Р е п у б л и к а С р б и ј а
ВИШИ СУД У НОВОМ ПАЗАРУ
Број: Су-I-1-56/22
Дана: 26.12.2022.године
Нови Пазар

На основу члана 8. Закона о информационој безбедности („Службени гласник РС“ бр.6/16, 94/17 и 77/19), члана 2. Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности инфомационо-коминикационих система од посебног значаја („Сл.гласник РС" бр.94/16), чл.52. Закона о уређењу судова („Сл.гласник РС" бр.111/08, 104/09, 101/10, 31/11, 78/11, 101/11, 101/13, 40/15, 106/15, 13,16, 108/16, 113/17, 65/18, 87/18 и 88/18) и чл.3. и 6. Судског пословника („Сл.гласник РС" бр.110/09, 70/11, 113/15, 39/16, 56/16, 77/16, 16/18, 43/19, 93/19 и 18/22), председник Вишег суда у Новом Пазару, донео је дана 26.12.2022. године.

АКТ О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА ВИШЕГ СУДА У НОВОМ ПАЗАРУ

I ОСНОВНЕ ОДРЕДБЕ

Предмет Акта

Члан 1.

Актом о безбедности информационо-комуникационог система Вишег суда у Новом Пазару (у даљем тексту: Акт о безбедности), у складу са Законом о информационој безбедности („Службени гласник РС“ бр.6/16, 94/17 и 77/19), ближе се дефинишу мере заштите информационо-комуникационих система у Вишем суду у Новом Пазару, а нарочито принципи, начин и процедура постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима информационо-комуникационог система Вишег суда у Новом Пазару (у даљем тексту: ИКТ систем).

Циљеви Акта о безбедности

Члан 2.

Циљеви доношења овог Акта су:

- одређивање начина и процедура за постизање и одржавање адекватног нивоа безбедности система;
- спречавање и ублажавање последица инцидентата којима се угрожава или нарушава информациона безбедност;
- подизање опште свести запослених о значају информационе безбедности, о ризицима и опасностима које су везане за коришћење информационих технологијама и мерама заштите приликом коришћења ИКТ система;
- прописивање овлашћења и одговорност запослених у вези са безбедношћу и ресурсима ИКТ система;
- 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 безбедности служе превенцији од настанка инцидената и минимизацији штете од инцидената и њихова примена је обавезујућа за све кориснике информатичких ресурса, као и за сва трећа лица која користе информатичке ресурсе суда.

Запослени у Вишем суду у Новом Пазару морају бити упознати са садржином Акта о безбедности и дужни су да поступају у складу са одредбама овог акта.

За праћење примене овог Акта надлежан је систем администратор у Вишем суду у Новом Пазару.

Одговорност запослених

Члан 4.

Запослени у Вишем суду у Новом Пазару су дужни да приступају информацијама и ресурсима ИКТ система само ради обављања редовних пословних активности, као и да благовремено информишу надлежног систем администратора у Вишем суду у Новом Пазару о свим сигурносним инцидентима и проблемима.

Непоштовање овог Акта о безбедности, као и свако угрожавање или нарушавање инфомационе безбедности, повлаче 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, податке који се чувају, обрашују, претражују или преносе помоћу електронских уређаја, организациону структуру путем које се управља ИКТ системом, корисничке налоге, тајне информације за проверу веродостојнисти, техничку и корисничку документацију, унутрашње опште акте и

процедуре.

II МЕРЕ ЗАШТИТЕ

Члан 6.

Мерама заштите информационо-комуникационог система Вишег суда у Новом Пазару се обезбеђује превенција од настанка инцидената, односно превенција и смањење штете од инцидената који угрожавају вршење надлежности и обављање делатности суда.

Актом о безбедности ИКТ система Вишег суда у Новом Пазару дефинисане су следеће мере заштите:

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

Члан 7.

Виши суд у Новом Пазару у оквиру организационе структуре утврђује послове и одговорност запослених у циљу управљања инфорамционом безбедношћу.

Правилником у унутрашњој организацији и систематизацији радних места уређене су обавезе и одговорност запослених у Вишем суду у Новом Пазару у вези са управљањем информационом безбедношћу.

2. Постизање безбедности рада ван просторија послодавца и употребе мобилних уређаја

Члан 8.

Виши суд у Новом Пазару дозвољава рад ван просторија послодаваца (увиђај на лицу места, реконструкција, саслушања...) и употребу мобилних уређаја од стране запослених уколико је осигурана безбедност на раду у случају обављања послова ван просторија послодавца, узимајући у обзир и ризике до којих може доћи услед неадекватног коришћења мобилних уређаја.

Рад ван просторија послодавца

Члан 9.

Обављање послова ван просторија послодавца обухвата:

-увиђаје на лицу места у парничном и кривичном поступку;
-реконструкције догађаја;
-одређена саслушања странака;

Рад ван просторија послодавца 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 инфорамционом систему (у даљем тексту: процедура).

VPN процедура дефинише правила и услове за повезивања на мрежу Вишег суда у Новом Пазару са удаљене локације. Правилном применом утврђеног поступка и начина приступа, Виши суд у Новом Пазару своди на минимум потецијалну изложеност штети која може настати услед неауторизваног приступа мрежи.

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

Ауторизованим корисницима није дозвољено да користе мрежу Вишег суда у Новом Пазару за активности које нису у домену пословних активности, радних и других задатака у вези са послом и предметом рада појединачно запосленог.

VPN процедуром дефинисани су захтеви који морају бити испуњени и то:

1. Приступ са удаљених локација мора бити заштићен коришћењем криптографских алгоритама.

2. Ауторизовани корисници морају чувати креденцијале својих налога и не смеју омогућавати присту било ком трећем лицу.

3. Приликом коришћења службеног рачунара за приступ са удаљене локације мрежи Вишег суда у Новом Пазару, ауторизовани корисник не сме истовремено бити повезан и на неку другу мрежу која може угрозити безбедност комуникације.

4. Приступ са удаљене локације мора бити одобрен од стране одговорног лица за надзор спровођења УР^ процедуре.

5. 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 Вишим судом у Новом Пазару.

6. Сви пословни подаци који се креирају приликом рада складиште се у информационом систему. Ради безбедности, пословни подаци се не сладиште на мобилним уређајима.

Рад ван просторија послодавца запослених и других радно ангажованих (ангажованих за рад у просторијама суда) одобрава систем администратор Вишег суда у Новом Пазару.

Коришћење мобилних уређаја

Члан 10.

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 садрже податке и имају могућност повезивања на мрежу. Приликом коришћења мобилних уређаја потребно је осигурати послове информације од могућег компромитовања.

Актом о безбедности ИКТ система у Вишем суду у Новом Пазру дефинише се начин физичке заштите од крађе и активности које је неопходно предузети у случају крађе или губитка мобилних уређаја, односно безбедносног инцидента, како не би било нарушена безбедност.

Виши суд у Новом Пазару спроводи обуку запослених који користе мобилне уређаје, у циљу подизања свести о додатним ризицима до којих долази услед оваквог начина рада.

Процедура у коришћењу мобилних уређаја у Вишем суду у Новом Пазару установљава следећа правила:

1. Сви уређаји морају бити заштићени јаком шифром.

2. На уређајима мора бити инсталирана антивирусна заштита.

3. Мора бити усвојена и оперативна процедура за потпуно брисање података када престаје потреба за чувањем истих.

4. Крађа или губитак мобилног уређаја се мора без одлагања пријавити надлежном лицу за информационе технологије и одговорном лицу, који затим спроводе активности у смислу очувања безбедности. Уколико се уређај пронађе, потребно је предати исти одоговорним лицима.

5. Корисницима није дозвољено да врше измене на хадверу или инсталираном софтверу који је власништво Вишег суда у Новом Пазару без претходне писане дозволе надлежног лица за информационе технологије и одговорног лица.

6. У циљу заштите података надлежно лице за информационе технологије ће евидентирати коришћење мобилних уређаја у одговарајућим логовима, које ће у случају потребе користити за истраживања и утврђивања евентуалних злоупотреба.

Процедура се примењује на све стално запослене, запослене на одређено време или лица ангажована по другим основима, који имају приступ или користе мобилне уређаје у власништву Вишег суда у Новом Пазару.

Право на коришћење мобилних уређаја ван седишта Вишег суда у Новом Пазару се стиче на основу писаног захтева корисника мобилног уређаја упућеног

руководиоцу органа и систем администратору у Вишем суду у Новом Пазару.

Мобилне уређаје који се користе морају бити претходно одобрени и/или набављени од стране Вишег суда у Новом Пазару, и оцењени као компатибилни са захтевима обезбеђења адекватног степена заштите.

Рад ван просторија послодавца може се остварити коришћењем уређаја који нису мобилни (на пример десктоп рачунари). Ови уређаји, при томе, морају имати примењене најмање безбедносне мере као и сродни уређаји који се налазе у окриву мреже, док се за заштиту комуникације морају применити исте мере као и за заштиту комуникације мобилних уређаја. Подешавање ових уређаја врше запослени систем администратор и техничар за ИТ подршку у Вишем суду у Новом Пазару. Корисници ових уређаја морају обезбедити довољно безбедан простор за њихов рад (засебна соба, положај дисплеја такав да се онемогући посматрање од неовлашћених особа и слично).

Систем администратор и техничар за ИТ подршку Вишег суда у Новом Пазару, одговорни су за вођење евиденције о свим уређајима намењеним за рад ван просторија послодавца.

