Politika informacijske sigurnosti

1 SVRHA

Kontakt tours (u daljnjem tekstu Društvo) donosi Politiku informacijske sigurnosti koja kao krovni dokument predstavlja okvir za upravljanje sustavom informacijske sigurnosti. Politikom informacijske sigurnosti definiraju se osnovna načela, te odgovornosti koje se odnose na upravljanje sigurnosti informacijskog sustava.

Obavljanje poslovnih aktivnosti *Društva* ovisi o ispravnom radu informacijskog sustava. Uloga informacijskog sustava je poboljšati produktivnost radnika i efikasnost poslovnog procesa, a informacije se smatraju osjetljivom i ključnom imovinom *Društva*.

Sustav upravljanja informacijskom sigurnosti uspostavlja se u svrhu zaštite informacija od prijetnji kojima se narušava njihova povjerljivost, integritet i/ili dostupnost radi osiguranja kontinuiteta poslovanja, smanjenja poslovnog rizika i povećanja prihoda od poslovnih prilika.

2 CILJ

Cilj ove Politike je uspostaviti okvir za upravljanje sigurnošću informacijskog sustava kojim će se umanjiti utjecaj sigurnosnih incidenata i zaštititi informacijsku imovinu (informacije, informacijske sustave, dokumentaciju, medije za pohranu podataka, telekomunikacijsku opremu i uređaje, mjesto rada, poziciju na tržištu, radnike), operativni kontinuitet, intelektualno i materijalno vlasništvo te pravne i poslovne interese od štete i gubitka uzrokovanih unutarnjim ili vanjskim, namjernim ili slučajnim, prijevarnim, prekršajnim i kaznenim djelovanjem u svrhu zaštite kontinuiteta poslovanja *Društva*.

2.1 Područje primjene

Obvezu pridržavanja odredbi Politike informacijske sigurnosti te svih sigurnosnih pravilnika i procedura koje proizlaze iz ove Politike imaju svi korisnici informacijskog sustava *Društva*, zaposlenici, sve osobe koje privremeno obavljaju poslove prema ugovoru te svi vanjski suradnici ili partneri *Društva* koji dolaze u doticaj sa resursima informacijskog sustava.

2.2 Odgovornosti

Osobe ovlaštene za zastupanje Društva usvaja politike, pravilnike i procedure te druge provedbene dokumente koji detaljno uređuju pojedine odredbe informacijske sigurnosti, način korištenja i provedbu programa sigurnosti informacijskih sustava.

Voditelj informacijske sigurnosti predlaže *ovlaštenoj osobi za zastupanje* sigurnosne standarde i procedure koje proizlaze iz sigurnosne politike i nadzire primjenu i provedbu sigurnosnih mjera za koje je ovlašten. *Voditelj informacijske sigurnosti* koordinira uspostavu i provedbu postavljenih ciljeva sigurnosti te je zadužen za kreiranje i reviziju Politike informacijske sigurnosti koju predlaže *ovlaštenim osobama za zastupanje* na usvajanje.

Svi radnici i vanjski suradnici *Društva* dužni su se pridržavati načela i principa koje propisuje ova Politika te svih ostalih akata koji proizlaze iz Politike informacijske sigurnosti te su obvezni prijavljivati uočene sigurnosne propuste ili incidente.

Nepridržavanje odredbi Politike informacijske sigurnosti te politika, pravilnika, procedura i uputa koje proizlaze iz ove Politike od strane radnika *Društva* smatrat će se povredom ugovora o radu koja može predstavljati razlog za pokretanje disciplinskog postupka, otkaz ugovora o radu skrivljenim ponašanjem radnika ili za izvanredni otkaz ugovora o radu. Nepridržavanje odredbi Politike informacijske sigurnosti te politika, pravilnika, procedura i uputa proizašlih iz ove Politike od strane vanjskih suradnika i partnera smatra se povredom ugovorne obveze koja može biti temelj za raskid ili otkaz ugovora.

3 NAČELA INFORMACIJSKE SIGURNOSTI

Prepoznavanje, procjena, analiza i obrada rizika čine temelj za ispravno funkcioniranje sustava informacijske sigurnosti. Rizik informacijskog sustava se procjenjuje najmanje jednom godišnje kako bi se ustanovile promjene u oblicima prijetnji prema informacijskom sustavu te uzele u obzir promjene u samoj organizaciji. *Društvo* će procjenu i obradu rizika temeljiti na metodologiji koja je u skladu sa zakonskim i regulatornim odredbama, međunarodnim standardima i najboljim svjetskim praksama.

Društvo u svrhu sprječavanja narušavanja povjerljivosti, integriteta i dostupnosti uređuje postupke zaštite informacija i podataka koji se stvaraju, preuzimaju, obrađuju, spremaju ili prosljeđuju resursima informacijskog sustava *Društva* imajući u vidu relevantne zakonske, regulatorne i ugovorne obveze.

Korisnici informacijskog sustava moraju biti upoznati s načinom primjerenog korištenja informacijskog sustava *Društva* kroz dokumentirane upute, metode zaštite i sigurnosne mjere iz svog djelokruga rada. Edukacija se provodi za sve nove i postojeće radnike *Društva* kako bi se osigurali osposobljeni i motivirani radnici te smanjio rizik od krađe, prijevare i zlouporabe resursa informacijskog sustava.

Radi smanjenja negativnog utjecaja na raspodjelu resursa, distribuciju hardvera i softvera i njihovo održavanje, identifikaciju i lociranje imovine te sigurnost informacijskog sustava *Društva* primjereno upravljaju imovinom informacijskog sustava.

Informacijski sustav potrebno je zaštititi na primjeren način te se u tu svrhu vrši adekvatna zaštita osoba, prostora i imovine *Društva*, sprječavanje neovlaštenog fizičkog i logičkog pristupa, oštećenja i ometanja prostora, zaštita informacija u mrežama i pratećoj mrežnoj infrastrukturi te aplikativnim servisima informacijskog sustava.

Upravljanje kontinuitetom poslovanja jedan je od strateških interesa *Društva* kako bi se zaštitili poslovni procesi od većih prekida ili katastrofa te izvršio oporavak uslijed neželjenog događaja u što kraćem vremenu. S tim ciljem *Društvo* će osigurati pouzdanu pričuvnu pohranu ključnih informacijskih resursa, razvit planove i procedure za upravljanje oporavkom od katastrofe i poduzimati sve potrebne mjere kako bi bile spremne pravovremeno i kompetentno odgovoriti na sigurnosne incidente koji mogu pogoditi resurse informacijskog sustava.

Vanjski suradnici *Društva* i relevantne treće osobe koje pristupaju informacijskom sustavu moraju biti upoznati s odredbama ove Politike čime formalno prihvaćaju svoj dio odgovornosti koji se odnosi na očuvanje prihvatljive razine sigurnosti informacijskog sustava.

Kako bi se osiguralo poštivanje i provođenje gore navedenih načela te podržavanje poslovnih ciljeva *Društva* uz efikasno korištenje resursa informacijskog sustava, *Društvo* će upravljati informacijskim sustavom vodeći računa o strateškom usmjerenju *Društva*, uspostavljanjem učinkovitog sustava izvješćivanja te osiguranju sukladnosti sa zakonskim, regulatornim i ugovornim zahtjevima kao i zahtjevima međunarodnih standarda iz domene upravljanja sustavom informacijske sigurnosti.

4 ZAVRŠNE ODREDBE

Ova Politika će biti dostupna svim korisnicima informacijskog sustava *Društva.*

Verzija: 1.0

Datum zadnje izmjene: 25.05.2018.