ПОЈМОВНИК О РАДУ СА ТАЈНИМ ПОДАЦИМА

1. **Административна безбедност** је адекватна и ефикасна класификација и заштита званичних информација које захтевају заштиту у интересу националне безбедности као и њихова декласификација када више не захтевају заштиту.

2. **Административна зона** је простор или просторија у којој се обрађују и чувају тајни подаци степена тајности „ИНТЕРНО".

3. **Акредитација икт система** подразумева да 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

4. **Активирање containment мера:** Ове мере подразумевају брзу реакцију како би се инцидент изолово и спречило даље ширење оштећења.

5. **Алармни уређаји** су уређаји који служе за обезбеђивање објекта и предмета, тако што звучним или светлосним сигналом упозоравају на недозвољену активност. Могу бити механички, електрични и електронски.

6. **Апсолутне сметње (непосредни разлог за ускраћивање сертификата)** - Ово су здравствени проблеми који аутоматски дисквалификују особу, јер представљају трајан или тежак ризик по безбедност.

7. **Архивска грађа** јесте целина докумената или записа насталих или примљених деловањем и радом субјеката у изворном или репродукованом облику документа, без обзира на форму и формат бележења, као и прописане евиденције о њему.

8. **Аутентичност** је својство које значи да је могуће проверити и потврдити да је податак створио или послао онај за кога је декларисано да је ту радњу извршио.

9. **Аутентификација** – процес верификације идентитета корисника, система или уређаја пре одобравања прступа тајним подацима.

10. **Ауторизација** – процес одређивања права и привилегија корисника након успешне аутентификације.

11. **Accountability („одговорност и праћење поступања")** – свако лице које рукује тајним подацима мора бити у потпуности одговорно за своје поступке у вези са тим подацима, а орган је у обавези да обезбеди систем надзора, праћења и евидентирања активности.

12. **Безбедносна акредитација** - обухвата физичку и административну заштиту података, као што су контрола приступа, обука запослених и примена мера заштите. Спроводи је Канцеларија Савета за националну безбедност и заштиту тајних података и друге институције, у зависности од врсте система.

13. **Безбедносна зона I степена** је простор или просторија у којој се обрађују и чувају тајни подаци степена тајности „ДРЖАВНА ТАЈНА", „СТРОГО ПОВЕРЉИВО" и „ПОВЕРЉИВО". Самим уласком у ову зону сматра се да је остварен приступ тајним подацима.

14. **Безбедносна зона II степена** је простор или просторија у којој се обрађују и чувају тајни подаци степена тајности „ДРЖАВНА ТАЈНА", „СТРОГО ПОВЕРЉИВО" и „ПОВЕРЉИВО".

15. **Безбедносна култура** је безбедносна активност која изражава спремност деловања и понашања у складу са стеченим знањима и вештинама, као и у складу са прихваћеним вредносним ставовима. Огледа се у препознавању опасности, реаговању на њих избегавањем опасности, отклањањем опасности или упућивањем на оне субјекте који ће професионално реаговати и сачувати угрожене вредности.

16. **Безбедносна провера** је поступак који пре издавања сертификата за приступ тајним подацима спроводи надлежни орган, у циљу прикупљања података о могућим безбедносним ризицима и сметњама у погледу поузданости за приступ тајним подацима.

17. **Безбедносна свест** подразумева знање и став који чланови организације имају у погледу заштите одређених вредности – националне безбедности, одбране, унутрашњих и спољних послова, људских слобода и права, као и физичке и интелектуалне имовине, а посебно информација и података којима располаже организација (орган јавне власти, правно лице или комапнија).

18. **Безбедносна сметња** представља чињеницу која онемогућава издавање сертификата.

19. **Безбедносне процедуре** су прописана правила за поступање лица у раду са тајним подацима.

20. **Безбедносни брифинг** представља упознавање са прописима којима се уређује тајност података и последицама неовлашћеног приступа и коришћења тајних података.

21. **Безбедносни инцидент** дешава се када постоји стварни или потенцијални ризик за штићене податке и даље категорисан као кривично дело или прекршај.

22. **Безбедносни ризик** је стварна могућност нарушавања безбедности тајних података.

23. **Безбедносни упитник** је саставни део документације у поступку издавања сертификата за приступ тајним подацима.

24. **Безбедност** означава стање неког субјекта (појединца, групе људи, заједнице, институције) које карактерише одсуство невоља, брига, несрећа, опасности и других зла.

25. **Блокада приступа:** За спречавање даљих оштећења, неопходно је ограничити приступ угроженим подацима и предузети техничке мере као што су lock-out и повлачење докумената.

