Na osnovu člana 23. stav 2. Statuta broj: OPU-IP: 1302/2011 od 18.10.2011.godine „Sine Qua Non" Društva za pružanje intelektualnih usluga, zastupanje i zaštitu autorskih prava d.o.o. Sarajevo, Skupština donosi dana 10.10.2011. godine.

# PLAN SIGURNOSTI ZAŠTITE LIČNIH PODATAKA

## I. OSNOVNE ODREDBE

Član 1.

Ovaj opšti akt se donosi u cilju osiguravanja zaštite ličnih podataka uposlenika, spoljnih saradnika i autora koje „Sine Qua Non" Društvo za pružanje intelektualnih usluga, zastupanje i zaštitu autorskih prava d.o.o. Sarajevo koristi u obavljanju svoje registrovane djelatnosti.

Član 2.

Pod „ličnim podacima" u smislu ovog opšteg akta se naročito podrazumjevaju slijedeći podaci:

- ime i prezime,
- pseudonim,
- JMBG odnosno CIPS,
- datum rođenja,
- adresa/prebivališta odnosno boravišta,
- alternativna adresa za dostavu pošte,
- naziv banke kod koje ima otvoren račun,
- broj transakcijskog računa i partija, broj telefona,
- broj fiksnog telefona i mobitela, broj faxa, e-mail adresa,
- državljanstvo,
- IP broj
- WID broj
- ISWC broj
- isplata autorskih naknada/tantijema.
- Plate uposlenika

Član 3.

Lični podaci iz člana 2. čine poslovnu tajnu Društva.

Član 4.

## II. SVRHA

Uspješna zaštita ličnih podataka podrazumijeva niz administrativnih, tehničkih i fizičkih mjera.
Uvažavajući sve principe i standarde upravljanjem podataka, „Sine Qua Non" će kontinuirano riješavati niz otvorenih pitanja u segmentima:
Relevantnosti: Provjeru podataka/informacija bitnih za poslovanje i odlučivanje,
Legalnosti: Osigurati legalnost i etičnost podataka/informacija,
Sigurnosit:Zaštiti podatke/informacije od neovlaštenog pristupa i zloupotrebe.

Član 5.

III. CILJ

Naš cilj, u razvoju i implementaciji ovog sveobuhvatnog pisanog plana informacijske sigurnosti je:
a) Osigurati sigurnost i tajnost ličnih podataka
b) Zaštita od svih predviđenih prijetnji ili opasnosti za sigurnost i integritet takvih informacija
c) Zaštita od neovlaštenog pristupa ili korištenja takvih informacija na način koji stvara znatan rizik od krađe identiteta ili prijevara.

Član 6.

Plan određuje naš postupak za ocjenu elektronske i fizičke metode pristupa, prikupljanja, pohranjivanja, korištenja, prijenosa i zaštite ličnih podataka članova „Sine Qua Non".

Član 7.

U formuliranju i provedbi plana, mi ćemo:

(1) razumno predvidjeti moguće unutarnje i vanjske rizike za sigurnost, tajnost i / ili cjelovitost bilo elektroničkih, papirnih ili drugih zapisa koji sadrže osobne podatke,
(2) procijeniti vjerojatnost i potencijalne štete od tih prijetnji, uzimajući u obzir osjetljivost ličnih podataka,
(3) procjenu dostatnosti postojećih politika, procedure, klijente informacijskih sustava i druge zaštitne mjere na mjestu za kontrolu rizika,
(4) dizajnirati i provesti plan koji stavlja zaštitne mjere kako bi se smanjili ti rizici, u skladu sa zahtjevima
(5) redovito pratiti učinkovitost tih mjera zaštite

Član 8.

Pristup zapisima koji sadržavaju lične informacije će se ograničiti samo na one osobe koje su razumno potrebne znati takve informacije kako bi ostvarili svoje legitimne poslovne svrhe ili bi im se to trebalo omogućiti skladu s drugim državnim propisima.

Član 9.

Sve sigurnosne mjere razmatrat će se najmanje jednom godišnje, ili kad god ima bitnih promjena u našim poslovnim praksama kojima se opravdano može implicirati sigurnost ili integritet zapisa koji sadrži lične podatke. Koordinator za zaštitu podataka mora biti odgovoran za ovaj pregled, te će u potpunosti obavijestiti o upravljanju rezultatima pregleda i svim preporukama za poboljšane sigurnosti koji proizlaze iz tog pregleda.