Евиднеција о уређајима треба да садржи податке који су неопходни да би се уређаји и/или корисник недвосмислено идентификовали, као што су произвођач, модел, серијски број, инвентарски број, MAC адреса, IMSI, IMEI, корисник који је задужио уређај његов јединствени матични број и слично.

Корисник мобилног уређаја у обавези је да сваки безбедносни инцидент пријави систем администратору и техничаку за ИТ подршку у Вишем суду у Новом Пазару без одлагања, а најкасније у року од 24 сата да достави писану изјаву о оконостима безбедносног инцидента. Под појмом „безбедносни инцидент“ се сматра крађа, губитак мобилног уређаја или било који други догађај који доводи до нарушавања тајности и интегритета података који се налазе на мобилном уређају.

Запослени техничар за ИТ подршку Вишег суда у Новом Пазару у обавези је да по пријави безбедносног инцидента неодложно блокира несталом мобилном уређају приступ инфорамционом систему и кориснику промене креденцијале за приступ.

У случају да се пронађе мобилни уређај чији нестанак је пријављен, запослени систем администратор–надлежни техничар за АТ подршку у Вишем суду у Новом Пазару, извршиће трајно брисање комплетног медијума за смештање оперативног система, апликација и података и поновну инсталацију оперативног система и потребних апликација. Под појмом „трајног брисања“ се сматра процедура брисање података на тај начин да се искључује могућност накнадног повраћаја тих података, а у складу са препоруком NIST 800-88 Revision 1.

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

Члан 11.

Виши суд у Новом Пазару се стара да запослени који управља ИКТ системом, односно запослени који користе ИКТ систем имају адекватан степен образовања и способности као и свест о значају послова који обављају.

Провера кандидата и услови запошљавања

Члан 12.

Виши суд у Новом Пазару, спроводи радње у циљу провере испуњености услова сваког појединачног кандидата за засполење, у складу са одговорајућим прописима и етичким правилима, сразмерно пословним захтевима, класификацији информација којима ће имати приступ и сагледаним ризицима.

Сви запослени радно ангажовани појединци по другом основу којима је додељен приступ поверљивим информацијама, морају потписати споразум о поверљивости и заштити података информација од трећих лица, пре него што им се дозволи приступ опреме за обраду информација.

Обавезе у току запослења

Члан 13.

Руководилац Вишег суда у Новом Пазару је дужан да захтева од свих запослених и радно ангажованих лица да примењује мере заштите безбедности, у складу са овим актом и важећим процедурама.

Виши суд у Новом Пазару у циљу развоја, инмплементације и одржавања система заштите и безбедности података обезбеђује услове за интерграцију 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;
- Спроводи програме заштите на конзитентан и уједначен начин у свим организационим јединицама;
- Кооридинира безбедност и заштиту података у информационом систему са физичком заштитом истих.

Запослени систем администатор – надлежни техничар за АТ подршку у Вишем суду у Новом Пазару, који је надлежан за праћење, анализу, извештавање и предузимање активности на плану спровођења усвојене политике и процедура, континуирано се обучава у циљу унапређења техничког и технолошког знања.

Запослени систем администатор – надлежни техничар за АТ подршку у Вишем суду у Новом Пазару је ауторизован и 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

Члан 14.

Сви запослени у Вишем суду у Новом Пазару 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

Члан 15.

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

Дисциплински поступак покреће преседник Вишег суда у Новом Пазару, а по предлогу систем администатора у Вишем суду у Новом Пазару.

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

Члан 16.

Запослени 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. Дужности и обавезе које остају важење и после престанка ангажовања и треба да буду садржане у тексту уговора о раду са запосленим и условима заснивања радног односа, односно уговора о ангажовању лица ван радног односа.

Ова мера је ближе одређена актом о безбедности ИКТ у Вишем суду у Новом Пазару.

За поступање приликом престанка запослења и ангажовања задужена је управа суда и систем администатор у Вишем суду у Новом Пазару, који предузима следеће активности:

- Проверавају испуњеност свих услова у погледу чувања и изношења података у електронском и папирном формату,
- Прегледају све налоге и приступе систему који су били доступни запосленом,
- Преузимају од запосленог електронске и друге мобилне уређаје,
- Утврђује начин контакта са бившим запосленим након одласка,
- Проверавају враћене мобилне уређаје и уређаје за преношење података,
- Дају налог за укидање налога електронске поште и свих других права приступа систему Вишег суда у Новом Пазару на дан престанка радног односа или другог

основа ангажовања бившег запсоленог,

- Прегледају све налоге за приступ одлазећег запосленог и прикупљају приступне шифре и кодове са циљем укидања/промене истих на дан одласка,
- Преузимају картице или друге уређаје којима се омогућава приступ пословним просторијама и опреми Вишег суда у Новом Пазару.

5. Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 17.

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

Пописивање имовине

Члан 18.

Виши суд у Новом Пазару врши идентификацију имовине која одговара животном циклусу информацијама и документује њен значај.

Животни циклус информација обухвата креирање, обраду, складиштење, пренос, брисање и уништавање података информација. Виши суд у Новом Пазару прави попис добара који је тачан, ажуран, конзистентан и усклађен са другом имовином.

Евиденција о информационим добрима и средствима и имовини за обраду информационих добара води систем администатор, односно запослен техничар за ИТ подршку у Вишем суду у Новом Пазару.

Власништво над имовином, прихватиљиво коришћење имовине и њен повраћај

Члан 19.

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

Виши суд у Новом Пазару у оквиру интерног акта о руковању имовином уређује правила за прихватљиво коришћење имовине повезане са информацијама и опремом за обраду информација.

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

Током отказног рока запослених, Виши суд у Новом Пазару контролише њихово неовлашћено копирање, умножавање или преузимање релевантних заштићених

информација.

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

Члан 20.

Класификовање података је поступак утврђивања и појединачног додељивања нивоа тајности података, у складу са њиховим значајем за Виши суд у Новом Пазару.

Виши суд у Новом Пазару означава типове и локације података као поверљиве интерне или јавне. Имовина се означава уз помоћ идентификационих налепница које носе одговарајућу класификациону ознаку.

Виши суд у Новом Пазару класификациону шему поверљивости информација базира на четири нивоа:

- Откривање не изазива никакву штету;
- Откривање изазива мању непријатност или мању штету;
- Откривање има значајан краткорочни утицај на пословање или тактичке циљеве;
- Откривање има озбиљан утицај на дугорочне стратешке циљеве или угоржава опстанак.

Виши суд у Новом Пазару врши класификацију ради:

- Јачања корисничке одговорности, како би корисници могли да уоче и препознају пословну вредност података приликом очувања или слања и постану свесни одговорности за неовлашћено коришћење или преношење;
- Подизање свести о вредности информације или документа;
- Заштите података у покрету ради боље и интелигентније интреграције са DLP, WEB gateway и осталим производима за заштит параметара и крајњих уређаја;
- Заштите садржаја;
- Интерграција са системима за архивирање.

Класификација докумената мора да буде усклађена са правилима контрле приступа.

Виши суд у Новом Пазару поступа у складу са усвојеном шемом класификовања података. Посебном процедуром се дефинишу радње за поступање, обраду, складиштење и пренос података.

Процедура о поступању са имовином подразумева следеће:

- Ограничења приступа која подржавају захтеве за заштиту сваког нивоа класификација;
- Одржавање званичног записа о овлашћеним примаоцима имовине;

- Заштита привремених или трајних копија података на нивоу који је у складу са заштитом оригиналне информације;
- Складиштење информационе имовине у складу са спецификацијама произвођача;
- Јасно обележавање свих копија медија на које је овлашћени прималац треба да обрати пажњу.

7. Заштита носача података

Члан 21.

Виши суд у Новом Пазару обезбеђује спречавање неовлашћеног откривања, модификовање, уклањања или уништења података који се чувају на носачима података.

Евиденција носача на којима су снимњени подаци, води се од стране систем администатора, односно техничара за ИТ подршку Вишег суда у Новом Пазару.

Управљање преносним носачима података (медијума)

Члан 22.

Виши суд у Новом Пазару је дужан да развија и имплементира процедуру о управљању преносним носачима, у складу са усвојеном шемом класификовања података.

Процедура о управљању преносним носачима садржи следеће одредбе:

- Садржај сваког медијума који се може поново користити и који ће се износити изван организације, онда када више није потребан треба да се неповратно избрише;
- За све медијуме који се износе из организације онда када је то неопходно и изводљиво, треба захтевати одобрење, а о свим таквим изношењима треба водити евиденцију, како би се сачувао траг за проверу;
- Све медијуме треба складишити на безбедном и заштићеном месту, у складу са препорукама произвођача;
- Коришћење криптографских техника за заштиту података на преносним медијумима, ако су поверљивост или интергритет података важни;
- 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 преносивих медија;
- Покретне преносне медијуме треба користити само ако за то постоји пословна потреба;
- Уколико постоји пословна потреба за коришћење преносних медија, неопходно је пратити пренос података на такве медијуме.

Расходовање носача података (медијума)

Члан 23.

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

Расходовање медијума на безбедан начин Виши суд у Новом Пазару врши свођењем на минимум ризика од могућег преузимања осетљивих података од стране неовлашћених особа.

Процедуру за безбедно расходовање медијума који садрже поверљиве податке утврђени су различити начини процеса расходовања, а у складу са осетљивошћу података.