26. **Водич за поступање у случају инцидента са тајним подацима** представља кључни инструмент за адекватно управљање ситуацијама које угрожавају безбедност и интегритет заштићених података у оквиру органа јавне власти и правних лица.

27. **Губитак поверења** - Недостатак адекватне заштите тајних података може довести до значајног губитка поверења у органе јавне власти.

28. **Data Breach/Компромитација података** је безбедносни инцидент у коме се осетљиви, заштићени или поверљиви подаци копирају, преносе, гледају, краду или користе од стране појединца који је неовлашћен за приступ тим подацима.

29. **Дебрифинг** подразумева упознавање са прописима и обавезама по престанку потребе за приступом тајним подацима по различитим основама.

30. **Директива 488/2001/ЕЦ Европског парламента и Савета** односи се на заштиту класификованих информација које се стварају и обрађују у Европској унији, и представља правни оквир за регулисање безбедности и размене класификованих података између држава чланица и институција ЕУ. Ова директива поставља стандарде који се односе на обраду класификованих информација у државама чланицама, као и на поступке везане за безбедност, комуникацију и размену тих информација. Директива прописује правила за приступ класификованим информацијама, што подразумева да особе које имају приступ класификованим подацима морају проћи безбедносне провере.

31. **Дигитални потпис** – криптографски механизам који обезбеђује аутентичност, интегритет и непорецивост дигиталног документа.

32. **Документ** је сваки носач података (папир, магнетни или оптички медиј, дискета, УСБ меморија, смарт картица, компакт диск, микрофилм, видео и аудио запис и др.), на коме је записан или меморисан тајни податак.

33. **Доношење формалне одлуке о тајности** - Орган јавне власти је у обавези да донесе генеричну или појединачну писмену одлуку о одређивању степена тајности података, уз процену утицаја и потенцијалне штете по интересе Републике Србије у случају откривања, злоупотребе или уништења података. Тајност податка, под условима и на начин утврђен законом о тајности података, одређује овлашћено лице.

34. **Доставница** је потврда о томе да је лично или посредно достављање извршено која садржи лично име и адресу лица и податке којима се идентификује уручено писмено.

35. **Евиденције** подразумевају да 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.

36. **Евиденција корисника тајних података** је евиденција коју води руковалац тајним подацима у органу јавне власти.

37. **Етички аспекти безбедносних провера медицинских података** укључују заштиту приватности, избегавање дискриминације, осигурање информисаног пристанка, јасне и праведне циљеве, као и минимизацију интервенције.

38. **Жалба** је правно средство у управном поступку које се може изјавити против управног акта тј. против првостепеног решења.

39. **Зависност од информационо-комуникационих технологија (ИТ)** - подразумева прекомерну употребу дигиталних алата, као што су мобилни телефони, рачунари, друштвене мреже или видео игре, која може довести до 16 поремећаја концентрације, смањене продуктивности или чак психолошких проблема.

40. **Зависност од коцке (патаљије)** - може бити проблем који утиче на појединца у различитим аспектима живота, укључујући и његов радни учинак и понашање у ситуацијама које захтевају висок ниво одговорности и пажње, као што је рад са класификованим информацијама.

41. **Зависност од секса или сексуална зависност**, која се карактерише прекомерном и неконтролисаном потребом за сексуалним активностима која може бити психолошки и физички штетна, може се разматрати као фактор у безбедносним проверама за приступ класификованим информацијама, али као и код других зависности, њен утицај зависи од озбиљности и последица које она има на појединца.

42. З**аштита података** је скуп различитих технолошких метода којима се дигитални подаци штите током процеса дигиталног преноса података или дигиталне комуникације.

43. **Злоупотреба информација** - Неовлашћени приступ тајним подацима може довести до извоза осетљивих информација и коришћења од стране странака које имају непријатељске намере према Србији.

44. **Злоупотреба тајних података** - Лице које злоупотреби тајне податке, било да их дели, продаје или на неки други начин користи против националне безбедности, може бити осуђено на казне затвора.

45. **Зонирање** - представља систематску поделу просторија у зоне различитих нивоа безбедности у складу са Законом о тајности података, Уредбом о посебним мерама заштите тајних података у информационо-телекомуникационим системима и Уредбом о посебним мерама физичко-техничке заштите тајних података.

46. **Идентификација категорија података** - Подаци се анализирају како би се утврдило да ли испуњавају услове за означавање као тајни, укључујући прописима предвиђене категорије података, као и процену могућег утицаја на националну безбедност, јавни интерес, територијални интегритет и економске интересе. У овом кораку се такође разматра и општи значај података, као и последице које би њихово откривање могло имати на рад органа јавне власти.