Član 10.

IV. FIZIČKA SIGURNOST

Fizička zaštita sale IS-a se ostvaruje najjednostavnije kontrolom:

- pristupa server sali,
- ulaska u server salu.

Zaštita mrežne infrastrukture

Kada govorimo o nivou mrežne infrastrukture ona podrazumjeva fizičku zaštitu ,tj. zabranu pristupa ili bar, kontrolu pristupa mrežnoj infrastrukturi koju čine kablovi i mrežni uređaji:

- HUB-ovi,
- switch-evi,
- router-i.

Član 11.

Prestankom rada zaposlenika, moraju se vratiti svi zapisi koji sadrže lične podatke u bilo kojem obliku, da mogu u vrijeme takvog raskida biti u posjedu bivšeg zaposlenika (uključujući sve kao informacije pohranjene na prijenosnim računalima ili drugim prijenosnim uređajima i medijima, datotekama, evidencijama, papirima, itd.).
Prestankom rada zaposlenika fizički i elektronski pristup do ličnih podataka moraju biti odmah blokirani. Takav zaposlenik je dužan predati sve tipke, pristupne kodovi ili značke, posjetnice i sl., koji omogućuju pristup prostorijama ili informacijama društva.
Štoviše, takavom zaposleniku daljinski elektronički pristup ličnim podacima mora biti onemogućen, njegov / njezin voicemail pristup e-pošti, pristup internetu, i lozinci mora biti poništen. Koordinator za zaštitu podataka mora voditi vrlo osiguran glavni popis svih kombinacija za zaključavanje, lozinki i ključeva.

Član 12.

Elektronički pristup identifikacije korisnika, nakon više neuspješnih pokušaja da se dobije pristup mora bti blokiran.Trenutačnom radniku user-ID i zaporke je potrebno povremeno promijeniti. Pristup ličnim podacima mora se ograničiti samo aktivnim korisnicima i aktivnim korisničkim računima. Zaposlenici se potiču da prijave svako sumnjivo ili neovlašteno korištenje korisničkih informacija. Zaposlenicima je zabranjeno držanje otvorene datoteke koje sadrže lične podatke na svojim radnim stolovima kad nisu na svojim radnim stolovima. Na kraju radnog dana, sve datoteke i druge evidencije koje sadrže lične podatke moraju biti osigurane na način koji je u skladu s planom o pravilima za zaštitu sigurnosti ličnih informacija. Svaki odjel će izraditi pravila (imajući u vidu poslovne potrebe tog odjela) da bi se osiguralo da se razumna ograničenja o fizičkom pristupu zapisa koji sadrže lične informacije nalaze se na mjestu.

Član 13.

V. INFORMACIJSKA SIGURNOST

Opsežan sistem informacijske sigurnosti podrazumijeva:
- Pristup elektroničkim pohranjenim ličnim podacima će elektronski biti ograničen na one
- Zaposlenike koji imaju jedinstveni ID log-in, i re-log-in će biti potreban kada je računalo

neaktivno za više od nekoliko minuta.

Član 14.

Mora postojati up-to-date firewall zaštita i operativni sustav sigurnosne zakrpe, razumno osmišljeni kako bi očuvali integritet ličnih podataka, instaliran na svim sistemima obrade ličnih podataka.

Član 15.

U mjeri u kojoj je to tehnički izvedivo, svi lični podaci pohranjeni na laptop ili drugi prijenosni uređaj moraju biti kodirani, jer moraju svi podaci i datoteke koje se prenose preko javne mreže ili bežično biti zaštićeni.

Član 16.

Svi računalni sistemi moraju se pratiti u slučaju neovlaštenog korištenja ili pristupa ličnim informacijama. Posjetitelju neće biti dozvoljeno da posjeti bez pratnje bilo koje područje unutar naših prostora koji sadrži lične podatke. Papir ili elektronički zapisi (uključujući zapise pohranjene na tvrdom disku ili drugim elektronskim medijima) koji sadrži lične podatke odlagati će se samo na način koji u skladu s pozitivnim propisima.

Član 17.

Ovaj akt stupa na snagu danom donošenja.

Datum: 10.10.2011.

Broj: 1624/11

PREDSJEDNICA UPRAVE

Amela Hadrović - Hasanefendić