Процедура за безбедно расходовање медијама даје следеће смернице:

- Неопходно је уредити начин за идентификовање медијума који садрже осетиљиве податке за које ће можда бити потребно безбедно расходовање;
- Медијуме који садрже осетљиве податке треба расходовати спаљивањем или кидањем, или брисањем података ради коришћења у неком другом апликативном програму унутар организације;
- Расходовање медијума који садрже осетивље податке је потребно евидентирати, како би се сачувао траг за проверу.

Физички пренос носача података (медијума)

Члан 24.

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 заштитити медијум.

Смернице за безбедан транспорт су:

- Користири поуздани транспорт или курире,
- Потребно је увести проверу идентитета курира;
- Карактеристике опреме за пренос морају да буду такве да обезбеде заштиту од свих физичких оштећења која би могла настати током преноса.

У случају транспорта носача података са информацијама, председник суда у договору са запосленим у ИКТ служби суда одређује лице које ће вршити транспорт и начин транспорта.

8. Ограничење приступа подацима и средствима за обраду података

Члан 25.

Подацима и средствима за обраду података је неопходно ограничити приступ у

складу са утврђеним степеном тајности података и усвојеном шемом класификовања података према чл.11. овог акта.

Виши суд у Новом Пазару ће формирати контролну листу приступа која садржи попис свих информационих обејаката и субјекте који им могу приступити.

Корисницима је дозвољен приступ само у мрежи и мрежним услугама за чије коришћење су овлашћени.

Виши суд ће у Новом Пазару ће посебним документом уредити приступ мрежи и мрежним уређајима.

Процедура о приступу мрежи и мрежним уређајима садржи следеће:

- Листа мрежа и мрежних услуга којима је приступ дозвољен;
- Начини ауторизације ради утврђивања коме је одобрен приступ, којој мрежи и којим услугама;
- Средства која се користе за приступ мрежи и мрежним услугама;
- Захтеви у погледу верификације корисника за приступ различитим мрежни услугама;
- Начини надгледања коришћења мрежних услуга.

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

Члан 26.

Виши суд у Новом Пазару управља приступом ИКТ системом и услугама кроз употребу корисничких идентификатора.

Управљање корисничким идентификаторима врши се уз поштовање следећих принципа:

- Кориснички идентификатори су јединствени, тако да се корисници могу везати уз њих и учинити одговорним за своје активности;
- Коришћење заједничких идентификатора дозвољава се само онда када је то погодно за обављање посла уз претходно одобрење;
- Корисницима којима је престао радни однос или период ангажовања тренутно се онемогућавају или уклањају кориснички идентификатори;
- Периодично идентификовање и уклањање или онемогућавање вишеструких корисничких идентификатора;
- Вишеструки идентификатори неког корисника се не издају другим корисницима.

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 (администаторских) права на приступ врши се на основу одлуке председника Вишег суда у Новом Пазару.

Привилегована права на приступ додељују се посебно за сваки системски објекат уз дефинисани рок трајања тих права.

Привилегована права на приступ која треба доделити корисничком идентификатору другачија су од оних која се користе за редовне активности.

Редовне пословне активности не треба вршити из привилегованих корисничких идентификатора.

Компетенције корисника са привилегованим правима на приступ се редовно преиспитују ради провере да ли су у складу са њиховим обавезама.

Забрањено је неовлашћено коришћење општих корисничких идентификатора администатора.

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

Виши суд у Новом Пазару једном годишње врши 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.

10. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију

Члан 27.

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.

Шифре морају да:

- Садрже најмање девет алфанумеричких карактера;

- Садрже најмање једно велико и једно мало слово;
- Садрже најмање један број (0-9).

Шифре не заснивати на личним подацима корисника као што су име, телфонски број или датум рођења и не смеју садржати више од три узастопна идентична бројчана или словна знака.

Корисницу су дужни да привремене шифре промене приликом првог пријављивања на систем.

11. Предвиђање одговарајуће употребе криптозаштите ради заштите тајности, аутентичности и интегритета података

Члан 28.

У циљу заштите података Виши суд у Новом Пазару развија и имплементира политику коришћења криптографских контрола и успоставља механизме и систем за управљање кључевима.

Криптозаштита обезбеђује:

- Аутентификацију (идентификацију корисника и других ситемских ентитета који захтевају приступ или одобрење акције корисника);
- Непорецивост (примена криптографских техника, најчешће дигиталног потписа, како би се добила потврда о извештавању или неизвештавању неке акције од стране појединачног корисника);
- Поверљивост (применом шифровања врши се заштита осетљивих или критичних информација које се складиште или преносе);
- Интергритет (непроменљивост података који се преносе).

Поступак криптографске контроле обухавата:

- 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 алгоритама за криптовање података, јачине и квалитета криптографског алгоритма;
- Примену шифровања за заштиту осетљивих података приликом преноса мобилним или другим медијумима, уређајима или преко комуникационих водова;
- Управљање кључевима (заштита криптографских кључева, повраћај шифрованих података у случају губљења, компримитовања или оштећење кључева).

Управљање кључевима

Члан 29.

Виши суд у Новом Пазару примењује следеће методе за управљање кључевима које обухватају њихов цео животни циклус:

- Генерисање кључева;
- Издавање и добијање сертификата за јавне кључеве;
- Складиштење кључева (кључеви се чувају на посебним уређајима или паметним картицама, на месту које је физички обезбеђено);
- Дистрибуцију кључева (додела кључева намењеним ентитетима и активација самог кључа);
- Замену или ажурирање кључева;
- Поступак у случају компромитовања кључева;
- Деактивацију кључева;
- Обнављање изгубљених или оштећених кључева;
- Прибављање резервних копија или архивирање кључева;
- Уништавање кључева;
- Евидентирање и проверу активности у вези са управљањем кључева.

Кључеви се могу користити само у периоду који одреди председник Вишег суда у Новом Пазару у договору са запосленим систем администатором.

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

Члан 30.

Виши суд у Новом Пазару је дужан да предузме 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 средстава и документи ИКТ система, као и спречавање оштећења и ометања информација.

Зона раздвајања и успостављање система физичке безбедности

Члан 31.

Опрема за обраду информација се штити закључавањем просторија у којима се налази.

У складу са проценом ризика дефинисане су следеће зоне раздвајања: канцеларија информатичке службе, сервер сала (сервер соба), главни дистрибутивни панел (ГДП) и дистрибутивни панели (ДП) са активном и пасивном мрежном опремом.

Зоне раздвајања су:

- Зоне раздвајања у згради или на локацији која садржи опрему за обраду информација треба да буду физички исправне (тј. не треба да постоје процепи у зони или области у којој би се лако могао десити упад); спољни кров, зидови и подови на тој локацији треба да буду од чврстог материјала, а сва спољна врата треба да буду потпуно заштићена од неовлашћеног приступа помоћу контролних механизама, нпр. решеткама, алармима, бравма итд.; врата и прозори треба да буду закључани у свим случајевима када су без надзора, а када су у питању прозори треба размотрити спољну заштиту посебно у

приземљу;

- Треба поставити пријавнице са особљем или друга средства за контролу физичког приступа до локације или зграде; приступ локацијама или зградма треба да буде ограничен само на овлашћено особље;
- Онда када је то применљиво, треба да буду изграђене физичке препреке како би се спречио неовлашћени физички приступ и загађење из околине;
- Сва пожарна врата у безбедносној зони раздвајања треба да имају алармни уређај, да буду под надзором и да се испитују на спој са зидовима како би се успоставио потребан ниво отпорности у складу са одговарајућим регионалним, националним и међународним стандардима; треба да функционишу у складу са локалним противпожарним правилима у погледу осигурања од отказа;
- Да би се надледала сва спољна врата и доступни прозори, треба поставити против – провалне алармне системе у складу са националним, регионалнимили међународним стандарадима; области без особља треба да буду под алармом у сваком тренутку; надзор треба такође обезбедити и за друге области, нпр. за просторије са рачунарима или за просторије за комуникације;
- Опрема за обраду информација којом управља организација треба да буде физички одвојена од оне којом управљају трећа лица.

Контрола физичког уласка
Члан 32.

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

Контрола физичког уласка подразумева:

- Евидентирати датуме и време уласка и изласка посетилаца, а све посетиоце треба надгледати осим ако је њихов приступ није претходно одобрен; приступ треба одобравати само за специфичне, ауторизоване сврхе и издавати упутство о захтевима за безбедност области и о процедурама за ванредне ситуације;
- Приступ областима у којима се обрађују или чувају поверљиве информације треба да буде ограничен само на овлашћене особе, применом одговарајућих контрола приступа, нпр. имплементацијом двофакторских механизама за проверу веродостојности, као што су картице за приступ и тајни лични идентификациони број;
- Треба безбедно одржавати и надгледати евиденцију или електронску проверу свих приступа;
- 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;
- Запосленима код пружаоца услуга обезбеђења треба одобрити ограничен приступ безбедносним областима или опреми за обраду осетљивих података и омогућити када за то постоји потреба; овакав приступ треба да буде одобрен и надгледан у сваком тренутку;
- Права приступа безнедносним областима треба редовно преиспитивати и ажурирати, а уколико постоји потреба и укинути.

Заштита канцеларија, просторија, средстава, као и заштита од претњи екстерних фактора из окружења

Члан 33.

Виши суд у Новом Пазару обезбеђује и примењује одговарајућу контролу приступа, чиме се омогућава физичка безбедност канцеларија, просторија и средстава. Такође, безбедним конфигурисањем се онемогућава приступ кључној опреми, а у циљу спречавања видљивости поверљивих информацијама, активностима споља. Физичка заштита се мора планирати за случајеве природних катастрофа, непријатељских напада или несрећа.

