



ПЛАН ЗАШТИТЕ ТАЈНИХ ПОДАТАКА У ОРГАНУ ЈАВНЕ ВЛАСТИ

План заштите тајних података у органу јавне власти је кључни документ организационе безбедности који дефинише све мере и поступке заштите тајних података које орган поседује или обрађује. Као такав, он је пресудан за очување интегритета информација и националне безбедности. План има за циљ да осигура да се тајни подаци обрађују, чувају, преносе и уништавају у складу са највишим стандардима безбедности. Он је основни стуб организационе безбедности у сваком органу јавне власти. Омогућава правилно управљање тајним подацима и осигурава њихову заштиту, што је од кључног значаја за очување националне безбедности.

ОСНОВНИ ЕЛЕМЕНТИ ПЛАНА УКЉУЧУЈУ:

- Одређивање одговорних лица:** У плану се дефинишу особе које су одговорне за одређивање тајних података, руковалац тајних података, као и лице одговорно за вршење унутрашње контроле. Такође, ова лица су одговорна и за надзор над поступцима заштите тајних података и примењивање мера у складу са изменама у законодавству и технологији.
- Процедуре:** План укључује процедуре за правилно одређивање степена тајности података у складу са законом (интерно, поверљиво, строго поверљиво, државна тајна), као и одређивање начина обраде, чувања и уништавања тајних података, и безбедносне мере које се предузимају при сваком кораку.
- Процена ризика за рад са тајним подацима:** У оквиру израде и редовног ажурирања плана заштите тајних података, орган јавне власти мора редовно вршити процену ризика који угрожавају безбедност тајних података. Процена ризика укључује све потенцијалне претње, као што су напади на информационе системе, злоупотреба приступа или лоша примена мера заштите, као и процену њиховог утицаја на безбедност и интегритет података.
- Мере физичке, техничке и организационе заштите:** Описују се методе које се примењују за безбедност простора у којима се чувају тајни подаци, као и заштита ИКТ система који обрађују тајне податке. Ово укључује физичке баријере, као што су ограде и приступне контроле, као и технолошке мере, као што су криптовање података, двострука аутентификација и безбедносни протоколи за комуникацију.
- Акредитација ИКТ система:** ИКТ системи који обрађују тајне податке морају бити акредитовани од стране Министарства одбране у вези са технолошким аспектима и крипто опремом. Канцеларија Савета за националну безбедност и заштиту тајних података врши безбедносну акредитацију тих ИКТ система како би се осигурало да су у складу са највишим безбедносним стандардима.
- Обука и свест:** План предвиђа обуку свих запослених који имају приступ тајним подацима, како би били упознати са својим обавезама у вези са заштитом тајних података, као и са најновијим претњама и методама одбране. Обука се редовно ажурира како би одражавала нове изазове у области безбедности информација.



ПЛАН ЗАШТИТЕ ТАЈНИХ ПОДАТАКА У ОРГАНУ ЈАВНЕ ВЛАСТИ

- 7. Санкције за кршење заштите:** Планирање санкција у случају неовлашћеног приступа или откривања тајних података. Санкције се односе на кршења правила рада са тајним подацима, било да се ради о физичким просторима или ИТ системима.
- 8. План поступања у ванредним ситуацијама:** Обухвата процедуре и мере које треба предузети у случају напада, злоупотребе или другиј ванредних ситуација које угрожавају безбедност података.
- 9. Праћење стања сертификата:** Обухвата праћење издатих сертификата за физичка и правна лица, укључујући проверу ваљаности сертификата у контексту њиховог приступа тајним подацима.
- 10. Рад са правним лицима:** Управа и сарадња са правним лицима код поверљивих набавки, посебно у области индустријске безбедности, који укључују безбедност информација и технологија у производним и сервисним процесима.
- 11. Евиденције:** Орган јавне власти мора водити евиденције о одређеним степенима тајности, приступу тајним подацима, обуци запослених, инцидентима везаним за безбедност, ревизијама безбедносних мера и уништавању тајних података.
- 12. Ажурирање плана:** Напомена је да се донети план заштите тајних података мора редовно ажурирати у складу са изменама и допунама прописа, технолошких стандарда, научених лекција у раду са тајним подацима и новонасталим претњама и ризицима за рад са тајним подацима.

Обавезе које произилазе из Плана:

- 1. Усаглашеност са стандардима безбедности:** Обавеза органа да се усагласи са националним и међународним стандардима у области информационе безбедности, посебно у области безбедности ИТ система који обрађује тајне податке.
- 2. Хоризонтална и вертикална координација:** Планирање и примена мера заштите тајних података подразумева сарадњу између различитих нивоа руковођења и сектора унутар органа јавне власти. Хоризонтална координација обухвата размену информација и униформну примену мера безбедности међу различитим секторима, док вертикална координација осигурава јасну подршку и надзор руковођења.



ПЛАН ЗАШТИТЕ ТАЈНИХ ПОДАТАКА У ОРГАНУ ЈАВНЕ ВЛАСТИ

- 3. Обавезна обука:** Редовна обука запослених који имају приступ тајним подацима, како би се осигурало да су сви усклађени са најновијим мерама и процедурама. Континуирана комуникација између органа јавне власти и свих учесника у процесу заштите тајних података је од изузетног значаја. Обука свих запослених треба укључивати не само прављење и примену плана, већ и разумевање свих аспеката ризика и координације у оквиру органа јавне власти.
- 4. Систем мониторинга и ревизије:** Систем за праћење и ревизију који осигурава да се све мере заштите примењују на адекватан начин. Ревизија и ажурирање плана у складу са новим претњама, технолошким напредцима и променама у законодавству.

План заштите тајних података није директно прописан Законом о тајности података, али се он се сматра имплицитно обавезним као део комплетног система заштите тајних података, који обједињује све мере и процедуре заштите тајних података у органу јавне власти и који мора бити у складу са важећим законима и прописима, како о тајности података, тако и о информационој безбедности и канцеларијским пословањем, као и одговарајућим секторским (ресорним) прописима у складу са надлежностима и пословима које обавља орган јавне власти.

НАПОМЕНА : СВЕ МОДЕЛЕ ОБРАЗАЦА, ОДЛУКА И ЕВИДЕНЦИЈА КОЈЕ СУ САСТАВНИ ДЕО ПЛАНА ЗАШТИТЕ ТАЈНИХ ПОДАТАКА МОЖЕТЕ ПРОНАЋИ НА САЈТУ КАНЦЕЛАРИЈЕ САВЕТА ЗА НАЦИОНАЛНУ БЕЗБЕДНОСТ И ЗАШТИТУ ТАЈНИХ ПОДАТАКА

 **Модели образаца, одлука и евиденција**

**КАНЦЕЛАРИЈА САВЕТА ЗА НАЦИОНАЛНУ БЕЗБЕДНОСТ
И ЗАШТИТУ ТАЈНИХ ПОДАТАКА**

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

web: www.nsa.gov.rs