47. **Изјава** чини саставни део документације на основу које је издат сертификат за приступ тајним подацима, односно дозвола.

48. **Индустријска безбедност** представља примену мера ради обезбеђења заштите тајних података, од стране извођача или подизвођача, у преговорима који претходе закључивању уговора и током целог века трајања тајних/поверљивих уговора.

49. **Инсајдер (енг. insider - "неко унутра")** је назив за особу која је припадник неке друштвене групе због чега располаже одређеним сазнањима недоступним широј јавности.

50. **Интегритет** значи очуваност изворног садржаја и комплетности података;

51. **Интерна контрола** представља мере пажње усмерене на спречавање грешака, прекомерних трошкова и преваре, проверава и обезбеђује поузданост информација.

52. **Информанти** су лица која случајно и пригодно сазнају за планирана или извршена кривична дела и њихове учиниоце.

53. **Информатори (поузданик, вигилант и агент провокатор)** су особе спремне да дуже време полицији пружају криминалистички и кривично правне релевантне информације, при чему се њихов идентитет чува у тајности.

54. **Информациона безбедност** представља скуп мера које омогућавају да подаци којима се рукује путем икт система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност и непорецивост тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица.

55. **Информациона безбедност тајних података** обухвата интегрисани скуп међузависних мера и активности усмерених на заштиту тајних информација које се обрађују у комуникационо-информационим системима – КИС.

56. **Информациона гаранција** представља гаранцију од стране органа јавне власти или правног лица да ће адекватно штитит податке од неовлашћеног приступа, коришћења, дељења или злоупотребе уз поштовање прописа и стандарда за заштиту података.

57. **ISO/IEC 27001** је међународни стандард за управљање безбедношћу информација. Детаљно описује захтеве за успостављање, имплементацију, одржавање и континуирано побољшање система управљања безбедношћу информација (ISMS) – чији је циљ да помогне организацијама да учине безбеднијом информациону имовину коју држе.

58. **Јавни подаци** су концепт у коме одређени подаци треба да буду слободно доступни свима на коришћење и поновну употребу, без ауторских или било каквих других ограничења.

59. **Кемз (Компромитација електромагнетним зрачењем)**- представља шири концепт који обухвата техничке и организационе мере за спречавање цурења података путем електромагнетних емисија.

60. **Класификација инцидената** - У складу са одредбама Закона о тајности података („Сл. гласник РС“, бр. 72/2009), инциденти у систему заштите тајних података класификују се према степену ризика по заштићене интересе и врсти повреде закона. У најширем смислу, свака компромитација штићених података подразумева неовлашћен приступ, откривање, измену, уништавање или губитак података, што представља повреду основних принципа заштите и може довести до озбиљних последица по јавне органе, правна лица или појединце.

61. **Компромитација тајног податка** представља умишљајно, нехатно или немарно откривање тајних података непозваним и неовлашћеним лицима.

62. **Компромитација штићених података** у најширем смислу (тајних података, личних података, банкарске тајне, пореске тајне, пословне и професионалне тајне) настаје када дође до неовлашћеног откривања, приступа, измене, уништења или губитка података, чиме се угрожава њихова поверљивост, интегритет или доступност. Такви догађаји могу проузроковати озбиљну штету по орган јавне власти, правно лице, организацију или појединца.

63. **Контролна листа у случају инцидента** - Органи јавне власти и правна лица се охрабрују да примењују унапред дефинисану листу за проверу, као алат за брзо и ефикасно реаговање у случају инцидента.

64. **Контраобавештајна заштита** је посебан вид обавештајне активности чији је циљ заштита тајних података сопствене државе, заштита виталних државних органа и институција, спречавање деловања противничких обавештајних служби на територији своје земље и друго.

65. **Корисник тајног податка** је држављанин Републике Србије или правно лице са седиштем у Републици Србији, коме је издат сертификат од стране надлежног органа, односно страно физичко или правно лице коме је на основу закљученог међународног споразума издата безбедносна дозвола за приступ тајним подацима, као и функционер органа јавне власти који на основу овог закона има право приступа и коришћења тајних података без издавања сертификата.

66. **Кривично дело (Кривична одговорност)**: Инцидент који је довео или могао довести до компромитације тајних података, укључујући: • неовлашћено саопштавање, предаја или омогућавање приступа тајним подацима, • губитак, уништење или откривање докумената који садрже тајне податке, • прибављање тајних података без одобрења.

67. К**ривично дело** је безбедносни инцидент који би разумно могао да доведе или јесте довео до губитка или компромитовање штићених података и захтева истрагу ради даље анализе и покретања кривичног поступка.

68. **Криптографски производ** је софтвер или уређај путем кога се врши криптозаштита.

