

Politika bezbjednosti informacija

Informacija je podatak sa određenim značenjem, koji ima upotrebnu vrijednost odnosno saznanje koje se može prenijeti u bilo kojem obliku (pisanom, audio, vizualnom, elektronskom ili nekom drugom). Da bi se informacijama moglo kvalitetno upravljati potrebno ih je na adekvatan način klasifikovati, precizno im odrediti svrhu, vrijednost, dostupnost kao i ostale attribute. Vlasništvo nad informacijama i njihova upotreba postali su ključni za funkcionisanje države, privrede, javnih službi i svakodnevni život građana.

Informaciona bezbjednost u savremenim uslovima postala je jedan od ključnih faktora razvoja, zbog čega se uspostavljaju brojni standardi koji uključuju najbolju praksu i preporuke o bezbjednom upravljanju informacijama.

Iz gore navedenog očituje se potreba za implementaciom sistema za upravljanje i bezbjednost informacija u Kliničkom centru Banja Luka.

Namjena ovakvog pristupa informacijama je da obezbjedi i zaštiti informacije i imovinu od svih prijetnji, bilo internih ili eksternih, slučajnih ili namjernih kroz uspostavljanje, implementaciju, izvršavanje, nadziranje, preispitivanje, održavanje i poboljšanje sistema menadžmenta bezbjednosti informacija (ISMS). Implementacija ove politike i pravila je važna za održavanje integriteta informacionog sistema za pružanje usluga. Politika bezbjednosti informacija obezbjeđuje i garantuje:

- informacije će biti zaštićene od neovlašćenog pristupa istim,
- održavaće se povjerljivost informacija,
- informacije neće biti otkrivene neovlašćenim osobama bilo slučajnim ili namjernim aktivnostima,
- integritet informacija će se sačuvati kroz zaštitu od neovlašćene izmjene,
- mogućnost pristupa i izmjene informacija ovlašćenim licima kada je to potrebno,
- biće obezbjeđena usaglašenost sa svim kontrolnim i zakonskim zahtjevima,
- podrška politici kroz kontinuirane poslovne planove koji će se određivati, održavati i testirati u stalnom praktičnom radu,
- obučavanje zaposlenih u svim organizacionim jedinicama,
- sve povrede sigurnog rukovanja informacijama će se razmatrati i istražiti,
- sve povrede sigurnosti će se dokumentovati i istražiti.

Menadžment će definisati viziju bezbjednosti informacija sa ciljem neometanog poslovanja, zaštite povjerljivih informacija i daljeg uspješnog razvoja organizacije, kao i postizanja zadovoljstva korisnika pruženom uslugom i kvalitetom pružene usluge.

Svi zaposleni su odgovorni za implementaciju politike bezbjednosti i zaštite informacija i moraju da pruže podršku rukovodstvu koje je propisalo politiku i pravila.

Osnovni ciljevi ove politike su:

- zaštita informacija Kliničkog centra Banja Luka,
- zaštita informacija korisnika koji koriste usluge Kliničkog centra,
- zaštita informacione imovine koja pripada Kliničkom centru,
- pružanje pouzdanih informacija zaposlenima i čuvanje njihove povjerljivosti u svim slučajevima pristupa postojećim informacijama.

Svrha ove politike je da identifikuje rizike po imovinu, vrijednost imovine i da se utvrdi moguća ranjivost i potencijalni uzroci nekog neželjenog incidenta koji mogu dovesti do štete na sistemu ili u ustanovi. Da se upravlja rizicima na prihvatljivoj nivou kroz

dizajniranje, implementaciju i održavanje ISMS. Da je u saglasnosti sa drugim standardima i dokumentima Kliničkog centra, uključujući:

- standard ISO 9001:2008,
- zakonsku regulativu koja tretira područje rada Kliničkog centra Banja Luka,
- dokumenta sistema menadžmenta i sistema kvaliteta,
- da je u saglasnosti sa ugovorenim obavezama Kliničkog centra,
- da obezbjeđje djelovanje u saglasnosti sa standardom ISO 27001:2005.

GENERALNI DIREKTOR
Prof. dr sc. med. Mirko Stanetić
