Sistem upravljanja varovanja informacij (SUVI) je integralni del sistema vodenja družbe Komunala Novo mesto d.o.o. Z vzpostavljanjem SUVI stopamo na pot sistematičnega in celovitega pristopa k varovanju informacij, kar pa ne pomeni, da to ni bilo že dosedaj vgrajeno v naše delovanje. Kot podlago za SUVI prevzemamo mednarodna standarda:

- ISO/IEC 27001:2013 lnformacijska tehnologija - Varnostne tehnike - Sistemi upravljanja informacijske varnosti – Zahteve,
- ISO/IEC 27002:2013 lnformacijska tehnologija - Varnostne tehnike - Pravila obnasanja pri nadzoru informacijske varnosti.

Pri tem se naslanjamo tudi na druge dobre prakse in tehnološke dosežke na področju varovanja informacij. S SUVI zagotavljamo podlage za skladnost poslovanja z regulatornimi zahtevami, kot so:

- Zakon o varovanju osebnih podatkov - uradno prečiščeno besedilo (ZVOP-1-UPB, ULRS 94/2007),
- Zakon o varovanju osebnih podatkov 2 (podlaga Splošna uredba o varstvu podatkov; *angl*. General Data Protection Regulation – GDPR), ki je začela veljati 25.5.2016, njene določbe pa bomo morali uporabljati s 25. 5. 2018 v vseh državah članicah,
- Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP, ULRS 57/2000),
- Zakon o gospodarskih družbah (ZGD-1, ULRS 42/2006 z vsemi dopolnitvami).

POLITIKA VAROVANJA INFORMACIJ

Namen SUVI je varovanje informacijskih sredstev oziroma informacijskega sistema naše družbe pred grožnjami, ki lahko vplivajo na zaupnost, integriteto in razpoložljivost. Grožnje prepoznavamo kot notranje ali zunanje ter namerne ali nenamerne. Integriteta informacijskega sistema in varnost informacij sta ključni za uspešnost in trajnost delovanja naše družbe. To od nas pričakujejo tudi partnerji, odjemalci.

Uspešnost in trajnost delovanja naše družbe gradimo na kakovosti in zaupanju. Nanju pomembno vpliva varnost informacijskega sistema in informacij. Njihovo nepooblaščeno razkritje, nedostopnost ali celo izguba lahko predstavljajo neposredno poslovno škodo in izgubo ugleda. Zato vodstvo družbe podpira in zagotavlja potrebne vire za varovanje informacij.

Politika varovanja informacij obsega:

- Razvrščanje informacijskih sredstev glede na raven zaščite, ki jo potrebujejo.
- Varovanje informacij pred nepooblaščenim dostopom.
- Zagotavljanje zaupnosti in neokrnjenosti informacij.
- Upoštevanje varnostnih zahtev v zvezi z zaposlenimi.
- Upravljanje fizičnega in logičnega varovanja informacijskih sredstev ter prostorov.
- Upoštevanje zakonskih in drugih predpisov ter pogodbenih zahtev.
- Upoštevanje življenjskega cikla sistemov pri njihovem razvoju, uvedbi in vzdrževanju.
- Zagotavljanje neprekinjenega poslovanja.
- Ozaveščanje vseh zaposlenih o ukrepih in novostih na področju varovanja informacij.
- Nadzor delovanja in uporabe informacijskih sredstev.
- Upravljanje incidentov na področju varovanja informacij.
- Sankcioniranje kršitev Politike varovanja informacij.

Politiko varovanja informacij udejanjamo s postopki in navodili, ki natančneje opredeljujejo njene posamezne vidike, npr. sprejemljiva raba elektronske pošte, zaščita proti zlonamerni kodi, izdelovanje varnostnih kopij podatkov, upravljanje identitet uporabnikov, politika čiste mize, načrt neprekinjenega poslovanja in podobno.

V njih so smiselno in glede na posamezno področje opredeljene vloge, odgovornosti in postopki za:

- vodstvo družbe,
- odgovorno osebo za področje varovanja informacij,
- lastnike podatkov in procesov,
- dobavitelje in ponudnike tehnologij,
- uporabnike,
- notranje presojevalce oz. revizorje informacijskih sistemov in
- stranke ter druge zainteresirane strani.

V družbi smo imenovali odgovorno osebo za varovanje informacij.

V skladu s sprejetimi dokumenti in zavezami v sklenjenih pogodbah s kupci in dobavitelji smo dolžni politiko varovanja informacij upoštevati vsi zaposleni in posredno tudi naši pogodbeni partnerji.

Datum: 12. maj 2018

Gregor Klemenčič
direktor