На основу члана 8. став 1. Закона о информационој безбедности ("Сл. гласник РС", бр. 6/2016, 94/2017 и 77/2019), чл. 2. и 3. Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја („Службени гласник РС", број 94/16) в.ф.председника Основног суда у Бујановцу, дана 07.02.2024.године доноси

**Акт о бе****збедности информационо-комуникационог система Основног суда у Бујановцу**

**I ОСНО****ВНЕ ОДРЕДБЕ**

Предмет Акта

Члан 1.

Актом о безбедности информационо-комуникационог система Основног суда у Бујановцу (у даљем тексту: Акт о безбедности), у складу са Законом о информационој безбедности (у даљем тексту: Закон), ближе се уређују мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима информационо-комуникационог система Основног суда у Бујановцу (у даљем тексту: ИКТ систем).

Циљеви Акта о безбедности

Члан 2.

Циљеви доношења Акта о безбедности су:

1. одређивање начина и процедура за постизање и одржавање адекватног нивоа безбедности система;
2. спречавање и ублажавање последица инцидената којим се угрожава или нарушава информациона безбедност;
3. подизање свести код запослених о значају информационе безбедности, ризицима и мерама заштите приликом коришћења ИКТ система;
4. прописивање овлашћења и одговорности запослених у вези са безбедношћу и ресурсима ИКТ система;
5. свеукупно унапређење информационе безбедности и провера усклађености примене мера заштите.

Обавеза примене одредби Акта о безбедности

Члан 3.

Мере заштите ИКТ система које су ближе уређене Актом о безбедности служе превенцији од настанка инцидената и минимизацији штете од инцидената и њихова примена је обавезна за све запослене.

Запослени у Основном суду у Бујановцу морају бити упознати са садржином Акта о безбедности и дужни су да поступају у складу са одредбама овог акта, као и других интерних процедура које регулишу информациону безбедност.

Одговорност запослених

Члан 4.

Запослени у Основном суду у Бујановцу су дужни да приступају информацијама и ресурсима ИКТ система само ради обављања редовних пословних активности, као и да благовремено информишу овлашћено лице о свим сигурносним инцидентима и проблемима.

Непоштовање одредби Акта о безбедности, као и свако угрожавање или нарушавање информационе безбедности, повлачи дисциплинску одговорност запосленог.

Предмет заштите

Члан 5.

Мере заштите ИКТ система односе се на електронске комуникационе мреже, електронске уређаје на којима се чува и врши обрада података коришћењем рачунарског програма, оперативне и апликативне рачунарске програме, програмски код, податке који се чувају, обрађују, претражују или преносе помоћу електронских уређаја, организациону структуру путем које се управља ИКТ системом, корисничке налоге, тајне информације за проверу веродостојности, техничку и корисничку документацију, унутрашње опште акте и процедуре.

**II МЕРЕ ЗАШТИТЕ**

Успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система

Члан 6.

Основни суд у Бујановцу у оквиру организационе структуре утврђује послове и одговорности запослених у циљу управљања информационом безбедношћу.

Интерни акти који уређују обавезе и одговорности запослених у вези са управљањем информационом безбедношћу:

* Акт о безбедности ИКТ-а.

Председник Основног суда у Бујановцу донеси појединачни акт, у складу са актом о систематизацији, којим одређује одговорна лица за обезбеђивање и праћење безбедности информационог система Основном суду у Бујановцу. Сви запослени морају бити упознати са процедуром заштите безбедности ИКТ система.

Члан 7.

Рад на даљину

Радни однос за обављање послова ван просторија послодавца обухвата:

* Рад на даљину;
* Рад од куће;
* Виртуелно радно окружење.

Такође, рад на даљину у смислу овог Акта односи се на ситуацију када је запослени и други радно ангажовани обавезан да изврши одређене послове на мрежи послодавца, а налази се ван просторија послодавца.

Предметно ангажовање и омогућавање обављања задатих и неопходних послова се уређује путем Процедуре за VPN приступ информационом систему (у даљем тексту: VPN процедура).

