Ovim dokumentom Visoko sudbeno i tužiteljsko vijeće Bosne i Hercegovine (u daljnjem tekstu: VSTV) iskazuje svoje temeljno opredjeljenje za upravljanje sigurnošću informacija i upravljanje informacijsko-komunikacijskim (u daljnjem tekstu: IKT) servisima VSTV-a. Ova politika se prvenstveno primjenjuju na zaposlene u VSTV-u, a posredno, kroz pozitivne propise i interna akta, i na sve korisnike pravosudnog informacijskog sustava i IKT servisa VSTV-a, druge institucije s kojima VSTV razmjenjuje informacije, kao i na dobavljače i ostale posredne sudionike u poslovnim procesima VSTV-a u opsegu i kontekstu utjecaja na sposobnost zaštite ili mogućnost narušavanja povjerljivosti, dostupnosti i integriteta informacija koje se pojavljuju u opsegu Integriranog sustava upravljanja (u daljem tekstu: ISU).

Politika sigurnosti informacija i upravljanja informacijsko-komunikacijskim servisima Visokog sudbenog i tužiteljskog vijeća Bosne i Hercegovine

VSTV se opredjeljuje za uspostavu i primjenu ISU sukladno zahtjevima međunarodnih standarda ISO 27001 i ISO 20000-1, čijom primjenom se kontinuirano i trajno osigurava povjerljivost, integritet i dostupnost informacijske imovine, kao i kvaliteta IKT servisa koje VSTV pruža svojim korisnicima.

Pod informacijskom imovinom koja je predmet zaštite podrazumijevaju se:

- Informacije korisnika usluga koje se nalaze u sustavima koje VSTV uspostavlja i održava;
- Informacije dobivene od strane korisnika usluga tijekom realiziranja poslovnih procesa VSTV-a;
- Informacije kreirane od strane VSTV-a i informacije u vlasništvu VSTV-a;
- Informacije dobivene od partnera i dobavljača VSTV-a;
- Svi drugi resursi neophodni za obradu informacija potrebnih za pružanje usluga klijentima i korisnicima.

Uspostavom Politike sigurnosti informacija i upravljanja IKT servisima VSTV se obvezuje da:

- Kontinuirano štiti informacije kojima se pristupa tijekom realizacije procesa VSTV-a u oblastima:
  - zaštite od neovlaštenog pristupa informacijama,
  - održavanja povjerljivosti informacija,
  - zaštite od otkrivanja informacija neovlaštenim osobama, namjerno ili nenamjerno,
  - očuvanja integriteta informacija zaštitom od neovlaštenih izmjena i
  - osiguravanja kontinuirane dostupnosti informacija ovlaštenim osobama;
- Osigurava visoku dostupnost IKT servisa, sukladno definiranom katalogu i planu servisa;
- Kontinuirano ispunjava ugovorne, zakonske i regulatorne zahtjeve, posebno u pogledu očuvanja povjerljivosti osobnih informacija i drugih kritičnih informacija;
- Provodi odgovarajuće programe podizanja svijesti o informacijskoj sigurnosti sa zaposlenima i, gdje je to primjenljivo, drugim zainteresiranim stranama;
- Prijavljuje, istražuje i pravodobno reagira na sve povrede i sumnjive aktivnosti vezane za sigurnost informacija;
- Identificira, odgovarajućom procjenom rizika, vrijednost informacijske imovine, razumije njenu ranjivost i prijetnje koje je mogu izložiti riziku, te upravlja rizicima visoke razine kako bi se sveli na prihvatljivu razinu kroz dizajniranje, implementaciju i održavanje kontrola za smanjenje rizika;
- Održava i testira planove kontinuiteta poslovanja;
- Ispuni zahtjeve važećih verzija ISO/IEC 27001 i ISO/IEC 20000-1 standarda, te stekne i održava certifikaciju implementiranog sustava, uz kontinuiran rad na stalnom unaprjeđenju sustava.