„Србија Карго“ а.д.
Број: 4/2017-464-162
Датум: 08.12.2017. године
Б е о г р а д

На основу члана 8. Закона о информационој безбедности ("Службени гласник РС", бр. 6/16 и 94/17) и члана 24. Статута Акционарског друштва за железнички превоз робе "Србија Карго", Београд ("Службени гласник РС", број 60/15 и "Службени гласник Железнице Србије", број 14/17), Одбор директора је, на седници одржаној 08.12.2017. године, донео

О Д Л У К У

1. Доноси се Акт о безбедности информационо – комуникационог система „Србија Карго“ а.д.
2. Акт из тачке 1. је саставни део ове одлуке.
3. Одлука ступа на снагу даном доношења.
4. Одлуку објавити у „Службеном гласнику Железнице Србије“.

ОДБОР ДИРЕКТОРА

Душан Гарибовић

Мира Вукмировић

Владимир Булатовић

Акт о безбедности

информационо-комуникационог

система

"СРБИЈА КАРГО" а.д.

I. ОСНОВНЕ ОДРЕДБЕ

II. МЕРЕ ЗАШТИТЕ

III. ЗАВРШНЕ ОДРЕДБЕ

"Србија Карго" а.д.
Број: 4/2017-464/1-162
Датум: 08.12.2017. године
Београд

На основу члана 8. став 1. Закона о информационој безбедности („Службени гласник РС", бр. 6/16 и 94/17), 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) и члана 24. Статута Акционарског друштва за железнички превоз робе „Србија Карго", Београд („Службени гласник РС", број 60/15 и „Службени гласник Железнице Србије", број 14/17), Одбор директора „Србија Карго" а.д. је, на седници одржаној 08.12.2017. године донео

Акт о безбедности информационо-комуникационог система "Србија Карго" а.д.

I. ОСНОВНЕ ОДРЕДБЕ

Предмет Акта о безбедности

Члан 1.

Актом о безбедности информационо-комуникационог система "Србија Карго" а.д. (у даљем тексту: Акт о безбедности), 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-комуникационих технологија "Србија Карго" а.д. (у даљем тексту: ИКТ систем).

Циљеви Акта о безбедности

Члан 2.

Циљ доношења Акта о безбедности је:

- постизање и одржавање адекватног нивоа безбедности система;
- спречавање и ублажавање последица инцидената којим се угрожава или нарушава информациона безбедност и функционисање ИКТ система;
- подизање свести код запослених о значају информационе безбедности, ризицима и мерама заштите приликом коришћења ИКТ система;
- дефинисање одговорности запослених у вези са безбедношћу и ресурсима ИКТ система;
- свеукупно унапређење информационе безбедности и примене мера заштите.

Обавеза примене одредби Акта о безбедности

Члан 3.

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

Сви запослени који директно користе или имају додира са ИКТ системом (у даљем тексту: Корисници ИКТ система) морају бити упознати са садржином Акта о безбедности и дужни су да поступају у складу са одредбама овог акта, које регулишу информациону безбедност.

Сектор за информационо-комуникационе технологије (у даљем тексту: Носилац ИКТ функције) одговоран је за спровођење и праћење примене мера безбедности, као и за проверу адекватне заштите ИКТ система и података на начин који је утврђен овим актом.

Одговорност запослених

Члан 4.

Запослени су дужни да приступају информацијама и ресурсима ИКТ система само ради обављања редовних пословних активности, да воде рачуна да ни на који начин не угрозе безбедност ИКТ система и пословних информација, као и да благовремено информишу овлашћено лице о свим сигурносним инцидентима и проблемима.

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

Предмет заштите

Члан 5.

У циљу брзог и прецизног обављања пословних процеса као и побољшања пословних резултата "Србија Карго" а.д. (у даљем тексту: Друштво), обезбеђује запосленим корисницима неопходне услове за обављање редовних послова и омогућава коришћење ИКТ система на којима се креирају, обрађују и чувају подаци Друштва.

Стварањем услова за оптимално коришћење ИКТ система Друштво омогућава аутоматизовање процеса рада, олакшава и чини ефикаснијом комуникацију између запослених, између Друштва и његових клијената и пословних партнера, и тиме обезбеђује значајан извор пословних информација о тржишту, производима, пословним партнерима и корисницима као и новим технологијама и сервисима.

Информациона добра обухватају јединице за обраду података (персоналне рачунаре, сервере, пратећу опрему...), рачунарску мрежу и пратећу опрему, податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компоненти, техничку и корисничку документацију, унутрашње опште акте и процедуре.