VPN процедура дефинише правила и услове за повезивање на мрежу Основном суду у Бујановцу са удаљене локације. Правилном применом утврђеног поступка и начина приступа, Основном суду у Бујановцу своди на минимум потенцијалну изложеност штети која може настати услед неауторизованог или неконтролисаног приступа мрежи.

VPN процедура се примењује на све запослене у Основном суду у Бујановцу и сараднике који користе рачунаре или мобилне уређаје за повезивање на мрежу Основном суду у Бујановцу, и уређује приступ са удаљених локација у сврху обављања посла у име и за рачун Основном суду у Бујановцу, укључујући коришћење електронске поште и мрежних ресурса, као и начин приступа мрежи Основном суду у Бујановцу са удаљених локација.

Ауторизованим корисницима није дозвољено да користе мрежу Основном суду у Бујановцу за активности које нису у домену пословних активности, радних и других задатака у вези са послом и предметом рада појединачно запосленог.

Захтеви који морају бити испуњени и дефинисани у VPN процедури:

* 1. Ауторизовани корисници морају чувати креденцијале својих налога и не смеју омогућити приступ било ком трећем лицу.
  2. Приликом коришћења службеног рачунара за приступ са удаљене локације мрежи Основном суду у Бујановцу, ауторизовани корисник не сме истовремено бити повезан и на неку другу мрежу која може угрозити безбедност комуникације.
  3. Приступ са удаљене локације мора бити одобрен од стране одговорног лица за надзор спровођења VPN процедуре.
  4. Сви уређаји који су повезани на интерну мрежу преко удаљених локација морају имати инсталирану заштиту у виду антивирусног софтвера. Трећа лица су у обавези да примењују захтеве из закључених уговора са Основном суду у Бујановцу.
  5. Сви пословни подаци који се креирају приликом рада на даљину складиште се у информационом систему. Ради безбедности, пословни подаци се не складиште на мобилним уређајима.

Рад на даљину запослених или других радно ангажованих (ангажованих за рад у просторијама суда) одобрава председник суда.

Коришћење мобилних уређаја

Мобилни уређаји подразумевају све преносне електронске уређаје намењене за комуникацију на даљину. У мобилне уређаје спадају преносиви рачунари, таблети, мобилни телефони, PDA и сви други мобилни уређаји који садржи податке и имају могућност повезивања на мрежу. Приликом коришћења мобилних уређаја потребно је осигурати пословне информације од могућег компромитовања.

Рад на даљину може се остварити и коришћењем уређаја који нису мобилни (на пример, десктоп рачунари). Ови уређаји, при томе, морају имати примењене најмање исте безбедносне мере као и сродни уређаји који се налазе у оквиру мреже, док се за заштиту комуникације морају применити исте мере као и за заштиту комуникације мобилних уређаја. Подешавање ових уређаја врше овлашћена лица. Корисници ових уређаја морају обезбедити довољно безбедан простор за њихов рад (засебна соба, положај дисплеја такав да се онемогући посматрање од стране неовлашћених особа и слично).

Обезбеђивање да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који обављају и у потпуности разумеју своју одговорност

Члан 8.

Запослени који управљају ИКТ системом, односно запослени који користе ИКТ систем имају адекватан степен образовања и способности, као и свест о значају послова које обављају.

Провера кандидата и услови запошљавања

У Основном суду у Бујановцу спроводе се радње у циљу провере испуњености услова сваког појединачног кандидата за запослење, у складу са одговарајућим прописима и етичким правилима, сразмерно пословним захтевима, класификацији информација којима ће имати приступ и сагледаним ризицима.

Обавезе у току запослења

Руководство Основном суду у Бујановцу је дужно да захтева од свих запослених и радно ангажованих лица да примењују мере заштите безбедности, у складу са овим актом и важећим процедурама.

Основном суду у Бујановцу у циљу развоја, имплементације и одржавања система заштите и безбедности података обезбеђује услове за интеграцију контролних механизама тако што:

* Обезбеђује да се поступци заштите спроводе на организован начин и у складу са процедурама и у континуитету;
* Штити информације и податке са сличним профилом осетљивости и карактеристикама на једнак начин у свим организационим јединицама;
* Координира безбедност и заштиту података у информационом систему са физичком заштитом истих.