Рад у безбедносни зонама

Члан 34.

Безбедносне зоне подлежу следећим мерама заштите:

- Особље мора бити обавештено о активностима унутар безбедносне зоне;
- Забрањује се рад без надзора у безбедносним зонама;
- Безбедносне зоне које се не користе морају бити физики закључане и чија провера се врши периодично;
- Не дозвољава се уношење фотографских, видео, аудио или других уређаја за записивање, осим уз претходно одобрење одговорног лица.

Евиденцију о уласку у безбедносну зону води правосудна стража и запослени техничар за ИТ подршку.

13. Заштита од губитка, оштећења, крађе или другог облик аугрожавања безбедности средстава која чине ИКТ систем

Постављање и заштита опреме

Члан 35.

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;
- Опрема за обраду информација која служи за приступ и коришћење осетљивих података се поставља на места која нису видљива неовлашћеним особама;
- 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;
- Забрањено је конзумирање хране и пића и пушење у близини опреме за обраду информација;

- Редовно се прате температура и влажност ваздуха;
- Опрема мора бити заштићена од атмосферских падавина;
- Опрема у индустријском окружњу се штити применом специјалних метода заштите.

Правосудна стража и запослени техничар за ИТ подршку у Вишем суду у Новом Пазару редовно прате услове околине, као што су температура и влажност који би могли негативно да утичу на рад опреме за обраду информација.

Помоћне функције за подршку

Члан 36.

Опрема се штити од прекида напајања, тако што се:

- Помоћна опрема за напајање одржава у складу са спецификацијама опреме произвођача и прописима;
- Капацитет помоћне опреме редовно процењује;
- Редовно прегледа и испитује у погледу правилног функционисања и врши поправке кварова;
- Обезбеђује вишеструко напајање са различитих траса.

Безбедносни елементи приликом постављања каблова

Члан 37.

Каблови за напајање и телекомуникациони каблови који преносе податке или који представљају подршку информационим услугама штите се од прислушкивања, ометања или оштећења на следећи начин:

- Водови напајања и телекомуникациони водови који улазе у просторије за обраду информација су подземни, онда када је то могуће, или имају адекватну алтернативну заштиту,
- Каблови за напајање се одвајају од комуникационих каблова да би се спречиле сметње,
- За осетљиве или критичне системе се постављају оклопљени водови, користе се закључане просторије или кутије и примењују се електромагнетско оклапање ради заштите каблова,
- Неовлашћено прикључење уређаја на каблове се врши технички претраживањем и физичком провером,
- Приступ до разводних табли и у просторије за каблове се контролише.

Одржавање опреме

Члан 38.

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

- Опрема се одржава у складу са препорученим сервисним интервалима и према спецификацијама које је дао испоручилац,
- Поправке сервисирање опреме обавља само особље овлашћено за одржавање,
- О свим сумњивим или стварним неисправностима, као целокупном превентивном и корективном одржавању сачувају записи,
- Осетљиве информације треба избрисати из опреме,
- Пре враћања опреме у рад након одржавања, потребно је прегледати како би проверили да није неовлашено коришћена или оштећена.

Измештање и премештање имовине

Члан 39.

Опрема, информације или софтвер се измештају само уз одобрење одговорног лица, а током измештања се примењују следећа правила:

- Треба да се одреде запослени и спољни корисници који имају овлашћења да одобре измештање имовине,
- Треба да се поставе временска ограничења за измештање опреме и да се проверава усклађеност приликом повратка,
- Треба документовати идентитет и улогу лица која користе или поступају са имовином приликом премештања и ова документација треба да буде враћена са опремом, информацијама или софтвером.

Безбедност измештене опреме и имовине

Члан 40.

На измештену опрему треба применити безбедносне механизне заштите, узимајући у обзир различите ризике приликом рада изван просторија.

Безбедно расходовање или поновно коришћење опреме

Члан 41.

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.

Безбедност опреме корисника без надзора

Члан 42.

Корисници треба да обезбеде да опрема која је без надзора има одговарајућу заштиту, у циљу онемогућавања приступа заштићеним информацијама и подацима.

Остављање осетљивих и поверљивих докумената и материјала

Члан 43.

Сва осетљива и поверљива документа и материјали морају да буду уклоњени са радне површине и одложени на одговарајуће место које се закључава у периоду када запослени није присутан на свом радном месту и никада се документа и материјали не користе.

Процедура за остављање осетљивих и поверљивих документата и материја је следећа:

1. Све осетљиве и поверљиве информације у штампаном или електорнском облику запослени морају одложити на сигутно место на крају радног дана или када нису присутни на свом радном месту.

2. Рачунари морају бити закључани у одсуству запосленог и угашени на крају радног дана.

3. Ормари и фиоке у којима се чувају поверљиви подаци морају бити закључани када се не користе, а кључеви нер смеју бити остављени на приступаном месту без надзора.

4. Лаптопови морају бити везани уз помоћ одговарајуће опреме или закључани у фиоци. Таблети и остали прености уређаји морају бити закључани у фиоци.

5. Носачи података као што су дискови и flash меморија морају бити одложени и закључани.

6. Шифре за приступ не смеју бити написане и остављене на приступачном месту.

7. Штампани материјал који садржи осетљиве информације се мора одмах преузети са штампача приликом штампања.

8. Материјал који је намењем за бацање треба уништити или одложити на место које се закључава, а које је намењено за одлагање такве врсте материјала.

14. Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 44.

У циљу обезбеђивања исправног и безбедног функционисања средтава 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, конторлу приступа у просторије са серверском инфраструктуром, комуникационом опремом и системима за складиштење података, као и у случајевима измештања делова ИКТ система.

Усвајање и примена радних процедура

Члан 45.

Виши суд у Новом Пазару успоставља радне процедуре које садрже инстукције

за детално извршење следећих послова:

а) инсталација и конфигурација система,

б) обраду и поступање са информацијама (аутоматско и мануелно),

в) израда резервних копија,

г) обрада захтева за временски распоред активности,

д) израда инструкција за поступање у случају грешке или у другим ванредним ситуацијама која могу да настану у току изршавања посла, укључујући ограничења у коришћењу системских помоћних функција,

ђ) утврђивање листе контаката за подршку и ескалацију (укључујући екстерне контакте за подршку) у случају неочекиваних оперативних или техничких потрешкоћа,

е) израда инстукација за управљање поверљивим подацима,

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

з) управљање системским записима (логовима),

и) процедуре за надледање.

За усвајање, измене и допуне радних процедура овлашћен је председник Вишег суда у Новом Пазару у сарадњи и на предлог систем администратора суда.

Управљањем расположивим капацитетима

Члан 46.

Коришћење ресурса се континуирано надлегда, подешава и пројектује у складу са захтевним капацитетима, како би се осигурале неопходне перфомансе система. Периодично се спроводе следеће активности:

а) брисање застарелих података,

б) повлачење из употребе апликација, система, база података или окружења,

в) оптимизација серије процеса и распореда,

г) одбијање или ограничавање пропусног опсега услуга захтеваних у погледу ресурса, ако оне нису критичне за пословање.

Раздвајање окружења за развој, испитивање и рад

Члан 47.

Окружења за развој, испитивање и рад су међусобно раздвојена, како би се смањио ризик од неовлашћеног приступа или промена у радном окружењу.

Смернице за раздвајање су:

а) треба дефинисати и документовати правила за преношење софтвера из развојног статуса у оперативни статус,

б) развојни и опетативни софтвери треба да се извршавају на различитим системима или рачунарским процесорима, као и у различитим доменима или директоријумима,

в) промене у оперативним системима и апликцацијама треба испитивати у

окружењу за испитивање или режиму одржавања пре него што се примене на оперативне системе,

г) испитивање не треба да се ради на оперативним системима, осим у изузетним околностима,

д) компајлери, едитори и други развојни алати или системски помоћни програми не треба да буду доступни из оперативних система, ако се то не захтева,

ђ) да би се смањио ризик од грешке, корисници треба да примењују различите корисничке профиле за оперативне и системе за испистивање, а менији трега да приакзју одговарајуће идентификационе поруке,

е) осетљиве податке не треба копирати у системско развојно окружење, осим ако нису обезбеђене еквивалентне контроле за систем за испитивање.

За обезбеђивање исправног и безбедног функционисања средстава за обраду података и примену радних процедура задужен је запослени техничар за инфорамционо-техничку подршку у Вишем суду у Новом Пазару.

15. Заштита података и средства за обраду података од злонамерног софтвера

Члан 48.

Злонамерни софтвер обухвата све програме који су направљени у намери да отежају рад или оштет нки 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 захтевиним и потребним променама.

Поступак контроле и предузимање мера против злонамерног софтвера

Члан 49.

Виши суд у Новом Пазару одређује и примењује контроле отлривања, спречавања и опоравка, ради заштите од злонамерног софтвера.

