[logo organizacije]

[naziv organizacije]

POLITIKA INFORMACIJSKE SIGURNOSTI

Oznaka:	
Verzija dokumenta:	
Datum verzije:	
Izradio:	
Odobrio:	
Stupanj povjerljivosti:	

Comment [DK1]: Za pomoć oko ispunjavanja ovog dokumenta pogledajte:

Video tutorijal: 'How to Write the ISMS Policy According to ISO 27001'
http://www.iso27001standard.com/tutorial/free-video-tutorial-how-to-write-the-iso-27001-information-security-policy/

Comment [DK2]: Ovaj članak će Vam pomoći razumjeti svrhu Politike informacijske sigurnosti: Politika informacijske sigurnosti – koliko detaljna treba biti?
http://www.iso27001standard.com/blog/2010/05/26/information-security-policy-how-detailed-should-it-be/

Comment [DK3]: Ako Vam je potreban dokument koji će dati detaljna pravila za informacijsku sigurnost, iskoristite Politiku pravilne uporabe koja je uključena u Paket dokumentacije.

Politiku pravilne uporabe možete zasebno kupiti ovdje:
http://www.iso27001standard.com/documentation/acceptable-use-policy/

Comment [DK4]: Potrebno je dopuniti ovaj dokument na svim mjestima gdje se nalaze uglate zagrade [ ].

Comment [DK5]: Sustav označavanja dokumenata treba uskladiti sa postojećim sustavom označavanja dokumentacije u organizaciji; ukoliko takav ne postoji onda se ovaj redak može brisati.

©2015 Ovaj predložak smiju koristiti klijenti tvrtke EPPS usluge d.o.o. www.iso27001standard.com sukladno licenčnom ugovoru

Evidencija promjena na dokumentu

Datum	Verzija	Izradio	Opis promjena
GGGG-MM-DD	0.1	Dejan Košutić	Osnovni nacrt dokumenta

Sadržaj

1. SVRHA, PODRUČJE PRIMJENE I KORISNICI 3

2. REFERENTNI DOKUMENTI 3

3. OSNOVNI POJMOVI INFORMACIJSKE SIGURNOSTI 3

4. UPRAVLJANJE INFORMACIJSKOM SIGURNOŠĆU 3

4.1. CILJEVI I MJERENJE 3
4.2. ZAHTJEVI VEZANI ZA INFORMACIJSKU SIGURNOST 4
4.3. UPRAVLJANJE INFORMACIJSKOM SIGURNOŠĆU 4
4.4. KONTINUITET POSLOVANJA 4
4.5. ODGOVORNOSTI 4
4.6. KOMUNIKACIJA POLITIKE 4

5. POTPORA PROVEDBI ISMS-A 5

6. VALJANOST I UPRAVLJANJE DOKUMENTOM 5

©2015 Ovaj predložak smiju koristiti klijenti tvrtke EPPS usluge d.o.o. www.iso27001standard.com sukladno licenčnom ugovoru.

1. 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 ISMS-a.

Korisnici ovog dokumenta su svi djelatnici [naziv organizacije], kao i relevantne vanjske strane.

2. Referentni dokumenti

- norma ISO/IEC 27001 točka 5.2 te 5.3
- Odluka o opsegu ISMS-a
- Metodologija za procjenu i obradu rizika
- Izvješće o primjenjivosti
- Popis pravnih, regulatornih i ugovornih obveza
-
- [Politika kontinuiteta poslovanja]
- [Procedura za upravljanje incidentima]

Comment [DK6]: Navesti ostale interne dokumente organizacije na koje se veže ova politika – npr. strateški plan razvoja, poslovni plan, dokument o upravljanju rizicima na strateškom nivou i sl.

Comment [DK7]: Vidjeti točku 4.4

Comment [DK8]: Vidjeti točku 4.5

3. Osnovni pojmovi informacijske sigurnosti

Povjerljivost – karakteristika informacije da je dostupna samo ovlaštenim osobama ili sustavima.

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

Raspoloživost – karakteristika informacije da joj mogu pristupiti ovlaštene osobe kad je potrebno.

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.

4. Upravljanje informacijskom sigurnošću

4.1. Ciljevi i mjerenje

Generalni ciljevi vezani za sustav upravljanja informacijskom sigurnošću su sljedeći: postizanje boljeg imidža na tržištu / smanjenje štete od potencijalnih incidenata, / usklađenost sa zakonskim ciljevima.