Овлашћена лица у Основном суду у Бујановцу, која су надлежна за праћење, анализу, извештавање и предузимање активности на плану спровођења усвојене политике и процедура, континуирано се обучавају у циљу унапређења техничког и технолошког

знања, ауторизована су за предузимање хитних и неодложних мера у случају постојања непосредне опасности за податке и документацију које су под мерама заштите.

Упознавање са безбедношћу информација, стицање знања и обука

Сви запослени у Основном суду у Бујановцу су у обавези да прођу одговарајућу обуку и редовно стичу нова и обнављају постојећа знања о процедурама које уређују безбедност информација, на начин који одговара њиховом пословном ангажовању и радном месту.

Дисциплински поступак

Дисциплински поступак се спроводи против запослених који су нарушили безбедност информација или на други начин извршили повреду правила и политике на снази и примени у Основном суду у Бујановцу.

Дисциплински поступак се покреће председник Основног суду у Бујановцу, а по предлогу, лица овлашћеног за праћење, прикупљање, анализу и обраду података.

Заштита од ризика који настају при променама послова или престанка радног ангажовања лица запослених код оператора ИКТ система

Члан 9.

Запослени и по другом основу ангажована лица, дужни су да чувају поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система, након престанка или промене радног ангажовања.

За поступања приликом престанка запослења предузимају се следеће активности:

* проверава се испуњеност свих услова у погледу чувања и изношења података у електронском и папирном формату,
* прегледају се сви налози и приступи систему који су били доступни запосленом,
* преузимају се од запосленог електронски и други мобилни уређаји,
* утврђује начин контакта са бившим запосленим након одласка,
* даје се налог за укидање налога електронске поште и свих других права приступа систему Основног суда у Бујановцу на дан престанка радног односа или другог основа ангажовања бившег запосленог,
* прегледа све налоге за приступ одлазећег запосленог и прикупља приступне шифре и кодове са циљем укидања/промене истих на дан одласка,
* преузима картице или друге уређаје којима се омогућава приступ пословним

Члан 10.

Информациона добра обухватају податке у датотекама и базама података, програмски код, конфигурацију хардверских компоненти, техничку и корисничку документацију, унутрашње опште акте и процедуре.

Пописивање имовине

У Основном суду у Бујановцу врши се идентификацију имовине која одговара животном циклусу информација и документује њен значај. Животни циклус информације обухвата креирање, обраду, складиштење, пренос, брисање и уништавање података и информација. У Основном суду у Бујановцу прави се попис добара који је тачан, ажуран, конзистентан и усклађен са другом имовином.

Евиденцију о информационим добрима и средствима и имовини за обраду информационих добара води референт у судској управи Стојан Стошић обзиром да у суду не постоји систематизовано радно место систем администратора и ИТ техничара, послове ИТ техничара у складу са годишњим распоредом за 2024.годину обавља референт Стојан Стошић.

Власништво над имовином, прихватљиво коришћење имовине и њен повраћај

Појединци којима је дата одговорност за контролисање животног циклуса имовине дужни су да правилно управљају имовином током целог животног циклуса.

Запослени и екстерни корисници су обавезни да врате сву имовину Основном суду у Бујановцу коју поседују након престанка њиховог запослења, уговора или споразума о ангажовању на одређеним пословима и задацима.

Током отказног рока запослених, контролише се њихово неовлашћено копирање, умножавање или преузимање релевантних заштићених информација.

Класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком из члана 3. Закона о информационој безбедности.

Члан 11.

Класификовање податка је поступак утврђивања и појединачног додељивања нивоа тајности податка, у складу са њиховим значајем.

Основни суд у у Бујановцу означава типове података као поверљиве, интерне или јавне. Имовина се означава уз помоћ идентификационих налепница које носе одговарајућу класификациону ознаку.

Класификација се врши ради:

* Јачања корисничке одговорности, како би корисници могли да уоче и препознају пословну вредност податка приликом чувања или слања и постану свесни одговорности за неовлашћено коришћење или преношење;
* Подизања свести о вредности информације или документа;
* Заштите садржаја;
* Интеграције са системима за архивирање.

