E-Smart Systems d.o.o.
Privredno društvo za projektovanje, razvoj, proizvodnju, trgovinu i implementaciju u oblasti informacionih tehnologija
Republika Srbija, 11030 Beograd, Kneza Višeslava 70a, Tel: + 381 11 30 50 200 Fax: +381 11 30 50 222,
http://www.e-smartsys.com office@e-smartsys.com
Mat. broj: 17247565 , Reg. broj: 01117247565 , Šif. delatnosti: 6201, PIB: 101833141

L-IMS-008
Šifra dokumenta

Politika bezbednosti informacija Društva E-Smart Systems d.o.o.

U Društvu E-Smart Systems d.o.o. Beograd informacije predstavljaju osnovu svih poslovnih procesa. Za Društvo, bezbednost informacija znači sprečavanje neovlašćenog pristupa, otkrivanja, modifikacije, uništenja ili nedostupnosti informacija.

Osnovni ciljevi naših napora vezanih za obezbeđenje bezbednosti informacija su:

- održavanje poverenja u poslovnim odnosima,
- zaštita prava na privatnost ličnih podataka,
- obezbeđenje poslovnih operacije
- potpuna usklađenost sa primenjivim zakonima, propisima i standardima iz domena bezbednosti, internim politikama bezbednosti informacija kao i potrebama najšire društvene zajednice
- tretman rizika i primena bezbednosnih kontrola na optimalnom nivou troška i u skladu sa poslovnom vrednošću
- Kontinualno unapređenje sistema upravljanja bezbednošću informacija, kako na tehnološkom, tako i na organizacionom nivou

Postavljene ciljeve planiramo, iskazujemo, sprovodimo, pratimo, merimo stepen njihovog ostvarenja i stalno ih usaglašavamo sa nastajućim promenama u okruženju i okviru poslovanja Društva.

Osnovni principi u primeni bezbednosti informacija u okviru poslovanja Društva su:

- očuvanje poverljivosti, integriteta, dostupnosti, autentičnosti svih informacija od značaja za poslovanje Društva i neosporivosti obrade izvršene nad njima
- bezbedno prikupljanje, obrada, čuvanje i izlučivanje svi informacija proisteklih iz poslovanja sa posebnom pažnjom posvećenom ličnim podacima svih učesnika
- jasno komuniciranje svih zahteva vezano za bezbednost informacija svim zainteresovanim stranama
- pravovremena i efektivna identifikacija, procena i tretman rizika iz domena informacione bezbednosti
- proaktivno praćenje izmena primenjivih zakona, propisa i standarda iz domena bezbednosti i blagovremeno usaglašavanje sa istim
- izbor pouzdanih i proverenih tehnologija za implementaciju bezbednosnih kontrola u informacionom sistemu Društva u skladu sa tehnološkim trendovima i preporučenom praksom

Svi zaposleni Društva od najvišeg rukovodstva do novozaposlenih su u obavezi da:

- se strogo pridržavaju principa primene bezbednosti informacija navedenim u ovoj politici,
- svakodnevno razvijaju i šire svest i znanja iz domena bezbednosti informacija
- učestvuju na obukama, treninzima i proverama znanja iz ove oblasti
- savesno postupaju u svakodnevnom radu u skladu sa ovom politikom i
- pravovremeno prijavljuju incidente i događaje povezane sa bezbednošću informacija

Najviše rukovodstvo Društva je u potpunosti posvećeno kontinualnom unapređenju sistema upravljanja bezbednošću informacija i zbog toga je ISO/IEC 27001 izabran kao okvir za implementaciju. U skladu sa tim sve

interne politike i procedure, evaluacija rizika i primenjene bezbednosne kontrole se preispituju i ažuriraju minimalno jednom godišnje. Svi zaposleni se stoga podstiču da učestvuju u internim i eksternim proverama kao i u radu stručnih foruma i organizacija iz domena bezbednosti informacija.

Na nivou Društva uspostavljena je, već više od deceniju, uloga Predstavnika rukovodstva za bezbednost informacija. Ovoj ulozi delegirane su odgovornosti i pun izvršni autoritet iz ovog domena. Najviše rukovodstvo kroz ovu ulogu aktivno upravlja sistemom bezbednosti informacija i dosledno radi na njenom ojačavanju. Najviše rukovodstvo Društva zadržava punu odgovornost za donošenje odluka vezanih za postavljanje ciljeva, tretmana rizika i promene politika iz domena informacione bezbednosti.

Shodno da informacije predstavljaju osnov poslovanja Društva, sve informacije vezane za poslovanje su predmet primene ove politike, bez izuzetaka i odstupanja. U slučaju nastajanja potrebe/zahteva za izuzetkom, isti mora biti jasno komuniciran sa PRBI i najvišim rukovodstvom, u cilju pronalaženja adekvatnog rešenja.

Odstupanja od ove politike u svakodnevnom radu nisu dozvoljena, a svaka povreda bezbednosti informacija biće smatrana povredom radne obaveze i sankcionisana u skladu sa Pravilnikom o radu i prema proceduri za utvrđivanje disciplinske odgovornosti.

Istorija promena:

Verzija	Datum	Opis promena
1.0	01.07.2011.	Prva verzija dokumenta
2.0	08.02.2013.	Dokument prilagođen praksama rada
3.0	01.07.2014.	Politika usaglašena sa zahtevima standarda ISO/IEC 27001:2013
4.0	06.02.2020,	Promenjen template dokumentacije
5.0	02.03.2020.	Politika ažurirana usled otvaranja ZelenData Centra
6.0	07.02.2024.	Politika usaglašena sa zahtevima standarda ISO/IEC 27001:2022
6.1	08.04.2024.	Dodata Istorija promena i oznaka nivoa poverljivosti

Potpisi:

Mirna Kojić Veljović
ESUFL001372703191
Digitally signed by Mirna Kojić Veljović ESUFL001372703191
Date: 2024.03.29 11:52:49 +01'00'

Srećko Atanasković
ESUPL0000000000 27-2402962870013
Digitally signed by Srećko Atanasković ESUPL000000000027-2402962870013
Date: 2024.03.29 13:49:55 +01'00'