Процедура о заштити од злонамерног софтвера је следећа:

1. Формална забрана коришћења неауторизованих софтвера,

2. Имплементација контрола које спречавају или откривају коришћење неовлашћеног софтвера,

3. Имплементација контрола које спрчавају или откривају коришћење познатих или сумњивих компромитованих веб-сајтова,

4. Успостављање формалне политике ради заштите од ризика повезаних са добијеањем датотека и софтвера од или пркео спољних мрежа, или на било ком другом медијуму, указујући на то које заштитне мере треба предузети,

5. Смањење рањивости које може да експлоатише непријатељски софтвер, нпр.кроз управљање техничким рањивостима,

6. Спровођење редовних преиспитивања софтвера и садржаја података у системима који подржавају критичне пословне процесе, пристусво било каквих неодобрених датотека или неауторизованих допуна треба формално истражити,

7. Инсталирање и редовно ажурирање софтвера за откривање злонамерног софтвера и опоравака ради перетраживања рачунара и медијума као контролу из предосторжности или на рутинској основи

Листа провера која се спроводе:

а) проверу, пре коришћења, свих датотека на електронским или оптичким медијумима, као и датотека примљених преко мрежа, да ли садрже злонамерни софтвер,

б) проверу, пре коришћења, садржаја прилога електронске поште и преузетих садржаја, да ли садрже злонамерни софтвер, ову проверу треба спроводити на разним местима, нпр: на серверима за електронску пошту, на стоним рачунарима или приликом уласка у мрежу оператора ИКТ система,

в) проверу постојања злонамерних софтвера на веб страницама,

г) дефинисање процедура за менаџмент и одговорност за поступање са заштитом од злонамерног софтвера у системима, обука за њихово коришћење, извештавање и опоравак од напада злонамерним софтвером,

д) припрему одговарајућих планова за континуитет пословања приликом опоравка од напада злонаметним софтвером, укључујући све неопходне резервне копије података и софтвера и механизме за опоравак,

ђ) имплементацију процедура за редовно прикупљање информација, као што је претплата на адресне спискове за доставу или провера веб – страница на којима се дају информацијама о новим злонамерним софтверима,

е) имплементацију процедура за верификовање информација о злонамерним софтверима и обезбеђење да су упозоравајући извештаји тачни и информативни, руководиоци треба да се осигурају да се за разликовање лажних од стварних злонамерних софтвера користе квалификовани извори, нпр: проверени часописи, поуздане странице на интернет мрежи или испоручиоци програма против злонамерних софтвера, сви корисници треба да буду свесни проблема појаве духовитих или злонамерних обмана и онога што треба да раде после њиховог пријема.

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

У случају да корисник примети необично понашање рачунара, запажење треба без одлагања да пријави информатичкој служби Вишег суда у Новом Пазару.

У циљу заштите о упада у ИКТ систем, систем администратор или техничар за ИТ подршку у Вишем суду у Новом Пазару дужан је да одржава систем за спречавање упада.

Корисницима који су прикључени на ИКТ систем, у случају доказане злоупотребе Интернета, систем администратор односно техничар за ИТ подршку у Вишем

суду у Новом Пазару, може укинути приступ.

16. Заштита од губитка података

Члан 50.

Виши суд у Новом Пазару врши израду резервних копија које обухватају системске информације, апликације и податке које су неопходни за опоравак целокупног система у случају наступања последица изазваних ванредним околностима.

Резервне копије информација и података

Члан 51.

Резервне копије информација, софтвера и дупликати система се редовно израђују и испитују.

Заштитне копије корисницима обезбеђују корисничке податке, функционалност сервиса и апликација након уништења или оштећења која су настала услед хакерских напада, отказа хардвера, грешака корисника, природних катастрофа и других несрећа.

Под заштитним копијама подразумева се прављење резервних копија корисничких података, конфигурационих ОС фајлова, критичних фајлова за функционисање оперативних система (серверских, корисничких и комуникационих) или целих оперативних система, апликација, сервиса и базе података.

Заштитне копије треба да омогуће брзо и ефикасно враћање у функцију система у случају нежељених догађаја и треба их правити у време када се не умањује расположивост сервиса, апликација, база података и комуникационих капацитета ИКТ система.

За чување заштитних копија користе се магнетне траке, екстерни хард дискови и С^/ОУЂ медији.

Систем администратор у Вишем суду у Новом Пазару извршаваће следеће задатке:

- Процењује осетљиве и критичне податке за које је потребно правити резервне кпије,
- Креира план прављења резервних копија,
- Прави заштитне копије серверско оперативног система и поатака комуникационог оперативног система и конфигурационих фајлова, апликација, сервиса и база података,
- Верификују успешно прављење резервних копија,
- Води евиденцију урађених резервних копија,
- Одлаже копије на безбедно место,
- Тестира исправност резервних копија и процедуре за прављење резервних копија,
- Рестаурира податке са резервних копија.

Плана израде резервних копија информацциија обухвата следеће:

- Тачне и потпуне записе о резервним копијама и документоване процедуре објављања,
- Обим и учесталост израде резервних копија,
- Резервне копије треба да одражавају пословне потребе организације и критичност тих информација по континуитет пословања организације,
- Треба их скадиштити на локацији на довољној удаљености, како би се избегло свако оштећење на главној локацији,
- Резервних копијама информација треба дати одговарајући ниво физичке заштите и заштите од утицаја околинме (описане у тачки 12) који је доследан мерилима која се примењују на главној локацији,
- Медијуме са резервним копијама треба редовно проверавати, ради сигурности њихове употребе у ванредним ситуацијама и када је то неопходно,
- У ситуацијама у којима је важна поверљивост, резервне копије треба заштити помоћу шифровања.

За заштиту од губитка података одговоран је председник суда и систем администратор – руководилац информатичке службе у Вишем суду у Новом Пазару.

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

Члан 52.

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

Записивање догађаја

Члан 53.

Виши суд у Новом Пазару прави записе о догађајима и бележи активност догађаја грешке и догађај у вези са информационом безбедношћу који се морају чувати и редовно преиспитивати.

Систем администратор односно техничар за ИТ подршку у Вишем суду у Новом Пазару немају дозволу да бришу или деактивирају дневнике о сопственим активностима.

Записи о догађајима садрже:

- Идентификаторе корисника,
- Активности система,
- Датуме, време, и детаље кључних догађаја, нпр: пријављивање и одјављивање,
- Идентитрет или локацију уређаја, ако је могуће и идентификатор система,
- Записе о успешним и одбијеним покушајима приступа систему,

- Записе о успешним и одбијеним покушајима приступа подацима и др. ресурсима,
- Промене у конфикурацији система,
- Коришћење привилегије,
- Коришћење системских помоћних функција и апликација,
- Датотеке којима се приступало и врсте приступа,
- Мрежне адресе и протоколе,
- Аларме које је побудио систем за контролу приступа,
- Активирање и деактивирање система заштите, као што су антивирусни системи и системи за откривање упада.

Заштита информација у записима

Члан 54.

Средства за записивање и записне 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 догађања или уписивања већ раније записаног.

Записи администратора и оператора

Члан 55.

Активности администратора и оператора система се записују, а записи штите и редовно преиспитују.

Власници привилегованих корисничких навода могу бити у стању да управљају записима на опреми за обраду информације која је под њиховом директном контролом на који се начин штите и прегледају записи да би се одржала одговорност за привилеговане кориснике.

Сатови свих одговарајућих система за обраду онформација заштите морају бити синхронизовани по Гриничком средњем времену.

За чување података о догађајима који могу бити од значаја за безбедност ИКТ система, задужен је систем администратор у Вишем суду у Новом Пазару.

18. Обезбеђивање интегритета софтвера и оперативних система

Члан 56.

Виши суд у Новом Пазару спроводи процедуре у којима се обезбеђује контрола интегритета инсталираног софтвера и оперативних система, у складу са смерницама за контролу промена и инталацију софтвера.

Контрола промена и инсталацију софтвера обухвата:

- Ажурирање оперативног софтвера, апликација и програмских библиотека могу да обављају само оспособљени администратори, по добијању одговарајућег овлашћења од руководиоца,
- Оперативни системи треба да садрже само одобрене извршне кодове, а не и развојне кодове или кобпилаторе,
- Апликационе или оперативни системски софтрвер треба имплементирати тек после обимног и успешно спроведеног испитивања, које обухвата испитивање применљивости, безбедности, утицаја на друге системе и погодности за коришћење, а треба их спровоидити на засебним системима, односно тестним окружењима,
- Треба осигурати да су све одговарајуће библиотеке изворних програма ажуриране,
- Пре имплементације било каквих промена, треба успоставити стратегију повратка на преходно стање, приликом свих ажурирања на библиотекама оперативних програма, треба одржавати записе за проверу,
- Као меру предострожност за неочекиване ситуације треба сачувати претходне верзије апликативног софтвера.
- Старије верзије софтвера треба архивирати, заједно са свим потребним информацијама и параметрима, процедурама, детаљима конфигурације и софтвером за подршку, све док се подаци не држе у архиви.

Инсталацију подешавања софтвера може да врши само запослени систем администратор у Вишем суду у Новом Пазару који има овлашћења само за то.

19. Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 57.

Виши суд у Новом Пазару 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.

Управљање техничким рањивостима

Члан 58.

Виши суд у Новом Пазару благовремено прикупља информацију о техничким рањивостима информационих система који се користе, вреднује изложеност тим рањивостима и предузима одговарајуће мере, узимајући у обзир припадајућих ризика.

Посебне информације клоје су потребне за подршку управљања техничким рањивостима обухватају продавца софтвера, бројеве верзија, текуће стање размештаја, као и особе које су одговорне за тај софтвер.