Класификација документа мора да буде усклађена са правилима контроле приступа.

Заштита носача података

Члан 12.

Овлашћено лице у служби суда, обезбеђује спречавање неовлашћеног откривања, модификовања, уклањања или уништења података који се чувају на носачима података.

Евиденцију носача на којима су снимљени подаци, води овлашћено лице за ИКТ у Основном суду у Бујановцу.

Управљање преносним носачима података (медијума)

* све медијуме треба складиштити на безбедном и заштићеном месту, у складу са препорукама произвођача;
* подаци треба да буду пренети на нови медијум пре него што постану нечитљиви;
* вишеструке копије вредних података треба чувати на одвојеним медијумима да би се додатно смањио ризик од случајног оштећења или губитка података;
* да би се ограничила могућност губљења података, треба предвидети регистровање преносних медијума;
* покретне преносне медијуме треба користити само ако за то постоји пословна потреба;

Расходовање носача података (медијума)

Када више нису потребни, медијуми су расходују на безбедан начин, применом Процедуре за безбедно расходовање медијума.

Расходовање медијума на безбедан начин Основном суду у Бујановцу врши свођењем на минимум ризика од могућег преузимања осељивих података од стране неовлашћених особа.

Физички пренос носача података (медијума)

Носачи података који садрже информације се штите од неовлашћеног приступа, злоупотребе или оштећења приликом транспорта. Када поверљива информација на медијуму није шифрована, потребно је додатно физички заштити медијум.

Смернице за безбедан транспорт:

* користити поуздани транспорт или курире

У случају транспорта носача података са информацијама, председник суда, заменик преедседика и секретар суда, у договору са овлашћеним лицем за ИКТ одређују лице које ће вршити транспорт и начин транспорта.

Ограничење приступа подацима и средствима за обраду података

Члан 13.

Подацима и средствима за обраду података је неопходно ограничити приступ у складу са утврђеним степеном тајности. Корисницима је дозвољен приступ само мрежи и мрежним услугама за чије коришћење су овлашћени.

Одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа

Члан 14.

Сваком кориснику се додељује право приступа ИКТ систему у складу са радним задацима које обавља. Кориснику се додељују јединствени подаци за логовање и јединствена шифра за логовање, који се не смеју делити са другим корисницима.

Додељивање привилегованих (администраторских) права на приступ врши се на основу одлуке председника Основног суда у Бујановцу.

Забрањено је неовлашћено коришћење општих корисничких идентификатора администратора.

Шифре за приступ општим корисничким идентификаторима администратора се мењају променом корисника.

У Основном суду у Бујановцу једном годишње врши се преиспитивање права корисника на приступ, као и након сваке промене (унапређење, разрешење и крај запослења).

Запосленима, другим радно ангажованим и екстерним корисницима информација и опреме за обраду информација по престанку запослења или истеку уговора укида се право на приступ.

Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију

Члан 15.

Аутентификације корисника којима је одобрен приступ систему врши се путем јединственог корисничког имена и шифре.

Сви корисници су дужни да:

* корисничко име и шифру држе у тајности, не откривају их другим лицима, укључујући и надређене особе;
* избегавају чување корисничког имена и шифре у писаном облику;
* промене шифру када примете да постоји било какав наговештај могућег компромитовања.

Предвиђање одговарајуће употребе криптозаштите ради заштите тајности, аутентичности односно интегритета података

Члан 16.

У циљу заштите података лице у ИКТ служби суда развијају и имплементирају политику коришћења криптографских контрола, и успостављају механизме и систем за управљање кључевима.

Поступак криптографске контроле обухвата:

* анализу и процене потреба примене криптографије у пословним процесима укључујући опште принципе према којима би пословне информације требало да се штите;
* ниво заштите се одређује узимањем у обзир типа алгоритма за криптовање података, јачине и квалитета криптографског алгоритма;

Физичка заштита објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система и обрађују

подаци у ИКТ систему

Члан 17.

