POLITIKA INFORMACIJSKE SIGURNOSTI

Sadržaj

Svrha, područje primjene i korisnici

Svrha ove politike najviše razine je propisati smisao, smjer, principe i osnovna pravila vezana za upravljanje informacijskom sigurnošću.

Ova Politika se primjenjuje na cjelokupni sustav upravljanja informacijskom sigurnošću (engl. *Information Security Management System* – ISMS), kao što je definirano u dokumentu *Odluka o opsegu integralnog sustava upravljanja*.

Korisnici ovog dokumenta su svi djelatnici Grada Pule, kao i relevantne vanjske strane.

Referentni dokumenti

- norma ISO/IEC 2700:2013 točka 5.2 te 5.3
- *Odluka o opsegu integralnog sustava upravljanja*
- *Metodologija za procjenu i obradu rizika*
- *ISMS SoA i status implementuranosti*
- *Statutarne, regulatorne i ugovorne obveze*
- *Postupak za upravljanje incidentima*

Osnovni pojmovi informacijske sigurnosti

Povjerljivost – karakteristika informacije da joj mogu pristupiti samo ovlaštene osobe ili sustavi.

Cjelovitost – karakteristika informacije da je mogu mijenjati samo ovlaštene osobe ili sustavi na dopušten način.

Raspoloživost – karakteristika informacije da je dostupna ovlaštenim osobama kad je potrebna.

Informacijska sigurnost – osiguravanje povjerljivosti, dostupnosti (raspoloživosti) i cjelovitosti (integriteta) informacija.

Sustav upravljanja informacijskom sigurnošću – dio cjelokupnog procesa upravljanja koji se bavi sa planiranjem, implementacijom, održavanjem, pregledom i poboljšanjem informacijske sigurnosti temeljno na uspostavi upravljanja rizicima.

Upravljanje informacijskom sigurnošću

Ciljevi i mjerenje

Generalni ciljevi vezani za sustav upravljanja informacijskom sigurnošću su sljedeći: postizanje boljeg imidža na tržištu i smanjenje šteta od potencijalnih incidenata, i usklađeni su sa poslovnim ciljevima, strategijom i poslovnim planovima organizacije. Gradonačelnik je odgovoran za pregled tih generalnih ciljeva ISMS-a i za postavljanje novih.

Za pregled postojećih i postavljanje novih generalnih ciljeva ISMS-a zadužen Gradonačelnik. Ciljeve za pojedine sigurnosne mjere (kontrole) ili grupe sigurnosnih mjera predlaže Voditelj ISU-a, a odobrava Gradonačelnik kroz *ISMS SoA i status implementuranosti* – ti ciljevi se trebaju pregledati i revidirati barem jednom godišnje.

Zahtjevi vezani za informacijsku sigurnost

Ova politika i cjelokupni ISMS moraju biti u skladu sa zakonskim propisima primjenjivim za organizaciju iz područja informacijske sigurnosti, zaštitom i tajnosti podataka i osobnih podatka kakao i sa ugovornim obvezama.

Detaljan popis svih ugovornih i zakonskih obveza je naveden u dokumentu *Statutarne, regulatorne i ugovorne obveze*.

Upravljanje informacijskom sigurnošću

Proces odabira načina upravljanja (zaštitnih mjera) definira se u *Metodologiji procjene i obrade rizika*.

Odabrani načini upravljanja i njihov status implementacije popisani su u *ISMS SoA i status implementuranosti*.

Odgovornosti

Osnovne odgovornosti za ISMS su sljedeće:

- Gradonačelnik je odgovoran da se implementacija i održavanje ISMS-a provodi u skladu sa ovom Politikom te da svi potrebni resursi stoje na raspolaganju.
- Voditelj ISU je odgovoran za operativnu koordinaciju ISMS-a, kao i za izvješćivanje o radu ISMS-a.
- Gradonačelnik mora provesti pregled ISMS-a barem jednom godišnje ili prilikom svake veće promjene, i o tome sastaviti zapisnik. Svrha pregleda od strane menadžmenta jest ustanoviti prikladnost, opravdanost i učinkovitost ISMS-a.
- obučavanje i osvješćivanje djelatnika za informacijsku sigurnost provodit će Voditelj ISU.

- za zaštitu cjelovitosti, dostupnosti i povjerljivosti informacijskih resursa zadužen je vlasnik svakog informacijskog resursa
- svi sigurnosni incidenti ili slabosti moraju se dojaviti Voditelju ISU.
- Vlasnici procesa određuju koje informacije vezane za informacijsku sigurnost će se proslijediti i kojim zainteresiranim strankama (unutarnjim i vanjskim), od koga i kada.
- Gradonačelnik odgovoran je za usvajanje i implementaciju Plana obučavanja i osvješćivanja koji se odnosi na sve osobe koje imaju ulogu u upravljanju informacijskom sigurnošću.

Komunikacija Politike

Gradonačelnik je zadužen da svi djelatnici Grada Pule budu upoznati sa ovom Politikom, kao i sve prikladne vanjske stranke.

Potpora provedbi ISMS-a

Ovime Gradonačelnik sa svojim najužim suradnicima iz Ureda Grada izjavljuje da će poduprijeti implementaciju i kontinuirano poboljšavanje ISMS-a sa dovoljno resursa, kako bi se postigli ciljevi zacrtani ovom Politikom, kao i zadovoljili svi utvrđeni zahtjevi.

Valjanost i upravljanje dokumentom

Ovaj dokument vrijedi od datuma digitalnog potpisa.

Vlasnik ovog dokumenta je Gradonačelnik, koji mora ovaj dokument pregledati i eventualno dopuniti najmanje jednom godišnje i on ga potpisuje.

Sljedeće kriterije treba uzeti u obzir kada se ocjenjuje učinkovitost i primjerenost ovog dokumenta:

- broj djelatnika i vanjskih stranaka koje imaju ulogu u ISMS-u, a da nisu upoznati sa ovim dokumentom
- neusklađenost ISMS-a sa zakonima i propisima, ugovornim obvezama te drugim internim dokumentima organizacije
- neučinkovitost implementacije i održavanja ISMS-a
- nedovoljno jasno određena odgovornost za provedbu ISMS-a

	Datum:	Ime i prezime:	Funkcija:	Potpis:
Izradio:	**23.02.2017**	**Dražen Stepanov**	**Voditelj ISU**	
Odobrio:	**12.04.2017**	**Boris Miletić**	**Gradonačelnik**	