69. **Криптозаштита** је примена метода, мера и поступака ради трансформисања података у облик који их за одређено време или трајно чини недоступним неовлашћеним лицима.

70. **Континуирани надзор**: Процес, не само стање.

71. **Ланац чувања (Chain of custody)** – документован процес праћења физичког или дигиталног тајног податка од тренутка његовог настанка до чувања, преноса или уништења, ради очувања доказне вредности.

72. **Листа "ПОТРЕБНО ДА ЗНА"** представља међународни принцип рада са тајним подацима који подразумева списак лица и радних места који имају приступ тајним подацима у оквиру органа јавне власти/ принцип двоструког кључа приступу тајним подацима.

73. **Листа "ПОТРЕБНО ПОДЕЛИТИ СА"** представља међународни принцип рада са тајним подацима који подразумева списак органа јавне власти који међусобно размењују тајне податке.

74. **Лични податак** је сваки податак који се односи на физичко лице чији је идентитет непосредно или посредно одређен или одредив-посебно на основу ознаке идентитета. Лични податак је свака информација која се односи на физичко лице које се у неком тренутку може идентификовати; то је карактеристична особина сваке појединачне особе.

75. **Лојалност** је значење изведено преко синонима: оданост, верност, исправност, поданичка верност, честитост, часност, привржености, поверљивост, постојаност, непроменљивост, искреност,поштење.

76. **Логовање и надзор** (logging & monitoring) – критично за детекцију инцидената.

77. **Мере заштите ИКТ система** су техничке и организационе мере за управљање безбедносним ризицима ИКТ система.

78. **Мере заштите** су опште и посебне мере које се предузимају ради спречавања настанка штете, односно мере које се односе на остваривање административне, информатичко-телекомуникационе, персоналне и физичке безбедности тајних података и страних тајних података.

79. **Мултифакторска аутентификација (MFA)** – метод аутентификације који захтева два или више независних фактора (нпр. лозинка + једнократни код).

80. **Надлежност** представља право и дужност доношења одлука које се односе на управљање делегираним ресурсима (људским, буџетским, техником и тајним подацима) да би се остварили циљеви националне и организационе безбедности, односно система зштите тајних података.

81. **НАТО стандард С-М (2002) 49** подразумева да безбедносне провере обухватају различите аспекте кандидата, укључујући: • Кривичну историју. • Психолошке процене. • Медицинске процене.

82. **NATO RESTRICTED, EU CONFIDENTIAL и сл.** – степени тајности у међународним системима (важно ако се размењују подаци са НАТО-ом, ЕУ-ом итд.).

83. **Недопуштена измена или уништавање тајних података**- Лица која униште, измене или на неки начин ометају очување тајних података, као и лица која не предузму прописане мере заштите података, могу бити кривично санкционисана.

84. **Неовлашћено откривање тајних података**- Лице које без овлашћења открије тајне податке или их користи у незаконите сврхе, може бити кривично гоњено.

85. **Неповољна историја у раду са тајним подацима** – Раније повреде правила о заштити тајних података или неодговорно поступање са поверљивим информацијама (пословна тајна, професионална тајна...)

86. **Непорецивост** представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи.

87. **Непоузданост власничке структуре** – Ако се утврди да су власници или оснивачи правних лица повезани са ризичним субјектима, страним утицајем или криминалним групама.

88. **Непоузданост и нестабилност** – Процена да кандидат није довољно одговоран, финансијски стабилан (дугови, честе промене радних места), или да има друге личне карактеристике које га чине подложним притиску или уцени.

89. **Обавеза обавештавања** - Сва лица која на било који начин раде са тајним подацима имају неодложну обавезу да пријаве сваки безбедносни инцидент или сумњу на повреду мера заштите. Обавештавање се врши непосредно надређеном, овлашћеном лицу за заштиту тајних података или руководиоцу органа. У зависности од тежине и природе инцидента, обавештавају се и Канцеларија Савета за националну безбедност и заштиту тајних података, службе безбедности (БИА или ВБА у складу са надлежностима) или надлежно тужилаштво.

90. **Обезбеђење** је планска примена и коришћење оперативно-тактичких метода, мера, радњи, средства и снага ради заштите од угрожавања одређених личности, људи, масовних скупова, имовине, отвореног-затвореног простора, фабричких хала, магацина или других објеката.

91. **Обрада података** је генерално, "прикупљање и употреба података ради стварања смислене информације".

92. **Обука и свест (TRAINING & AWARENESS)**: Критичан елемент персоналне безбедности.