Основни суд у Бујановцу предузимаће мере ради спречавања неовлашћеног физичког приступа посебно канцеларијама информатичке службе, сервер сали, активној и пасивној мрежној опреми, као и другим просторијама у којима се налази ИКТ опрема, средства и документи ИКТ система, као и спречавање оштећења и ометања информација.

Контрола физичког уласка

Безбедносне области морају бити заштићене одговарајућим контролама уласка како би се осигурало да је само овлашћеним појединцима дозвољен приступ, у складу са смерницама.

Смернице за контролу физичког уласка:

* евиднетирати датуме и време уласка и изласка посетилаца, а све посетиоце треба надгледати, осим ако њихов приступ није претходно одобрен;
* приступ областима у којима се обрађују или чувају поверљиве информације треба да буде ограничен само на овлашћене особе
* од свих запослених, уговарача и треће стране, као и од свих посетилаца треба захтевати да носе видљиву идентификацију и да известе особље обезбеђења уколико наиђу на посетиоце без пратиоца или примете особу која не носи видљиву идентификацију;

Евиденцију о уласку у безбедносну зону води правосудна стража.

Заштита од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава која чине ИКТ систем

Члан 18.

Постављање и заштита опреме

Опрема се поставља и штити на начин којим се смањује ризик од претњи и опасности из окружења, као и могућношћу неовлашћеног приступа.

Смернице за безбедност опреме:

* Опрема се поставља на месту које се може обезбедити од неовлашћеног приступа;
* Врши се редовна контрола система за обезбеђење, аларма, противпожарне заштите, као и инсталација за воду, струју, гас, електронске комуникације;
* Просторије са опремом треба редовно чистити од прашине;
* Опрема мора бити заштићена од атмосферских падавина;

Помоћне функције за подршку

Опрема се штити од прекида напајања, тако што се:

* помоћна опрема за напајање одржава у складу са спецификацијама опреме произвођача и прописима;
* редовно прегледа и испитује у погледу правилног функционисања и врши поправка кварова;

Одржавање опреме

Опрема се одржава како би се осигурали њена непрекидна расположивост и неповредивост, и то на следећи начин:

* опрема се одржава у складу са препорученим сервисним интервалима и према спецификацијама које је дао испоручилац;
* поправке и сервисирање опреме обавља само особље овлашћено за одржавање;
* осетљиве информације треба избрисати из опреме;
* пре враћања опреме у рад након одржавања, потребно је прегледати како би проверили да није неовлашћено коришћена или оштећена.

Безбедно расходовање или поновно коришћење опреме

Сви делови опреме који садрже медијуме за чување података потребно је верификовати да би се осигурало да су сви осетљиви подаци и лиценцирани софтвери пре расходовања или поновног коришћења безбедно уклоњени.

Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 19.

У циљу обезбеђивања исправног и безбедног функционисања средстава за обраду података, дефинишу се процедуре за руковање средствима, које се односе на отпочињање и завршетак приступа информационом систему, прављење резервних копија, одржавање опреме, руковање носачима података, контролу приступа у просторије са серверском инфраструктуром, комуникационом опремом и системима за складиштење података, као и у случајевивма измештања делова ИКТ система.

Усвајање и примена радних процедура

Основни суд у Бујановцу успоставља радне процедуре које садрже инструкције за детаљно извршење следећих послова:

а) инсталација и конфигурација система;

б) обраду и поступање са информацијама (аутоматски и мануелно);

в) израда резервних копија;

г) процедуре за поновно покретање система и опоравак, које се користе у случају отказа система

Заштита података и средстава за обраду података од злонамерног софтвера

Члан 20.

Злонамерни софтвер обухвата све програме који су направљени у намери да отежају рад или оштете неки умрежен или неумрежен рачунар. Заштита од злонамерног софтвера се заснива на софтверу за откривање злонамерног софтвера и отклањање штете, на познавању информационе безбедности, као и на одговарајућим контролама приступа систему и управљању захтеваним и потребним променама.

Поступак контроле и предузимање мера против злонамерног софтвера

Основни суд у Бујановцу одређује и примењује контроле откривања, спречавања и опоравка, ради заштите од злонамерног софтвера.