Comment [DK9]: Po potrebi izmijeniti i/ili dopuniti neke drugim ciljevima kao što su usklađenost sa propisima/zakonima, broj incidenata, zadovoljstvo korisnika i sl.

Možete pokušati poboljšati mjerivost ciljeva, npr. "smanjiti broj incidenta za 20% tijekom sljedećih 12 mjeseci."

©2015 Ovaj predložak smiju koristiti klijenti tvrtke EPPS usluge d.o.o. www.iso27001standard.com sukladno licenčnom ugovoru.

strategijom i poslovnim planovima organizacije. [funkcija]je odgovorna za pregled tih generalnih ciljeva ISMS-a i za postavljanje novih.

[redacted] za to ovlaštene], a odobrava [naziv funkcije] kroz Izvješće o primjenjivosti – ti ciljevi se trebaju pregledati barem jednom godišnje.

Comment [DK10]: Procijeniti da li je ovo dobra dinamika.

4.2. Zahtjevi vezani za informacijsku sigurnost

Ova politika i cjelokupni ISMS moraju biti u skladu sa zakonskim propisima primjenjivim za [redacted]

Comment [DK11]: Navesti i druga područja koja [redacted] osobnih podataka i sl.

[redacted] naveden u Popisu pravnih, regulatornih i ugovornih obveza.

4.3. Upravljanje informacijskom sigurnošću

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

[redacted]

4.4. Kontinuitet poslovanja

Comment [DK12]: Izbrisati ovu točku ukoliko se kontinuitet poslovanja neće implementirati.

Upravljanje kontinuitetom poslovanja propisano je kroz Politiku upravljanja kontinuitetom poslovanja

4.5. Odgovornosti

Osnovne odgovornosti za ISMS su sljedeće:

- [naziv funkcije] je odgovoran da se implementacija i održavanje ISMS-a provodi u skladu sa ovom Politikom te da svi potrebni resursi stoje na raspolaganju.
- [redacted]
- [redacted] 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 [naziv funkcije]
- [redacted] svakog informacijskog resursa
- svi sigurnosni incidenti ili slabosti moraju se dojaviti [naziv funkcije]
- [redacted]
- [naziv funkcije] odgovoran je za usvajanje I implementaciju Plana obučavanja i osvješćivanja [redacted]

Comment [DK13]: Član top menadžmenta

Comment [DK14]: Ovo može biti jedna ili više osoba; odgovornosti se mogu podijeliti na dodatne segmente ISMS-a.

Comment [DK15]: Ovo mora biti najviše [redacted] kolegij direktora ili sl.

Comment [DK16]: Može se staviti i više odgovornih osoba, i podijeliti ih po vrstama incidenata.

Comment [DK17]: Ili se može referencirati na Proceduru za upravljanje incidentima.

4.6. Komunikacija Politike

©2015 Ovaj predložak smiju koristiti klijenti tvrtke EPPS usluge d.o.o. www.iso27001standard.com sukladno licenčnom ugovoru.

[naziv funkcije] je zadužen da svi djelatnici [naziv organizacije] budu upoznati sa ovom Politikom, kao i sve prikladne vanjske stranke.

5. Potpora provedbi ISMS-a

Ovime [naziv funkcije ili tijela najvišeg menadžmenta u opsegu ISMS-a] 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.

6. Valjanost i upravljanje dokumentom

Ovaj dokument vrijedi od [datum].

Vlasnik ovog dokumenta je [naziv funkcije] koji mora ovaj dokument pregledati i eventualno dopuniti najmanje jednom godišnje.

Comment [DK18]: Ovo je preporučljiva dinamika; promijeniti po potrebi.

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

[funkcija]
[ime i prezime]

Comment [DK19]: Politiku mora odobriti glavni menadžment u opsegu ISMS-a.

_____

[potpis]

Comment [DK20]: Ovo je potrebno jedino ukoliko se u Proceduri za upravljanje dokumentacijom i zapisima odredilo da je potrebno potpisivati papirnatu verziju dokumenata.

©2015 Ovaj predložak smiju koristiti klijenti tvrtke EPPS usluge d.o.o. www.iso27001standard.com sukladno licenčnom ugovoru.