Поступак управљања техничким рањивостима подразумева следеће:

- Виши суд у Новом Пазару дефинише и успоставља улоге и одговорности у вези са управљањем техничким рањивостима, укључујући надзор, оцену ризика услед утврђене рањивости, исправке, следљивост имовине и све одговорности за потребна координирања,
- Најмање једном месечно а по потреби чешће, врши анализу дневника активности (activitylog, history, securitylog, transactionlog и др.) у циљу идентификације потенцијалних слабости ИКТ система,
- За софтверске и друге технологије (засноване на списку имовине) се одређују информациони ресурски за идентификовање одговарајућих техничких рањивости и за одржавање свести о истима, ови информациони ресурски се ажурирају на основу измена у инвентару или онда када се идентификују нови или други корисни ресурси,
- Дефинише се временски распоред реаговања на обавештење о могућим техничким рањивостима.
- Када је могућа техничка рањивост идентификована, тада се идентификују припадајући ризици и акције, које треба предузети, такве акције могу да обухвате исправке рањивих система и/или примену других контрола,
- У зависности од тога колико хитно треба неку техничку рањивост узети у разматрање, преузете активности се спроводе у складу са контролама које су везане за управљање променама или спровођењем процедура за одговор на инциденте нарушавања безбедности,
- Ако је исправка доступка од легитимног извора, онда се оцењују ризици у вези са инсталирањем те исправке (ризике који настају услед рањивости треба упоредити са ризиком везаним за инсталирање исправке),
- Исправке се морају прво испробати и вредновати пре него што се трајно угради како би се осигурало да ће оне бити ефективне и да неће довести до споредних утицаја који се не могу толерисати, ако исправка није на располагању, онда треба размотрити друге контоле као што су деактивирање услуга или могућности које се односе на рањивост, прилагођавање или додавање контрола приступа (нпр. Заштитну баријеру на границама мреже или појачано надгледање како би се открили или спречили постојећи напади и утицало на повећање свести о рањивости),
- О свим предузетим процедурама се праве записи за проверу, а процес управљања техничким рањивостима треба редовно надгледати и вредновати како би се осигуралњ његова ефективност и ефикасност,
- Најрпе се узимају у разматрање системи са високим ризиком,
- Ефективан процес управљања техничким рањивостима се усклађује са активностима које се однсое на управљање инцидентима, тако да обезеди техничке процедуре које треба спровести ако се догоди неки инцидент,
- Креира се процедура која узима у обзир ситуацију у којој је идентификована рањивост, али не постоји погодна контрамера. У овој ситуацији, организација треба да процени ризик у односу на познате рањивости и дефинише одговарајуће мере за откривање, као и корективне мере.

Уколико се идентификују рањивост које могу да угрозе безбедност ИКТ система, систем администратор односно техничар за ИТ подршку у Вишем суду у Новом Пазару, дужни су да одмах изврше подешавања, односно инсталира софтвер који ће отклонити уочене рањивости. Прво се узимају у разматрање системи са високим ризиком.

Ограничења у погледу инсталације софтвера

Члан 59.

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

Посебним актом је дефинисано које врсте софтвера запослени сме да инсталира, а које су забрањене.

20. Обезбеђивање да активности на ревизији ИКТ система имају што мањи утицај на функционисање система

Члан 60.

Приликом спровођења ревизије и ИКТ система, Виши суд у Новом Пазару обезбеђује да ревизија има што мањи утицај на функционисање система.

Поступак контроле информационих система:

- Са руководством су договорени захтеви за проверу приступа систему и подацима,
- Предмети подруђја испитивања за проверу су уанпред договрени и строго конторлисани,
- Испитивања за проверу су ограничена на приступ читањем,
- Приступ који није ограничен само на читање треба дозволити само за добијање издвојених копија системских датотека које се по завршеној провери бришу или се одговарајући штите уколико посстоји обавеза да се такве датотеке чувају према захтевима за документовае провере,
- Захтеви за посебну или допунску обраду морају бити идентификовани и о томе мора бити сачињен писани споразум,
- Испитивања за проверу могу утицати на доступност система, па се покрећу ван радног времена,
- Сав приступ се надгледа и записује се да би се направио референтни траг.

Планирање и спровођење ревизије ИКТ система може да врши само систем администратор у Вишем суду у Новом Пазару односно запослени корисник који има овлашћење за то.

21. Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 61.

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

Спецификација мрежних услуга, било да се оне пружају унутар самог Вишег суда у Новом Пазару, било од стране трећих лица, укључујући механизме безбедности, врсте услуга утврђених за захтев руководства. Мрежне услуге обухватају обезбеђивање

прикључака, услуга на приватним мрежама и мреже са допдатним функцијама, као и решења за упављање безбедношћу (заштита и системи за откривање упада).

У мрежама су међусобно раздвојене групе инфорамционих услуга, корисника и система, а мрежни администратор је одговоран за управљање мрежом.

Сустем администратор у Вишем суду у Новом Пазару, дужан је да стално врђи контролни прегледе мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности.

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

Члан 62.

Заштита података који се преносе комуникационим средствима унутар Вишег суда у Новом Пазару, између Вишег суда у Новом Пазару и лица ван Вишег суда уНовом Пазару, обезбеђује се утврђивањем одговарајућих правила, процедура, потписивањем уговора и споразума, као и примном адекватних конторла.

Правила коришћења електронске поште

Члан 63.

Употреба електронске поште мора бити у складу са успостављеним процедурама и адектватним конторлама над спровођењем иситх. Електронска пошта се може користитит 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

Члан 64.

Приступ садржајима на Интернету је дозвољен искчучиво за пословне намене. На мрежи је омогућено надгледање, односно користи се поступак периодичне ревизије и контролисања логовања, како на пријему тако и на слању.

Правила коришћења информационих ресурса

Члан 65.

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

Споразуми о прносу информација

Члан 66.

Безбедан пренос пословних информација између организације и трећег лица обезбеђује се поштовањем споразума о преносу информација.

Споразуми о преносу информација треба да укључе следеће:

1. Одговорности руководства за контролу и извештавање о преносу, отпреми и пријему,

2. Процедуре за обезбеђење следљивости и непроцењивости,

3. Минималне техничке стандарде за паковање и пренос,

4. Стандарде за идентификовање курира,

5. Обавезе и одговорности у случају инцидената нарушавање безбедности информација, као што је губитак података,

6. Коришћење договореног система, означавање осетљивих или критичних информација, уз осигуравање да је значење ознака одмах разумљиво и да су те информације заштићене на одговарајући начин,

7. Посебне контроле које су потребне да би се заштити осетљиви детаљи, попут криптографије,

8. Одржавање ланца надзора за информације у току преноса.

Размена електронских порука

Члан 67.

Заштита инфорамција укључених у размену електронских порука се регулише процедуром о безбедности у размени електронских порука.

Процедура о безбедности у размени електронских порука обухвата следеће:

- Заштиту порука од неовлашћеног приступа, модификовања или одбијања услуга које су у скаду са класификационом шемом коју је усвојио Виши суд у Новом Пазару,
- Осигурање исправног адресирања и транспорта поруке,
- Поштовање законских одредби, нпр. захтеве за електронске потписе,
- Добијање одобрења пре коришћења јавних спољних услуга, као што су размена хитних порука, приступи коришћења друштвене мреже или заједничко коришћење датотека, строже нивое утврђивања веродостојности, контролисање приступа из мрежа са јавним приступом.

Споразуми о поверљивости или неоткривању

Члан 68.

Споразуми о поверљивости или неоткривању имају за циљ заштиту информација у Вишем суду у Новом Пазару и обавезују потписнике да информације штите, користе и објављују их на одговоран и ауторизован начин.

Да би се идентификовали захтеви за споразуме о поверљивости или

неоткривању, треба узети у обзир следеће елементе:

1. дефиницију информација коју треба штитити,
2. очекивано трајање споразума, укључујући случајеве у којима је потребно да се поверљивост сачува неограничено,
3. поступања која се захтевају по истеку споразума, попут повраћаја или уништавања информација,
4. дозвољено коришћење поверљивих информација и пословних тајни, као и права потписника да користи информације,
5. право на проверу и праћење активности које укључују поверљиве инфорамције,
6. процес за обавештавање и извештавање о неовлашћеном неоткривању или приступу поверљивим информацијама,
7. радње које треба преузети у случају кршења овог споразума.

23. Питање информационе безбедности у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система

Члан 69.

У оквиру животног циклуса ИКТ система који укључује фазе концепирања, спецификације, пројектовања, развијања, тестирања, имплементације, коришћења, одржавања и на крају повлачења из употребе, Виши суд у Новом Пазару је у обавези да обезбеди информациону безбедност у свакој фази. Питање безбедности се анализира у раним фазама пројеката информационих система јер такво разматрање доводи до ефективнијих и рационалнијих решења.

Систем администратор у Вишем суду у Новом Пазару је задужен за технички надзор над реализациојом од стране извођача, односно испоручиоца.

О успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова ИКТ система систем администратор суда је дужан да уредно води евиденцију и документацију.

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

Анализе и спецификације захтева за информациону безбедност

Члан 70.

У захтеве за нове информационе системе или за побољшање постојећих информационих система морају бити укључени захтеви који се односе на информациону безбедност и они су саставни део уговора о набавци, модификацији и одржавању информационог система.

Захтеви за информациону безбедност укључују:

- проверу идентитета корисника;
- доступност, поверљивост, непроцењивост и интегритет података и имовине,
- Надгледање пословних процеса,
- Омогућавање приступа уз проверу веродостојности за пословне, привилеговане и техничке кориснике.

Спецификација захтева обухвата аутоматску контролу која ће бити уведена у информациони систем, као и потребу да постоји и ручна контрола, која мора бити примењена при вредновању развијених или купљених пакета софтвера, намењених за пословне апликације.

