

Kranj, 14.03.2019

POLITIKA VAROVANJA INFORMACIJ

Ključni cilj naše organizacije pri ponudbi celovitih projektov in tehnoloških rešitev je s kakovostnimi, zanesljivimi ter varnimi produkti in storitvami nenehno izpolnjevati pričakovanja in zahteve naših naročnikov ter v vseh pogledih opravičevati njihovo zaupanje.

Informacije in sistemi informacijske tehnologije so bistvena komponenta poslovanja naše organizacije ter glede na naravo našega dela tudi pomembna podpora poslovnih procesov naših poslovnih partnerjev. Ker so informacije, programska in strojna oprema predmet potencialnih in realnih groženj, kriminala, sabotaž ter drugih odpovedi in nesreč, smo v družbi opredelili temeljna načela in cilje politike varovanja informacij, ki jih spoštujemo ter na vseh nivojih uveljavljamo vsi sodelavci:

- Vzdržujemo varnost aplikacijske systemske programske opreme in informacij, pravilno in varno obratovanje naprav za procesiranje informacij v organizaciji, informacijskih sredstev, ki so dostopna tretjim strankam ter integriteto in razpoložljivost procesiranja informacij in komunikacijskih storitev. Vpeljan in redno testiran je Plan neprekinjenega poslovanja in v njegovem okviru tudi plan okrevalnega načrta
- Varujemo zaupnost, celovitost in razpoložljivost informacij in programske opreme, omrežnih storitev podporne infrastrukture. Kritične poslovne procese varujemo pred učinki večjih napak in nesreč.
- Zagotavljamo primerno raven varovanja informacij in informacijskih sredstev, oziroma dostopa do njih. To načelo velja tudi v primerih, ko gre za zagotavljanje informacijske varnosti pri vodenju IT projektov in podpornih aktivnosti, pri uporabi prenosnih računalnikov in naprav za delo na daljavo. Prav tako zagotavljamo popolno protivirusno zaščito za vsa informacijska sredstva v organizaciji.
- Preprečujemo nepooblaščen dostop do računalnikov in informacij v informacijskih sistemih, škodo in motnje v poslovnih prostorih in poslovnih informacijah, izgubo, poškodovanje ali zlorabo sredstev in prekinitve poslovnih aktivnosti, zlorabo, ali tatvino informacij ter naprav za procesiranje informacij, poškodovanje sredstev in prekinitve poslovnih dejavnosti, nepooblaščne modifikacije ali zlorabo informacij, ki se izmenjujejo med organizacijami, izgubo, spremembe ali zlorabo uporabnikovih podatkov v aplikacijskih sistemih.
- Zmanjšujemo tveganje človeških napak, kraje, prevare, ali zlorabe naprav, škodo varnostnih incidentov in okvar, in se iz njih učimo. V ta okvir sodi tudi odkrivanje nepooblaščenih dejavnosti. Vse varnostne incidente skrbno preučimo in po potrebi z njimi seznanimo vse zaposlene.
- Izogibamo se kršitvam katerekakoli od kazenskih in civilnih zakonov, statutarnih, zakonskih, ali pogodbenih obvez, in katerekoli od varnostnih zahtev.
- Izobražujemo vse uporabnike informacijskega sistema tako, da se uporabniki zavedo groženj informacijski zaščiti, da skrbijo za varnost informacij in so usposobljeni, da med svojim vsakodnevnim delom podpirajo varnostno politiko organizacije.

Opređeljena načela predstavljajo usmeritve in podporo vzpostavljenemu sistemu vodenja varovanja informacij (Information security management systems - ISMS), ki je skladen z zahtevami standardov družine ISO/IEC 27000. Sistem redno pregledujemo z notranjimi revizijami, oz. z revizijami certificiranih institucij, s čimer zagotavljamo skladnost sistema z varnostno politiko in z navedenimi standardi.

Direktor

Janko Štefančič