



BEZBEDNOSNA KULTURA I SVEST

Bezbednosna aktivnost koja izražava spremnost delovanja i ponašanja u skladu sa stečenim znanjima i veštinama, kao i u skladu sa prihvaćenim vrednosnim stavovima. Ogleda se u prepoznavanju opasnosti, reagovanju na njih izbegavanjem opasnosti, otklanjanjem opasnosti ili upućivanjem na one subjekte koji će profesionalno reagovati i sačuvati ugrožene vrednosti.

Znanje i stav koji članovi organizacije imaju u pogledu zaštite određenih vrednosti – nacionalne bezbednosti, odbrane, unutrašnjih i spoljnih poslova, ljudskih sloboda i prava, kao i fizičke i intelektualne imovine, a posebno informacija i podataka kojima raspolaže organizacija (organ javne vlasti, pravno lice ili kompanija).

INFORMACIONA KULTURA I SVEST

Praksa osiguranja informacija i upravljanja rizicima vezanim za upotrebu, obradu, skladištenje, prenos i arhiviranje informacija. Informaciona kultura i svest uključuje zaštitu integriteta, dostupnosti, autentičnosti, nepovršenosti i poverljivosti korisnika. Obuhvata i digitalne zaštite i fizičke tehnike.

Usvajanje adekvatnog ponašanja da se pronađu informacije, koristeći pritom bilo koji način ili medijum, koji na najbolji mogući način zadovoljava potrebe za informacijama, a koje vode mudrom i etičkom korišćenju informacija u društvu (digitalna pismenost?).

INFORMACIONO BEZBEDNOSNA KULTURA I SVEST

Deo u razvoju informacione bezbednosti koja se fokusira na prikupljanje saznanja i iskustava u vezi sa potencijalnim rizicima i pretnjama koje se brzo razvijaju, u vezi sa ljudskim ponašanjem, kako korisnika IKT sistema, tako i potencijalnih napadača.



Manifestije se u okviru organizacije kroz aspekte bezbednosti koji se odnose na:

- 1) vrednosti; 2) ponašanje; 3) stavove; 4) akcije; 5) aktivnosti rukovodstva (mendžmenta); i
- 6) fizičko okruženje.

ORGANIZACIONA KULTURA I SVEST

- Sistem zajedničkih značenja i simbola.
- Model osnovnih pretpostavki, vrednosti i normi, koje je data grupa razvila ili otkrila učeći kako da rešava probleme eksterne adaptacije i intarne integracije i koji funkcionišu dovoljno dobro da bi bili preneti novim članovima organizacije kao ispravan način mišljenja i osećanja u vezi sa tim problemima.
- Obrazac verovanja, vrednosti i naučenih načina postupanja sa iskustvom koji su se razvili kroz organizacionu istoriju i koji se manifestuju kroz materijalne objekte, kao i ponašanje članova organizacije.

SAJBER HIGIJENA

- Reč je o bezbednosnoj praksi koja uključuje sve korisnike interneta, i sa internetom poveza nih stvari, servisa, aplikacija, i uređaja sa ciljem zaštite sigurnosti i integriteta štićenih podataka i sprečavanja sajber napada.
- Odnosi se na prakse koje imaju za cilj sprečavanje infekcije malicioznim sofverom (malware), kao i sajber upade i gubljenje ili korupmiranje podataka i održavanje zdravog sajber okruženja.

**KANCELARIJA SAVETA ZA NACIONALNU BEZBEDNOST
I ZAŠTITU TAJNIH PODATAKA**

e-mail: office@nsa.gov.rs, kontakt@nsa.gov.rs

web: www.nsa.gov.rs