93. **Овлашћено лице за одређивање тајности података (произвођач)** подразумева да креатор тајних података може бити свако лице које има одговарајући безбедносни сертификат и које према својим дужностима и задацима треба да креира, тј. рукује тајним подацима - информацијама.

94. **Одговорност** када је у питању систем заштите тајних података и организациона безбедност, представља обавезу да се даваоцу овлашћења одговара за испуњавање тих овлашћења (обавеза поступања). Одговорност обухвата и давање информација и образложења за спровођење одређених поступака, активности или одлука, када је у питању рад са тајним подацима.

95. **Одлука о одређивању руковаоца тајним подацима у органу јавне власти** је одлука којом се одређује се руковалац тајним подацима у органу јавне власти.

96. **Одлука о одређивању тајних података у Органу јавне власти** је одлука којом се одређују се тајни подаци у Органу јавне власти што укључује и утврђивање степена и рока тајности.

97. **Одређивање тајних података** је поступак којим се податак, у складу са овим законом, одређује као тајни и за који се утврђује степен и рок тајности.

98. **Означавање података** - Подаци добијају јасну ознаку која укључује степен тајности, начин престанка тајности, податке о овлашћеном лицу, датум означавања, назив органа који је донео одлуку и правну основу.

99. **Означавање степена тајности** је означавање тајног податка ознакама: "ДРЖАВНА ТАЈНА", "СТРОГО ПОВЕРЉИВО", "ПОВЕРЉИВО" или "ИНТЕРНО".

100. **Орган јавне власти** је државни орган, орган територијалне аутономије, орган јединице локалне самоуправе, организација којој је поверено вршење јавних овлашћења, као и правно лице које оснива државни орган или се финансира у целини, односно у претежном делу из буџета, а који поступа са тајним подацима, односно који их ствара, прибавља, чува, користи, размењује или на други начин обрађује.

101. **Организационе мере заштите** представљају организацију заштите процеса рада и функционисања информационо-комуникационог система у редовним околностима и ванредним ситуацијама.

102. **Организациони услови** односе се нарочито на организацију процеса рада, заштиту приступа тајним подацима, заштиту од неовлашћеног коришћења тајних података, одређивање одговорног лица задуженог за спровођење мера заштите, као и утврђивање поступка у случају ванредних и хитних околности.

103. **Податак о личности** је сваки податак који се односи на физичко лице чији је идентитет одређен или одредив, непосредно или посредно, посебно на основу ознаке идентитета, као што је име и идентификациони број, података о локацији, идентификатора у електронским комуникационим мрежама или једног, односно више обележја његовог физичког, физиолошког, генетског, менталног, економског, културног и друштвеног идентитета.

104. **Патролирање** је услуга обезбеђења коју врше службеници обезбеђења крећући се у одређено време између више међусобно раздвојених места/објеката.

105. **Периметар** је део физичке безбедности који се мора поставити око објеката у којима се налазе штићени подаци, како би се спречило неовлашћен приступ.

106. **Персонална безбедност** представља низ процедура чији је основни циљ да се утврди да ли неко лице може бити овлашћено да добије приступ тајним подацима а да при томе не представља неприхватљив ризик за безбедност.

107. **План заштите тајних података** у органу јавне власти – је основни стуб организационе безбедности у сваком органу јавне власти. Он омогућава правилно управљање тајним подацима и осигурава њихову заштиту, што је од кључног значаја за очување националне безбедности. Иако сам План није директно прописан Законом о тајности података, он се сматра имплицитно обавезним као део комплетног система заштите тајних података, који мора бити у складу са важећим законима и прописима.

108. **План поступања у вандредним ситуацијама** обухвата процедуре и мере које треба предузети у случају напада, злоупотребе или другиј вандредних ситуација које угрожавају безбедност података.

109. **Повреда радне дисциплине (Дисциплинска одговорност)**: Инцидент који не доводи до компромитације тајних података, али представља незаконито или несавесно поступање у вршењу службене дужности.

110. **Податак од интереса за Републику Србију** је сваки податак или документ којим располаже орган јавне власти, који се односи на територијални интегритет и суверености, заштиту уставног поретка, људских и мањинских права и слобода, националну и јавну безбедност, одбрану, унутрашње послове и спољне послове.

111. **Пословна тајна** је податак који може да има економску вредност. Ова врста података није опште позната нити лако доступна трећим лицима. Банкарска тајна је пример пословне тајне, али њена специфичност јесте да иста прелази у више категорија (професионална тајна, лични подаци).

112. **Поступци због повреда радне дисциплине**: Одговорна лица која су прекршила процедуре могу бити предмет дисциплинских мера, као што су опомена, суспензија или отказ.

113. **Правне импликације** - Када дође до кршења процедура означавања и заштите тајних података, могу се покренути и правни поступци против одговорних лица.

