Zavod za informatiku Osijek, Radićeva 4, 31000 Osijek
tel: 031/221-850 fax: 031/221-869 // e-mail: zio@zio.hr //žr: 2340009-1110042039

Klasa: 030-01/11-01/4
Ur.broj: 2158/72-01-11-01

Predmet: Sigurnosna politika informacijsko-informatičkog sustava Zavoda za informatiku Osijek

Datum: 13. travnja 2011.
Revizija: 1/B od 19.05.2020.

1. Definicija sigurnosne politike

Sigurnosna politika dio je sustava upravljanja sigurnošću informacijsko-informatičkog sustava Zavoda za informatiku Osijek. Njezina je svrha definiranje prihvatljivog i neprihvatljivog načina ponašanja, raspodjele zadataka i odgovornosti u njezinu provođenju te propisivanje sankcije u slučaju nepridržavanja. Sastoji se od ovog osnovnog dokumenta, koji postavlja opće principe, i pratećih dokumenata (pravilnika) koji se mogu ustrojiti po potrebi a pobliže definiraju pravila za specifična područja primjene:

- Pravilnik o instalaciji i licenciranju softvera
- Pravilnik o izradi sigurnosnih kopija podataka (backup)
- Pravilnik o korištenju zaporki
- Pravilnik o korištenju elektroničke pošte
- Pravilnik o zaštiti od virusa
- Pravilnik o zaštiti od neželjene pošte (spama)
- Pravilnik o rješavanju sigurnosnih incidenata
- Pravilnik o rukovanju povjerljivim informacijama

Pravilnici su ovisni o promjenama u tehnologiji i organizaciji, pa se mogu mijenjati i dorađivati te je stoga Sigurnosna politika informacijsko-informatičkog sustava Zavoda za informatiku Osijek javno dostupna na poveznici www.zio.hr/sigurnosnapolitika. Svi djelatnici Zavoda za informatiku Osijek dužni su se upoznati s trenutno važećom revizijom sigurnosne politike i primjenjivati je te upozoriti vanjske korisnike na obavezu njene primjene.

2. Područje obuhvata sigurnosne politike

Pravila rada i ponašanja koja definira sigurnosna politika vrijede za:

- Svu računalnu opremu (hardver i softver) koja se nalazi u prostorima i u vlasništvu Zavoda
- Korisnike, među koje spadaju: zaposlenici, vanjski suradnici i korisnici usluga Zavoda
- Davatelje informatičkih usluga (administratore)
- Vanjske tvrtke koje po ugovoru rade na održavanju opreme ili softvera

3. Korisnici informatičko-informacijskog sustava

Korisnici su osobe koje se u svom radu ili učenju služe računalima i ostalom informatičkom opremom, proizvode dokumente ili unose podatke, ali ne odgovaraju za instalaciju i konfiguraciju softvera, niti za ispravan i neprekidan rad računala i računalne mreže. Dužnosti korisnika su:

- Pridržavanje pravila prihvatljivog korištenja, što znači da ne smiju koristiti računala za djelatnosti koje nisu u skladu sa potrebama posla, učenja, važećim zakonima, etičkim normama i pravilima sigurnosne politike
- 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. To znači da moraju od davatelja informatičkih usluga zatražiti da uspostave automatsku pohranu (backup) važnih informacija, ili u protivnom moraju sami izrađivati sigurnosne kopije.

Dokumenti u elektroničkom obliku smatraju se službenim dokumentima na isti način kao i dokumenti na papiru, pa su korisnici dužni osigurati njihovo čuvanje i ograničiti pristup samo ovlaštenim osobama.

4. Davatelji informatičkih usluga (administratori)

Davateljima informatičkih usluga smatraju se profesionalci iz redova zaposlenika Zavoda koji brinu o radu računala, mreže i informacijskih servisa. U Zavodu za informatiku Osijek nadležnosti davatelja informatičkih usluga (administratora) definirani su Pravilnikom o unutarnjem ustrojstvu Zavoda za informatiku Osijek. Oni odgovaraju za ispravnost i neprekidnost rada informacijskog sustava i svih servisa informacijsko-informatičkog sustava Zavoda.

5. Vanjske tvrtke

Za obavljanje poslova servisiranja, održavanja, podrške, obuke, zajedničkog poslovanja i konzultacija povremeno se može dopustiti pristup osobama iz vanjskih tvrtki ili ustanova pri čemu se vanjska tvrtka mora upozoriti na obvezu pridržavanja sigurnosne politike te čuvanja povjerljivih informacija s kojima dođu u dodir pri obavljanju posla. Ako u sigurnu zonu radi potrebe posla ulaze osobe koje nemaju ovlasti, mora im se osigurati pratnja.

Zavod zadržava pravo da osobama koje se predstavljaju kao djelatnici vanjskih tvrtki uskrati pristup ukoliko nisu na popisu ovlaštenih djelatnika.

6. Fizička sigurnost

Prostor na ustanovi dijeli se na dio koji je otvoren za javnost, prostor u koji imaju pristup samo zaposleni, te prostore u koje pristup imaju samo grupe zaposlenih, ovisno o vrsti posla koji obavljaju. Elektroničkim sustavom za kontrolu pristupa ograničava se pristup u sistem salu koja predstavlja sigurnu zonu, a sustavom videonadzora omogućuje se snimanje točaka prostora ključnih za nadzor fizičke sigurnosti.

7. Nepridržavanje

Korisnik koji se ne pridržava sigurnosne politike preuzima sve pravne posljedice koje iz toga proizlaze a zaposlenik se može i disciplinski kazniti.

8. Rok za primjenu

Sigurnosna politika stupa na snagu osmog dana od dana donošenja. Rok za prilagodbu sigurnosnoj politici je 15 dana od dana stupanja na snagu.

mr.sc. Dražen Tomić, dipl.inž.el.
Ravnatelj