Системски захтеви за информациону безбедност и процеси за увођење безбедности се интегришу у фази дизајнирања информационих система.

Формално тестирање и процес имплементације ће се примењивати за све купљене производе.

У уговору са извођачем, односно испоручиоца купљених производа, посебно се дефинишу захтеви за информациону безбедност.

У случају да безбедносна функционалност предложеног производа не задовољава одређен захтев, ризик и повезане контроле ће бити преиспитање пре куповине производа.

Обезбеђивање апликативних услуга у јавним мрежама

Члан 71.

Инфорамције обухваћене апликативним услугама које пролазе кроз јавне мреже треба заштити од малверзација, неовлашћеног откривања података и модификовања. Неопходно је потврдити идентитет корисника и извршити поделу овлашћења и одговорности за постављње садржаја, електронског потписивања или обављања трансакција.

Заштита трансакција апликативних услуга

Члан. 72.

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 трансакцији морају да приме електронски потпис,
- Приватност свих страна које учестувују у трансакцији,

- На комуникационим каналима примењено шифровање,
- Безбедност протокола који се користе у трансакцијама.

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

Члан. 73.

Под тестирањем ИКТ система, како и тестирањем делова система, подразумева се процена промене стања система, односно делова система, који су унапређени или изложени променама.

Под процесом тестирања подразумева се процес употребе једног или више задатих објеката под посебним околностима, да би се упоредиле актуелна и очекивања понашања.

Тестирање ИКТ система, односно делова система, дозвољено је под условом потпуне примене свих безбедносних мера наведених у овом члану.

За потребе испитивања и тестирања ИКТ система, односно делова система, Виши суд у Новом Пазару избегава коришћење оперативних података који садрже личне податке или било које поверљиве податке и информације на основу којих је могуће идентификовати појединачног добављача, купца, запосленог или др.

Уколико се за сврху испитивања користи лични подаци или неке друге повељиве информације, онда се сви осетљиви подаци и информације пре коришћења штите аноминизацијом личних података, уклањањем садржаја или изменом текса садржаја у предметном делу.

Уколико је за тестирање неопходно користити оперативне податке, примењују се следеће смернице:

- За свако копирање оперативних података у тесно окружење се издаје посебно овлашћење,
- Приликом тестирања апликативних система примењују се процедуре за контролу приступа које се примењују и на оперативним системима,
- Оперативне информације се одмах по завршетку испитивања бришу из тесног окружења.

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

За потребе тестирања ИКТ система односно делова система систем администратор суда, техничар за ИТ подршку у Вишем суду у Новом Пазару, може користити податке који нису осетљиви, које штити, чува и контролише на одговарајући начин.

Приликом тестирања апликативних система примењују се додатне процедуре за контролу приступа путем физичке заштите и применом криптографских мера за заштиту система и података од невлашћених приступа, а које се примењују и на оперативним системима.

Скуп криптографских мера које ће бити примењене за заштиту података утврђује администратор система, надлежни техничар за ИТ подршку у Вишем суду у Новом Пазару, узимајући у обзир њихову поузданост и сврсисходност.

25. Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга

Члан 74.

Уговору који се закључују са пружаоцима услуга који имају приступ информацијама, средствима или опреми за обраду информација Виши суд у Новом Пазару морају садржати уговорену одредбу о заштити чувању поверљивости информација, података и документације.

Пружаоци услуга имају права на приступ информацијама које су крајне неопходне за пружање предметне услуге која је уговорена са Вишим судом у Новом Пазару.

Виши суд у Новом Пазару успоставља контролу безбедности информација које се односе на процесе и процедуре које ће спроводити пружаоци услуга:

- Идентификовање и документовање врсте пружаоца услуга којима ће Виши суд у Новом Пазару дозволити да приступају информацијама,
- Стандардизовани процес за управљање односима између пружаоца услуга,
- Дефинисање врста информација које ће различитим типовима пружаоца услуга бити дозвољено ради приступања, праћења и контоле приступа,
- Минимални захтеви за безбедност информација за сваку врсту информација и врсту приступа,
- Процеси и процедуре за праћење придржавања утврђених захтева за безбедност за сваку врсту добављача и врсту приступа,
- Контроле за осигурање интегритета информација или обраде информација коју обезбеђује било која страна,
- Поступање са инцидентима и непредвиђеним ситуацијама које су у вези са приступом пружаоца услуга, укључујући одговорности и организације и пружаоца услуга,
- Управљање неопходним променама информација, опреме за обраду информација и свега осталог што требе да се премешта и осигурање да се безбедност информација одржава током прелазног периода.

Уговарање обавезе обезбеђивања бедзбедности споразумима са пружаоцима услуга

члан 75.

Пре отпочињања преговора, потецијални 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 инфорамције и подаци могу бити коришћени искључиво на начин претходно одобрен од стране Вишег суда у Новом Пазару, а за потребе извршење предмета преговора.

Потребно је да изјава о поверљивости, односно уговор о пружању услуга, садржи одредбу о поверљивости са јасно утврђеном обавезом и одговорношћу пружаоца услуге уз претњу раскида уговора и накнаде штете у корист Вишег суда у Новом Пазару у случају повреде ове одредбе.

Пример: „сви подаци и информације садржане у овом уговору о пружању услуга се сматрају поверљивим пословним подацима и не смеју бити саопштени или на други начин учињени доступним трећим лицима. Нарочито се сматрају поверљивим сви пословни подаци и информације које једна страна учини доступним другој уговорној страни ради извршења обавеза из овог уговора, уколико ти подаци нису јавно доступни нити су били претходно познати другој страни.

Свака уговорна страна се обавезује да податке и информације које јој буду учињене доступним усклади са овим уговором и обавезом извршења уговорних послова и обавеза, буду стављене на располагање и увид запосленима, уколико је то неопходно ради извршења обавеза из овог уговора.

Уговорне стране се нарочито обевезују да поступају обазриво са подацима о личности до којих могу доћи у поступку извршења услуга за Виши суд у Новом Пазару као и да те податке чувају и поступају у свему у складу са прописима који уређују заштиту података о личности.

У случају повреде ове обавезе уговорна страна чији су подаци коришћени има право раскида уговора и право да захтева накнаду штете услед неовлашћеног коришћења података и информација друге стране".

Пружаоци услуга дужни су да захтеве Вишег суда у Новом Пазару у погледу безбедности информација прошире и на своје подуговараче за додатне услуге или производе.

Систем администратом у Вишем суду у Новом Пазару одговоран је за контролу приступа и надзор над извршењем уговорних обавеза, као и за поштовање одредби правилника којима су такве активности дефинисане.

26. Одржавање уговореног нивоа информационе безбедности и пружених услуга у сладу са условима који су уговорени са пружаоцем услуга

Члан 76.

У циљу одржавања и обезбеђивања уговореног нивоа информационе безбедности и пружених услуга са условима који су уговорени са пружаоцем услуга, Виши суд у Новом Пазару успосатавља мере надзора и заштите за време пружања услуга и након извршеног посла.

Праћење и преиспитивање извршења уговорених обавеза пружаоца услуга

Члан 77.

Систем администратор у Вишем суду у Новом Пазару редовно прати, анализира, преиспитује и проверава извршене услуге и усаглашеност са уговореним услугама на следећи начин:

1. Надлегање и преиспитивање услуга се може вршитити преко трећег лица,

2. Неопходно је да се поштују сви услови из споразума у вези са безбедношћу информација, као и да се спрече сви инциденти и проблеми нарушавања безбедности, те омогући управљање на одговарајући начин,

3. Врши се оцена квалитета извршења и саобразности уговорене услуге,

4. Пружалац услуге има уговорену обевезу да организује и припреми периодичне састанке који ће обезбедити редовно оизвештавање ВИшем суду у Новом Пазару и унапредити квалитет уговорених услуга, односно умањити потенцијалну штету или инцитенте који могу настати у поступку извршења услуге или након почетка примене,

5. Информатичка служба суда одржава потпуну контолу над спровођењем сулуга и осугурава увид у све осетљиве или критичне безбедносне информације или друга средства за обраду информација којима трећа страна приступа, које процесуира или којима управља,

6. Информатичка служба суда одржава увид у безбедносне активности кроз јасно дефинисан процес извештавања,

7. Преиспитује трагове провере и записе о догађајима у вези са безбедношћу код пружаоца услуга, односно оперативним проблемима, отказима, праћењу неисправности и сметњама у вези са испорученим услугама.

Приликом закључења уговора неопходно је јасно дефинисати квалитативне, оперативне и финансијске критеријуме оцене, утврдити поступак извештавања, праћења и поступања у складу са захтевима Вишег суда у Новом Пазару у поступку извршења уговорених услуга и извршити оцену извршених услуга и квалитате пружаоца услуга.

Приликом надзора над извршењем квалитета и саобразности уговорене услуге проверава се да ли пружалац услуге задовољава све критеријуме који су били од пресудног значаја приликом избора, укључујући обим и квалитет услуге, као и да се у току поступка извршења услуге може утицати на побољшање квалитета услуге или начина и обима извршења, у складу са утврђеним стварним потребама у Вишем суду у Новом Пазару.

У поступку објективне евалуације квалитета и обима пружене услуге у односу на уговорену, потребно је прикупити све релевантне чињенице, податке и документацију у вези са извршењем услуге, као и прикупити податке од непосредних, крајних корисника у вези са предметом услуге. Евалуација се може извршити слањем упитника, разговором са изабраним појединцима или на основу анонимног анкетирања путем електронске поште.