114. **Правно лице** има регистровано седиште на територији Републике Србије;обављање делатности у вези са интересима из члана 8. овог закона; постојање одговарајуће безбедносне провере; ако није у поступку ликвидације или стечаја; није кажњавано мером забране вршења делатности, односно да му није изречена казна престанка правног лица или мере безбедности забране обављања одређених регистрованих делатности или послова,уредно измирење пореских обавеза и доприноса;

115. **Правовремено, транспарентно и систематизовано поступање у случају инцидента** представља један од основних стубова система заштите тајних података. Овакве процедуре морају бити део Плана заштите тајних података, укључујући и евиденцију свих пријављених инцидената, анализа узрока и извештавање према надлежним институцијама.

116. **Праћење стања сертификата** обухвата праћење издатих сертификата за физичка и правна лица, укључујући проверу ваљаности сертификата у контексту њиховог приступа тајним подацима.

117. **Прекршај (Прекршајна одговорност)**: Инцидент који није довео до компромитације тајних података, али указује на пропусте у примени прописаних мера заштите.

118. **Престанак тајности**: Процес укидања тајности (овде је споменута, али би могла имати посебну дефиницију).

119. **Прекршајни поступци**: Уколико је дошло до прекршаја у смислу неправилног чувања или поступања са тајним подацима, могу се изрећи новчане казне или друге мере као што су упозорење или јавна опомена.

120. **Принцип минимизације података** – релевантан за обраду тајних података.

121. **Провера медицинских података** је кључан аспект безбедносне провере јер омогућава процену да ли кандидат има менталне, неуролошке или друге здравствене сметње које могу утицати на његову способност да поуздано, свесно и одговорно рукује тајним подацима и информацијама.

122. **Провера медицинских података** је кључан аспект безбедносне провере јер омогућава процену да ли кандидат има менталне, неуролошке или друге здравствене сметње које могу утицати на његову способност да поуздано, свесно и одговорно рукује тајним подацима и информацијама. Провера медицинских података је неопходна ради заштите националне безбедности, тајних података и стабилности лица које раде са тајним подацима. Неопходно је осигурати да ниједна особа са тешким психофизичким поремећајима не добије приступ тајним подацима јер би то могло довести до озбиљних безбедносних ризика.

123. **Професионална тајна** је податак који професионалац у контакту са клијентом сазна о личном или породичном животу клијента, а што не сме бити доступно другим особама. Професионална тајна у себи садржи лични податак, односно личне податке, који су повезани са правилима струке.

124. **Процедура за означавање и одређивање степена тајности података** представља кључни корак у заштити осетљивих информација, докумената и података, као и очувању интереса Републике Србије. Ова процедура има за циљ да обезбеди безбедност података, уз транспарентност и одговорност органа јавне власти. Као тајни податак може се одредити податак од интереса за Републику Србију чијим би откривањем неовлашћеном лицу настала штета, ако је потреба заштите интереса Републике Србије претежнија од интереса за слободан приступ информацијама од јавног значаја.

125. **Процена околности настанка безбедносног инцидента у раду са тајним подацима, као и његова правна квалификација,** један је од најважнијих корака у обради и одређивању даљег поступања у складу са прописима. У зависности од врсте инцидента, различито ће се реаговати надлежни органи и применити одговарајући правни механизми.

126. **Процена претње за безбедност тајног податка (самопроцена)** - по Закону о тајности података представља безбедносну процену која се примењује у раду са тајним подацима. Процена претње за безбедност тајног податка или самопроцена није само идентификација неправилности, већ и континуиран процес унапређења. Комбинација редовне процене, обуке, технолошких решења, унутрашње контроле и надзора осигурава највиши ниво заштите.

127. **Процена ризика** је одређивање квантитативних и квалитативних вредности ризика који се односе на конкретну ситуацију и признато претње (назива опасност).

128. **Процена утицаја и ризика од инцидента у раду са тајним подацима** важан је корак у разумевању степена угрожавања који је наступио. То подразумева не само процену настанка материјалне штете, већ и потенцијалне последице по националну безбедност, права лица или организацију. Када се процењује да ли је инцидент могао имати међународне импликације, важно је узети у обзир степен осетљивости података, као и могућност да се повреда изазове преко граница.

129. **Рад са правним лицима** односни се на управу и сарадњу са правним лицима код поверљивих набавки, посебно у области индустријске безбедности, који укључују безбедност информација и технологија у производним и сервисним процесима.

