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. 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.

5. 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.

6. 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.

7. 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.

8. 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.

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

10. 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.

11. 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.

12. 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).

13. Безбедносна сметња представља чињеницу која онемогућава издавање сертификата.

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

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

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

17. Безбедносни ризик је стварна могућност нарушавања безбедности тајних података.

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

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

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

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

22. Документ је сваки носач податка (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.

23. 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.

24. 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.

25. 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.

26. 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.

27. Евиденцију корисника тајних података је евиденција коју води руковалац тајним подацима у органу јавне власти.

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

29. Заштита података је скуп различитих технолошких метода којима се дигитални подаци штите током процеса дигиталног преноса података или дигиталне комуникације.

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

31. 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.

32. 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.

33. 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.

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

35. 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.

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

37. Интегритет значи очуваност изворног садржаја и комплетности података;

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

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

40. 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.

41. 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.

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

43. 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.

44. 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.

45. 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.

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

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

48. Компромитујуће електромагнетно зрачење (КЕМЗ) представља ненамерне електромагнетне емисије приликом преноса, обраде или чувања података, чијим пријемом и анализом се може открити садржај тих података.

49. 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.

50. Кривично 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.

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

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

53. 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.

54. 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.

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

56. 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.

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

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

59. 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.

60. 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.

61. 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.

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

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

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

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

66. 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.

67. 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.

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

69. 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.

70. 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.

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

72. 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.

73. 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.

74. 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.

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

76. 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.

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

78. 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.

79. 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.

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

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

82. 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.

83. 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.

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

85. 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.

86. 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).

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

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

89. 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;

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

91. Прекршај је безбедносни инцидент који не доводи до губитка, компромитовања или сумње на безбедносни инцидент.

92. 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.

93. 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.

94. 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.

95. 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.

96. 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.

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

98. 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.

99. Расположивост је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;

100. 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.

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

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

103. 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;

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

105. 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.

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

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

108. 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“.

109. 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.

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

111. 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..).

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

113. 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;

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

115. 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.

116. 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.

117. 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.

118. 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.

119. 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.

120. 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.

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

122. 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.

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

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

125. 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.

126. 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.

127. 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.

128. 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).

129. 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.

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

131. 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.

132. 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.

133. 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.

134. 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;

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

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

137. 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.

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

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

140. 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.

141. 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.

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

КАНЦЕЛАРИЈА САВЕТА ЗА НАЦИОНАЛНУ БЕЗБЕДНОСТ
И ЗАШТИТУ ТАЈНИХ ПОДАТАКА

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

web: www.nsa.gov.rs