrada sigurnosnih kopija podataka na vanjski medij. Virus se u većini slučajeva širi preko zaraženih privitaka elektroničke pošte.
Stoga zaštita od virusa ne smije više biti stvar osobnog izbora, već obaveza ustanove, administratora računala i svakog korisnika.

Zaštita od virusa je obavezna te se provodi na nekoliko razina:

- na internim poslužiteljima, gdje se stavlja centralna instalacija
- na svakom osobnom računalu korisnika - administratori su obvezni instalirati protuvirusne programe na sva korisnička računala i konfigurirati ih tako da se izmjene u bazi virusa i u konfiguraciji automatski propagiraju s centralne instalacije na korisnička računala u

lokalnoj mreži, bez aktivnog sudjelovanja korisnika.
Korisnici ne smiju samovoljno isključiti protuvirusnu zaštitu na svome računalu. Ako iz nekog razloga moraju privremeno zaustaviti protuvirusni program, korisnici moraju obavijestiti informatičare.

16. Zaštita od neželjenih poruka (tzv. spam-a)

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, na primjer otvaranje računa za pranje novca, ili su prijevara, nastoje pobuditi samilost kako bi se izvukao novac (engl. Hoax). Za prepoznavanje ovakvih poruka korisnici mogu koristiti uslugu CARNet CERT-a Hoax recognizer

Administratori poslužitelja elektroničke pošte konfigurirat će računala tako da se što više neželjenih poruka zaustavi *(spamassasin)*.
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 spamera. 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.

Korisnici ne smiju radi stjecanja dobiti odašiljati propagandne poruke koristeći računalnu opremu koja pripada ustanovi.

17. Zaštita od spyware-a

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 štetne radnje. Posljedice mogu biti: usporeni rad računala, promijenjena početna web stranica, neprekidna aktivnost na Internetu, neželjeno otvaranje drugog prozora i sl. Najčešće dolaze potiho uz neki besplatan softver.

Administratori osobnih računala obvezni su na računalo instalirati odgovarajući antispyware program koji omogućava uklanjanje špijunskih programa s računala. Program je potrebno konfigurirati tako da ga može pokrenuti i tzv. obični korisnik računala.

Uzimajući u obzir kako spyware često dolazi s novim instaliranim besplatnim softverom, korisnici nisu ovlašteni sami instalirati softver bez kontrole zaposlenog informatičara.

18. Izrada sigurnosnih kopija

Zaposleni informatičari te ovlaštene treće osobe (vanjski informatičari koji održavaju određeni

softver, sustav i sl.) zaduženi su za izradu kopija pojedinih vrsta podataka. Veća pozornost obratit će se na spremanje važnijih podataka (baza podataka, mail, web, dns, itd.).
Izradu kopija podataka treba prilagoditi postojećoj tehnološkoj osnovi kojom raspolaže Klinika.
Podatke s osobnih računala spremaju korisnici (zaposlenici) pojedinačno. Ako im je u tome potrebna pomoć, obraćaju se informatičarima.

19. Sigurnosni incidenti

Svaki zaposlenik ili vanjski suradnik Klinike dužan je prijavljivati sigurnosne incidente, poput usporenog rada servisa, nemogućnosti pristupa, gubitka ili neovlaštene izmjene podataka, pojave virusa, itd.
Klinika će izraditi i održavati kontakt listu osoba kojima se prijavljuju problemi u radu računala i servisa.
Izvještaji o incidentima smatraju se povjerljivim dokumentima, spremaju se na sigurno mjesto i čuvaju 10 godina, kako bi mogli poslužiti za statističke obrade kojima je cilj ustanoviti najčešće propuste radi njihova sprečavanja, ali isto tako i kao dokazni materijal u eventualnim daljnjim procesima.
Ozbiljniji incidenti prijavljuju se CARNetovom CERT-u, preko obrasca na web stranici www.cert.hr.

Administratori smiju pratiti korisničke procese. Ako sumnjaju da se računalo koristi na nedozvoljen način, mogu provjerit sadržaj korisničkog direktorija.
Ako je utvrđen sigurnosni incident te zaposleni informatičar procijeni da je potrebno provesti daljnju istragu, na sjednici Poslovnog kolegija, kojoj obvezno prisustvuje Specijalist za sigurnost, izložit će se sigurnosni incident te će se donijeti odluka o provođenju istrage ili odluka o drugim prikladnim radnjama koje je potrebno poduzeti. Iznimno, ako je nužno hitno odlučiti, odluku može donijeti ravnatelj Klinike.
U istrazi je potrebno poštivati sljedeća pravila:

- Istragu provodi jedna osoba, ali uz prisutnost 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 CD, DVD, flash medij, itd.), 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.
- O istrazi se napiše izvještaj, kako bi u slučaju potrebe mogao poslužiti kao dokaz u daljnjim postupcima.
- Izvještaji o incidentu smatraju se povjerljivim dokumentima i čuvaju se tako da im pristup imaju samo ovlaštene osobe.

Svrha je istrage da se odredi uzrok nastanka problema, te da se iz toga izvuku zaključci o tome kako spriječiti ponavljanje incidenta, ili se barem bolje pripremiti za slične situacije. Ako je uzrok sigurnosnom incidentu bio ljudski faktor, protiv odgovornih se mogu poduzeti

odgovarajuće sankcije.
Klinika može osobama odgovornim za sigurnosni incident zabraniti fizički pristup prostorijama dok se ne riješi sigurnosni incident.
Svako otkriveno kazneno djelo potrebno je trenutno i neodgodivo prijaviti nadležnim institucijama.

20. Upravljanje povjerljivim informacijama

Povjerljivost je zaštita informacija kod koje je potrebno spriječiti otkrivanje informacija od strane neovlaštenih osoba ili sustava. Ukoliko se informacijama koje su označene kao povjerljive ne rukuje na pravilan način, može doći do povrede povjerljivosti, tj. otkrivanja povjerljivih informacija (usmenim putem, ispisom, kopiranjem, slanjem informacija e-poštom, itd.).
Klinika je obvezna upravljati povjerljivim informacijama sukladno pozitivnim pravnim propisima.
Klinika posebnu pozornost usmjerava u zaštitu povjerljivosti podataka pacijenta uzimaju u obzir kako su to podaci strogo osobne naravi i čije otkrivanje neovlaštenim osobama može predstavljati grupu povredu prava pacijenata.

Mediji koji sadrže povjerljive informacije ne bacaju se, već se uništavaju metodom koja osigurava da se trajno i pouzdano uništi sadržaj (usitnjavanjem i sl.).

URBROJ: 21-16/2-22
U Zagrebu, 26. svibnja 2022. godine

RAVNATELJICA KLINIKE
prof. prim. dr. sc. Petrana Brečić, dr. med.