130. **Радна тачка за рад са тајним подацима** представља функционални одређени део радног простора унутар органа јавне власти који је посебно организован ради пријема, обраде, приступа и чувања тајних података у органу јавне власти. Радна тачка не представља званично успостављену административну, односно безбедносну зону, већ служи као привремено решење за рад са тајним подацима у контролисаним и безбедним условима, до успостављања зона у складу са Уредбом о посебним мерама физичкотехничке заштите тајних података.

131. Р**асположивост** је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;

132. **Ревизија и ажурирање** - Ознаке тајности се периодично преиспитују и ревидирају како би се утврдило да ли је потребно задржати, променити или укинути степен тајности, због временског ограничења, престанка тајности утврђивањем датума, наступањем одређеног догађаја и истеком рока.

133. **Регистарски систем** представља уређен систем који мора да буде реализован у складу са прописима и стандардима из области ЗТП.

134. **Релативне сметње (процена појединачног случаја)** - Ово су стања која не морају аутоматски водити дисквалификацији, али могу представљати безбедносни ризик у зависности од тежине, учесталости симптома и начина лечења.

135. **Решење** представља управни акт надлежног органа којим је решена управна ствар која је била предмет управног поступка.

136. **Ризик информационо-комуникационог система** подразумева могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;

137. **Руковалац тајним податком** је физичко лице или организациона јединица органа јавне власти, који предузима мере заштите тајних података у складу са одредбама овог закона.

138. **Саботажа** описује намерне радње којима се наноси штета физичкој или виртуелној инфраструктури организације, укључујући непоштовање процедура одржавања или ИТ, контаминирање чистих простора, физичко оштећење објеката или брисање кода ради спречавања редовних операција.

139. **Сајбер безбедност** представља примену технологије, процеса и контроле ради одбране рачунара, сервера, мобилних уређаја, електронских система, мрежа и података од сајбер напада.

140. **Сајбер претња** укључује крађу, шпијунажу, насиље и саботажу свега што је повезано са технологијом, виртуелном стварношћу, рачунарима, уређајима или интернетом.

141. **Сертификат за приступ тајним подацима** је документ који потврђује да лице има право приступа и коришћења тајних података у одговарајућој мери по принципу „потреба да зна“.

142. **Сертификовање привредних субјеката** омогућава њихово учешће на расписаним тендерима у државама са којима Република Србија има закључене и ратификоване међународне споразуме о размени и узајамној заштити тајних података.

143. **Сегментација**: Подела информација према потреби да зна.

144. **Систем мониторинга и ревизије** је систем за праћење и ревизију који осигурава да се све мере заштите примењују на адекватан начин.

145. **Систем управљања безбедношћу информација (SUIB / ISMS)**: Организациони оквир.

146. **Скривање података** – Лице намерно или ненамерно не пријави све релевантне информације у сврху вршења безбедносне провере (непријављивање контаката са страним држављанима, скривање радног или криминалног досијеа,скривање медицинских података, лажирање информација о образовању..).

147. **Служба безбедности** је служба безбедности у смислу закона којим се уређују основе безбедносно-обавештајног система Републике Србије.

148. **Страни тајни податак** је податак који Републици Србији повери страна држава или међународна организација уз обавезу да га чува као тајни, као и тајни податак који настане у сарадњи Републике Србије са другим државама, међународним организацијама и другим међународним субјектима, у складу са закљученим међународним споразумом који је са страном државом, међународном организацијом или другим међународним субјектом закључила Република Србија;

149. **Страни утицај** – Чести контакти или породичне везе са страним држављанима који се могу сматрати безбедносним ризиком.

150. **Стручни надзор у систему заштите тајних података** представља процес стручне процене и верификације примене Закона о тајности података код органа јавне власти, са циљем осигурања усклађености прописа и ефикасности мера заштите. Овај процес омогућава идентификацију потенцијалних ризика и слабости, пружајући стручне препоруке за унапређење система заштите тајних података.

151. **Судски поступци** - Ако се утврди да је поступак означавања или обраде података био незаконит, могу се покренути цивилни поступци, где се може захтевати одговорност за штету коју су органи јавне власти или њихови запослени нанели.

152. **Security breaches/кршење безбедности** представља неовлашћени приступ информацијама на мрежама, серверима или уређајима, заобилажење сигурности на тим системима, што на крају резултира отицањем или компромитацијом података.

153. **Тајни податак** је податак од интереса за Републику Србију који је законом, другим прописом или одлуком надлежног органа донесеном у складу са законом, одређен и означен одређеним степеном тајности.

154. **Тајни податак означен степеном тајности "ДРЖАВНА ТАЈНА"** представља податак чијим би откривањем неовлашћеном лицу, његовом злоупотребом или уништавањем настала неотклоњива тешка штета по интересе Републике Србије.

