УПРАВА ЗА ЗАЈЕДНИЧКЕ ПОСЛОВЕ РЕПУБЛИЧКИХ ОРГАНА

ПОЛИТИКА БЕЗБЕДНОСТИ ИНФОРМАЦИЈА

Намена имплементираног система управљања безбедношћу информација је да обезбеди неометано пословање, заштиту поверљивих информација без обзира на њихов облик, развој организације, као и подизање задовољства корисника пруженим услугама и квалитетом саме услуге. Циљ безбедности информација је да се обезбеди и заштити информациона имовина организације од свих унутрашњих или спољашњих, намерних или случајних претњи, кроз успостављање, имплементацију, примену, праћење, преиспитивање, одржавање и побољшање ISMS као дела интегрисаног менаџмент система, а у складу са захтевима ISO 27001.

Ова политика представља оквир за успостављање циљева безбедности информација и обезбеђује и гарантује:

- Континуирано побољшање пословања и примену савремених информационих решења,
- Одржавање поверљивости информација,
- Омогућавање приступа информацијама које су потребне за пружање услуга и извођење пословних активности,
- Спречавање неовлашћеног приступа информацијама, редовну заштита података, софтвера и мрежне инфраструктуре,
- Очување интегритета информација кроз контролу приступа и привилегије корисника који им приступају,
- Ограничење приступа наших испоручиоца информацијама које се могу сматрати поверљивим,
- Континуирано стручно усавршавање и оспособљавање запослених кроз обуке и едукацију,
- Документовање, праћење и анализу инцидената свих повреда безбедности информација,
- Развијање и имплементацију планова континуитета пословања,
- Усаглашеност са свим примењивим законским, регулаторним и уговорним обавезама.

Руководство Управе за заједничке послове републичких органа је посвећено сталном унапређењу система управљања безбедношћу информација и обезбедиће да ова политика буде дистрибуирана и објашњена свим запосленима и заинтересованим странама, имплементирана и редовно ревидирана како би се континуирано проверавала прикладност. Управа за заједничке послове републичких органа ће најмање једном годишње спровести преиспитивање од стране руководства како би се обезбедила погодност, адекватност и ефективност политике, као и остале документације система безбедности информација. Сви запослени су дужни да се придржавају процедура и правила која су дефинисана овом политиком и другом документацијом система управљања безбедношћу информација. Запослени морају бити свесни својих одговорности у случају да дође до нарушавања безбедности информација као и целокупног ИТ система.

Београд, 20.11.2020. године

в.д. директора Дејан Матић