Управљање променама уговорених услуга од стране прожаоца услуга

Члан 78.

Уговором са пружаоцем услуга треба обезбедити могућност континуираног управљања променама уговорених услуга, укључујући одржавање и унапређење постојећих процедура и контолу безбедности инфорамција.

Промене које се узимају у обзир су промене у споразумима са пружаоцима услуга, повећање обима текућих услуга које се нуде, као и промене које уводи Виши суд у Новом Пазару ради инплементације нове или промењене апликације, система, контрола или процедура у циљу побољшања безбедности.

27. Превенција и реаговање на безбедносе инциденте што подразумева адекватну размену инфорамција о безбедносним слабостима ИКТ система, инцидентима и претњама

Одговорност појединаца и поступак одговора на инциденте

Члан.79.

Посебним процедурама се уређује начин одговора на инциденте нарушавања инфорамцине безбедности и одређује особа овлашћена за контакт у случајевима нарушавања безбедности, као и контак са надлежним органима.

Потребне процедуре су:

- Процедуре за припрему и планирање одговора на инциденте,
- Процедуре за надгледање, детекцију, анализу и извештавање о догађајима и инцидентима у вези са безбедношћу инфорамција,
- Процедуре за записивање активности у оквиру управљања инцидентима,
- Процедуре за поступање са судским доказима,
- Процедуре за оцењивање и одлучивање о догађајима у оквиру безбедности информација и оцењивање слабости у погледу безбедности информација,
- Процедуре за одговарање на инциденте, опоравак од инцидената и комуникацију са екстерним или интерним особама или организацијама.

Систем администратор у Вишем суду у Новом Пазару, придржавајући се процедура одређеним овим чланом, планира, детектује, анализира и информише надлежне у току и након инцидента.

Систем администратор у Вишем суду у Новом Пазару, треба да има одговарајућа техничка знања како би на најбржи и на одговарајући начин могли да одговоре на безбедносне инциденте.

Систем администратор у Вишем суду у Новом Пазару, у циљу превенције од безбедносних ризика обезбеђује више (различитих и другачијих) механизама за комуникацију и координацију у случају нарушавања безбедности. Ови механизми могу бити: обезбеђивање контакт информација (број телефона, електронска адреса) појединаца и чланова тима у оквиру организације и ван ње, систем за праћење проблема, шифровани

софтвер који би био коришћен од стране појединаца у оквиру организације и спољашњих странака, посебну осигурану просторију за чување података и складиштење поверљивог материјала.

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, запосени – корисник је дужан да о томе одмах обавести систем администратора у Вишем суду у Новом Пазару.

Извештавање о догађајима у вези са безбедношћу инфорамција

Члан 80.

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

Систем администратор суда је дужан да припреми план и неколико метада комуникације које би могле да се примене у зависности од инцидетна. Могуће методе комуникације су: електронска пошта, веб сајтови (интерни, екстерни, портали), телефонска комуникација, говорна порука, писмено извештавање, директан контакт.

У случају погрешног функционисања или других аномалијских понашања система врши се исто извештавање као и у случају догађаја у вези са информационом безбедношћу врши се исто извештавање као и у случају догађаја у вези са информационом безбедношћу.

Процедура за извештавање је следећа:

1. Запослени који сматра да је дошло до напада или злоупотребе података мора одмах припремити опис порблема и послати га електронском поштом сектору за информационе технологије (help desk)/ позвати број/ пријавити проблем путем Интернет стране за help desk;

2. Адресу електронске поште, број телефона и Интернет страну за help desk проверава систем администратор;

3. Систем администратор у Вишем суду у Новом Пазару, врши проверу пријављеног инцидента и даље поступа по одговарајућој процедури.

Када је идентификован инцидент запослени је дужан да одмах обавести систем администратора у Вишем суду у Новом Пазару као и да предузме мере у циљу заштите ресурса ИКТ система.

Систем администратор у Вишем суду у Новом Пазару води евиденцију о свим инцидентима, у складу са уредбом, на основу које, против одговорног лица, могу да се воде дисциплински, прекршајни или кривични поступци.

Извештавање о утврђеним слабостима систем заштите

Члан 81.

Сви запослени су у обавези да о уоченим и утврђеним слабостима ИКТ система

известе систем администратора у Вишем суду у Новом Пазару, у што краћем року, како би се инцидетни нарушавања информационе безбедности сперечили и спречио настанак штете.

Одговорно лице за обавештавање надлежних органа о инцидентима у ИКТ систему који могу да имају значајан утицај на нарушавање информационе безбедности, поступа у складу са одговарајућом процедуром.

Догађаји у вези са информационом безбедношћу се оцењују и у складу са анализом се доноси одлука да ли је потребно да се класификују као инциденти нарушавања информационе безбедности.

Одговор на инциденте нарушавања информационе безбедности

Члан 82

Виши суд у Новом Пазару је у обавези да усвоји План за превенцију од безбедносних ризика.

План за превенцију од безбедносних ризика садржи одговоре на питања ко треба да буде контактиран, када и како и које акције треба предузети моментално у случају одређеног напада:

- Класификациона шема-детаљи о подацима који се налазе у систему, њихов ниво осетљивости и поверљивости.
- Листа услуга-попис свих услуга које Виши суд у Новом Пазару пружа, рангира по важности.
- План backup и restore података-дефинише за које податке се ради backup, носаче података, на које ће се снимати, где се носачи чувају и колико често се backup изводи. Дефинише и псотуапк за restore података.
- План за замену опреме: садржи списак потребне опреме, рангиране по важности.
- Односи са јавношћу: утврђена је одговорна особа задужена за односе са јавношћу, као и упутство које информације је дозвољено јавно објавити у случају напада.

Прикупљено знање из анализе и решавања инцидената који су нарушили информациону безбедност, Виши суд у Новом Пазару користи да би се идентификовали инциденти који се понављају и смањила вероватноћа и утицај будућих инцидената.

Прикупљање доказа

Члан 83.

Виши суд у Новом Пазару дефинише и примењује процедуре за иднтификацију, сакупљање, набавку и чување информација које могу да служе као доказ у случају покретања дисциплнског, прекршајног и кривичног поступка.

28. Мере које обезбеђују континуитет

обављања посла у ванредним околностима

Члан 84.

Виши суд у Новом Пазару примењује мере које обезбеђују континуитет обављања посла у наведеним околностима, како би ИКТ систем у што краћем року био у функционаолном стању.

Планирање континуитета мера безбедности инфорамција

Члан 85.

Континуитет пословања се осигурава кроз План за обезбеђење континуитета пословања и Плана опоравка од нежељених догађаја ИКТ система.

План за обезбеђење континуитета пословања за хардверске компоненте ИКТ система треба да обухвати следеће:

- Документацију за логистички и физички дијаграм и копије пројеката,
- Заштитне копије конфигурационих фајлова и оперативног система активности уређаја,
- Постојање резервне опрме,
- Унапред направљене конфигурације за различите сценарије,
- Израду резервних копија.

Планом опоравка од нежељених догађаја ИКТ система треба:

- Проценити најкритичније апликације, податаке, конфигурационе фајлове и системски софтвер за који треба направити резервне копије,
- Одредитит место чувања копије,
- Одредитит нову локацију рада ИКТ система у случају немогућности рада на основној локацији/избор рачунара који ће привремено заменити сервер док се сервер не стави у функцију,
- Навести податке о тиму који ће бити ангажован на отклањању последица нежељених догађаја,
- Одредитит изворе непрекидног напајања електричном енергијом.

При изради Плана опоравка од нежељених догађаја ИКТ система потребно је предвидети:

- Постојање документације за сервисе, апликације и базе података,
- Процедуре инсталације и кофигурисање сервиса, апликација и база података,
- Место чувања инсталација сервиса, апликација и база података и резервне копије података,
- Податке о тиму који ће бити ангажован на отклањању последица нежељених догађаја,
- Развијене и одобрене документоване планове, одговоре и процедуре за

опоравак, детаљно наводећи како ће организација управљати догађајима који узрокују поремећаје и како ће одржавати своју безбедност информација.

Имплеметнација континуитета безбедности информација

Члан 86.

Да би се осигурао потребан ниво континуитета безбедности информација током ванредних ситуација, информатичка служба суда примењује процедуре и контроле описане у Плану за обезбеђење континуитета пословања.

Систем администратор у Вишем суду у Новом Пазару редовно врши проверу усвојених процедура контроле континуитета безбедности информација, како би оне биле адекватне и ефектне током ванредних ситуација.

Провера се врши вежбањем и испитивањем знања и рутине приликом руковања процесима, процедурама и контролама као и преиспитивањем ефективности мера безбеднсоти информација у случају промене информационих систем, процеса, процедура и контроле безбедности информација.

III ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Посебна обавеза опратора ИКТ система

Члан 87.

Обавеза систем администратора у Вишем суду у Новом Пазарује да најмање једном годишње изврши проверу ИКТ система и изврши евентуалне измене Акта о безбедности, у циљу провере адекватности предвиђених мера заштите, као и утврђених процедура, овлашћења и одговроности у ИКТ систему Вишег суда у Новом Пазару.

Ступање на снагу Акта о безбедности

Члан 88.

Акт о безбедности информационо-комуникационог ситема Вишег суда у Новом Пазару, ступа на правну снагу даном доношења.

ПРЕДСЕДНИК СУДА
Слађана Чоловић