155. **Тајни податак означен степеном тајности "ИНТЕРНО"** представља податак чијим би откривањем неовлашћеном лицу, његовом злоупотребом или уништавањем настала штета по рад, односно обављање задатака и послова органа јавне власти.

156. **Тајни податак означен степеном тајности "ПОВЕРЉИВО"** представља податак чијим би откривањем неовлашћеном лицу, његовом злоупотребом или уништавањем настала штета по интересе Републике Србије.

157. **Тајни податак означен степеном тајности "СТРОГО ПОВЕРЉИВО"** представља податак чијим би откривањем неовлашћеном лицу, његовом злоупотребом или уништавањем настала тешка штета по интересе Републике Србије.

158. **Тајност** је својство које значи да податак није доступан неовлашћеним лицима.

159. **Техничка заштита** је обезбеђење лица и имовине које се врши техничким средствима и уређајима, њиховим планирањем, пројектовањем, уградњом и одржавањем.

160. **Техничке мере заштите** представљају обезбеђење и заштиту података и информација и других елемената информационо-комуникационог система, који се остварују применом посебних техничко-технолошких процеса рада и/или спровођењем физичко-манипулативних мера заштите у било којој процедури у оквиру рада ИКТ система.

161. **Технички услови** односе се нарочито на физичко-техничку заштиту простора, односно просторија у којима се чувају тајни подаци, противпожарну заштиту, заштиту тајних података приликом преношења и достављања изван просторија у којој се чувају, транспорт тајних података, обезбеђивање и заштиту информационо-телекомуникационим средстава којима се врши преношење и достављање тајних података и спровођење прописаних мера крипто-заштите.

162. **Технолошка акредитација** - Фокусира се на техничке аспекте као што су заштита од компромитације електромагнетним зрачењем (КЕМЗ) и примена специфичних безбедносних мера, на основу прописа о одбрани, укључујући ЕУ и NATO стандарде.

163. **TEMPEST** је стандардизовани скуп техника и тестова за спречавање компромитације. Док **КЕМЗ** означава све мере заштите, TEMPEST је конкретно оријентисан ка сертификацији и тестирању уређаја (нпр. NATO SDIP-27).

164. **Уговор** је документ који подразумева посебне мере заштите тајних података које се примењују на све организационе и техничке услове за чување тајних података у поступку закључења уговора између органа јавне власти и правног или физичког лица на основу којег се тајни подаци достављају овим лицима.

165. **Унутрашња контрола** је процес установљен и спровођен од стране руководиоца органа јавне власти, организационе јединице или овлашћеног појединца.

166. **Управни поступак** је поступак доношења управних аката. Под управним поступком подразумевају се процедурална правна правила која се примењују у вези са доношењем одлука у управним стварима.

167. **Усаглашеност** са стандардима безбедности представља обавезу органа да се усагласи са националним и међународним стандардима у области информационе безбедности, посебно у области безбедности ИТ система који обрађују тајне податке.

168. **Управљање инцидентима безбедности** – организовани скуп активности за откривање, анализу, ограничавање и опоравак од безбедносних инцидената.

169. **Физичка безбедност/сигурност** представља примену мера физичке и техничке заштите на појединачним локацијама, зградама или отвореним просторима на којима се налазе или чувају штићени подаци (информације) које захтевају заштиту од губљења, неовлашћеног приступа, компромитовања или отуђења.

170. **Физичка заштита** је услуга обезбеђења која се пружа првенствено личним присуством и непосредном активношћу службеника обезбеђења у одређеном простору и времену у складу са планом обезбеђења, применом мера и овлашћења службеника обезбеђења;

171. **Физичко-техничка заштита** је обезбеђење лица и имовине применом физичке заштите и коришћењем средстава техничке заштите.

172. **Финансијска нестабилност** – Велики дугови, лоша финансијска ситуација или нерегуларно пословање, покретање ликвидације односно стечаја правних лица.

173. **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.

174. **Шифра** је пресликавање (трансформација, правило) којим се тајна порука пресликава у неразумљив низ знакова (слова, бројеве...)

175. **Шпијун** - (уходa, доушник, достављач, потказивач, вребач, жбир...)

176. **Шпијунажа** је прикривена или недозвољена пракса шпијунирања за потребе стране владе, организације, ентитета или особе ради добијања поверљивих информација ради војне, политичке, стратешке или финансијске користи.

177. **Штета** је нарушавање интереса Републике Србије настало као последица неовлашћеног приступа, откривања, уништавања и злоупотребе тајних података или као последица друге радње обраде тајних података и страних тајних података.

178. **Штићени простор** је објекат или простор на којем се врше услуге обезбеђења.