Садржај процедуре о заштити од злонамерног софтвера:

* 1. формална забрана коришћења неауторизованих софтвера;
  2. имплементација контрола које спречавају или откривају коришћење неовлашћеног софтвера;
  3. имплементација контрола које спречавају или откривају коришћење познатих или сумњивих компромитованих веб-сајтова;
  4. успостављање формалне политике ради заштите од ризика повезаних са
  5. инсталирање и редовно ажурирање софтвера за откривање злонамерног софтвера и опоравак ради претраживања рачунара и медијума као контролу из предострожности, или на рутинској основи.

Препоручује се доношење и процедуре о антивирусној заштити и процедуре о подизању свести запослених о информационој безбедности.

У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави лицу које обавља послове ИТ техничара.

Заштита од губитка података

Члан 21.

Основни суд у Бујановцу врши израду резервних копија које обухватају системске информације, апликације и податке који су неопходни за опоравак целокупог система у случају наступања последица изазваних ванредним околностима.

Чување података о догађајима који могу бити од значаја за безбедност ИКТ система

Члан 22.

У ИКТ систему формирају се записи о догађајима (логови) у вези са активностима корисника, грешкама и догађајима у вези са информационом безбедношћу.

Заштита информација у записима

Средства за записивање и записане информације су заштићени од неовлашћеног мењања и приступа.

Забрањено је неовлашћено уношење следећих измена:

* мењање типова порука које се записују;
* уношење измена у датотеке са записима или њихово брисање;
* препуњавање медијума за записе, што доводи до отказа записивања догађаја или уписивања преко већ раније записаног.

Обезбеђивање интегритета софтвера и оперативних система

Члан 23.

Инсталацију и подешавање софтвера може да врши само запослени - корисник који има овлашћење за то.

Заштита од злоупотребе техничких безбедносних слабости

ИКТ система

Члан 24.

Основни суд у Бујановцу врши анализу ИКТ система и утврђује степен изложености ИКТ система потенцијалним безбедносним слабостима, и предузима одговарајуће мере које се односе на уклањање препознатих слабости или примену мера заштите.

Уколико се идентификују рањивости које могу да угрозе безбедност ИКТ система, овлашћено лице суда је дужно да одмах изврши подешавања, односно инсталира софтвер који ће отклонити уочене рањивости. Прво се узимају у разматрање системи са високим ризиком.

Члан.25

Ограничења у погледу инсталације софтвера

Забрањено је инсталирање софтвера на уређајима који могу довести до изложености ИКТ система безбедносним ризицима.

Члан 26.

У циљу заштите података у комуникационим мрежама, уређајима и водовима врши се њихова контрола и заштита од неовлашћеног приступа.

Безбедност података који се преносе унутар оператора ИКТ система, као и између оператора ИКТ система и лица ван оператора ИКТ система

Члан 27.

Заштита података који се преносе комуникационим средствима унутар Основног суда у Бујановцу, између оператора ИКТ система и лица ван оператора ИКТ система, обезбеђује се утврђивањем одговарајућих правила и процедура.

Правила коришћења електронске поште

Употреба електронске поште мора бити у складу са успостављеним процедурама и адекватним контролама над спровођењем истих. Електронска пошта се може користити искључиво за пословне потребе; размена порука личног садржаја није дозвољена; сви подаци садржани у порукама или њиховом прилогу морају бити у складу са стандардима заштите података.

Правила коришћења Интернета

Приступ садржајима на Интернету је дозвољен искључиво за пословне намене.

Правила коришћења информационих ресурса

Информациони ресурси се користе искључиво у пословне сврхе, на раду или у вези са радом. Другу намену коришћења посебно одобрава одговорно лице, на образложени писани захтев корисника.

Размена електронских порука

Заштита информација укључених у размену електронских порука се регулише Процедуром о безбедности у размени електронских порука.

Процедура о безбедности у размени електронских порука треба да обухвати:

* заштиту порука од неовлашћеног приступа
* осигурање исправног адресирања и транспорта поруке;
* поштовање законских одредби, на пример захтеве за електронске потписе;
* добијање одобрења пре коришћења јавних спољних услуга, као што су размена хитних порука,приступ и коришћење друштвене мреже или заједничко коришћење датотека;

Члан 28.

У оквиру животног циклуса ИКТ система овлашћено лице у суду је задужено за технички надзор над реализацијом од стране извођача, односно испоручиоца, о успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова ИКТ система о чему води документацију.

Документација из претходног става мора да садржи описе свих процедура, а посебно процедура које се односе на безбедност ИКТ система.

Заштита трансакција апликативних услуга

Информације укључене у трансакције апликативних услуга се штите да би се спречио непотпун пренос, погрешно усмеравање, неовлашћено мењање порука, неовлашћено разоткривање, неовлашћено копирање порука или поновно емитовање.

Трансакције морају да подрже следеће услове:

* Обе стране које учествују у транскакцији морају да примене електронски потпис;
* Приватност свих страна које учествују у трансакцији;
* На комуникационим каналима примењено шифровање;
* Безбедност протокола који се користе у трансакцијама.

Заштита података који се користе за потребе тестирања ИКТ система односно делова система

Члан 29.

За податке који су означени ознаком тајности, односно службености као поверљиви подаци, или су подаци о личности коришћени приликом тестирања система, одговорно је лице овлашћено за приступ и манипулацију тим подацима, у складу са прописима којима је дефинисана употреба и заштита такве врсте података.

Члан 30.

Политика безбедности размене информација у пословним односима са пружаоцима услуга и између независних пружалаца услуга

Уговори који се закључују са пружаоцима услуга који имају приступ информацијама, средствима или опреми за обраду информација Основни суд у Бујановцу морају садржати уговорну одредбу о заштити и чувању поверљивости информација, података и документације.

Пружаоци услуга имају право на приступ информацијама које су крајње неопходне за пружање предметне услуге која је уговорена са судом.

Уговарање обавезе обезбеђивања безбедностиу споразумима

са пружаоцима услуга

Пре отпочињања преговора, потенцијални пружалац услуга у обавези је да потпише изјаву о поверљивости и заштити података, информација и документације, која садржи обавезу за пружаоца услуга да достављене или на други начин учињене доступним информације и подаци могу бити коришћени искључиво на начин претходно одобрен од стране Основног суда у Бујановцу, а за потребе извршења предмета преговора.

Одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга

Члан 31.

У циљу одржавања и обезбеђивања уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга, Основни суд у Бујановцу успоставља мере надзора и заштите за време пружања услуга и након извршеног посла.

Члан 32.

Сви запослени морају бити упознати са обавезом и процедуром извештавања о догађајима у вези са информационом безбедношћу.

Запослени који сматра да је дошло до напада или злоупотребе података мора одмах обавестити овлашћено лице и предузме мере у циљу заштите ресурса ИКТ система, против одговорног лица, могу да се воде дисциплински, прекршајни или кривични поступци.

Прикупљање доказа

Основни суд у Бујановцу дефинише и примењује процедуре за идентификацију, сакупљање, набавку и чување информација које могу да служе као доказ у случају покретања дисциплинског, прекршајног или кривичног поступка.

Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 33.

Основни суд у Бујановцу примењује мере које обезбеђују континуитет обављања посла у ванредним околностима, како би ИКТ систем у што краћем року био у функционалном стању:

* постојање резервне опреме;
* израду резервних копија.

**III ПРЕЛАЗНЕ И ЗАВРШ****НЕ ОДРЕДБЕ**

Члан 34.

Најмање једном годишње врши се провера ИКТ система и евентуалне измене Акта о безбедности, у циљу провере адекватности предвиђених мера заштите, као и утврђених процедура, овлашћења и одговорности у ИКТ систему.

Ступање на снагу Акта о безбедности

Члан 35.

Акт о безбедности ступа на снагу 07.02.2024. године

У Бујановцу, дана 07.02.2024.год. **ВФ ПРЕДСЕДНИКА СУДА,**

**Јелена Петричевић Младеновић**