Мере заштите ИКТ система односе се на: радне станице (кућишта персоналних рачунара са интегрисаним компонентама), пратећу опрему радних станица (мониторе, јединице за унос података: тастатура и "миш", штампаче и друго), електронске комуникационе мреже (електронске водове, рутере, свичеве, сервере...) Друштва (у даљем тексту: Рачунарску мрежу), серверске електронске уређаје на којима се чува и врши обрада података коришћењем рачунарског програма, оперативне и апликативне рачунарске програме, програмски кôд, податке који се чувају, обрађују, претражују или преносе помоћу електронских уређаја, корисничке налоге, унутрашње опште акте и документацију.

Својинска и ауторска права над подацима који су креирани коришћењем ИКТ Друштва од стране запослених (у даљем тексту: крајњих корисника) у радно време за које су крајњи корисници плаћени од стране Друштва, припадају Друштву. Запослени са собом носе права и обавезе, посебно у погледу тачности, ажурности и доступности тих података, као и чувања пословне тајне и заштите интереса Друштва.

Корисницима ИКТ система, који су одговорни за функционисање процеса рада, омогућен је несметан и сталан приступ подацима, који су креирани коришћењем ИКТ система Друштва, а у складу су са овлашћењима за одређено радно место и важећом организационом структуром Друштва, или одобрењем од стране непосредног руководиоца, а уз сагласност представника Сектора за ИКТ.

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

Појединци којима је дата одговорност за коришћење ИКТ имовине дужни су да правилно управљају имовином.

Друштво у циљу 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 над целокупним ИКТ системом, у континуитету и у складу са нормама безбедности;
- Штити информације и податке на једнак начин у свим организационим деловима;
- Координира безбедност и заштиту ИКТ система и података у информационом систему са физичком заштитом истих.

II. МЕРЕ ЗАШТИТЕ

Опште мере заштите ИКТ система и података Друштва

Члан 6.

Коришћење ИКТ система је намењено пословним потребама Друштва.

Носиоци ИКТ функције гарантују тајност садржаја информација, података и докумената у електронској форми која се прослеђује и/или складишти од стране

крајњих корисника ИКТ система и Друштва уопште, преко електронске поште, процеса за пренос и обраду података и помоћних програма.

Корисницима ИКТ система је неопходно ограничити приступ ИКТ систему, подацима и средствима за обраду података у складу са степеном тајности података. Крајњим корисницима ИКТ система је дозвољен приступ само радним станицама, мрежи и мрежним услугама за коју имају овлашћења да користе у складу са радним местом и припадајућим радним процесом.

Скуп апликација и софтвера којима располаже крајњи корисник ИКТ система, је дефинисан конкретним радним местом на које је запослени распоређен и радним задацима који су му додељени, а у складу са надлежностима утврђеним организационом структуром Друштва. Променом радног места и задатака, мења се и група расположивих софтвера.

Коришћење ИКТ система за личне или приватне потребе запослених (e-mail, office алати) дозвољено је у мери у којој то коришћење не угрожава или нарушава пословање Друштва и не крши обавезе запослених, а уз потпуну одговорност запосленог за све последице таквог коришћења ИКТ система. Друштво искључује било какву обавезу и одговорност за коришћење ИКТ система за личне или приватне потребе запослених или трећих лица.

Корисници ИКТ Друштва дужни су да поштују поверљивост ИКТ система, као и сервиса других лица у и/или изван Друштва.

Запосленима и другим корисницима ИКТ система забрањује се да се баве:

- надгледањем или пресретањем фајлова или електронских комуникација запослених или трећих лица;
- "хакерисањем" или неовлашћеним приступањем системима и/или налозима за које немају одобрење за употребу;
- коришћењем туђих налога, лозинки или средстава за приступ ИКТ систему;
- тестирањем или надгледањем рачунарских и/или мрежних безбедносних мера и "пробијањем" заштите и безбедносног система Друштва;
- уношењем злонамерног кода и софтвера (у даљем тексту: компијутерског "Вируса") у информациони систем.

Крајњим корисницима ИКТ система забрањује се да на радне станице (PC - Desktop рачунаре) и рачунарску мрежу и опрему самовољно прикључују било какве додатне уређаје и хардверске модуле и уређаје без одобрења Носиоца ИКТ функције.

Електронске поруке или други електронски подаци, који покушавају да сакрију идентитет пошиљаоца, или да представе пошиљаоца као неког другог корисника, нису дозвољени.

ИКТ систем Друштва се не може користити за неовлашћено и својевољно слање или складиштење било каквих података који:

- откривају пословну тајну Друштва или пословног партнера, откривају личне податке приватних корисника услуга Друштва, и/или који могу да нанесу штету Друштву било које врсте;
- дискриминишу или злостављају било ког појединца или групу;

- су погрдни за било ког појединца или групу;
- су опсцени и/или неморални;
- су клеветнички или застрашивачки према било коме;
- су у супротности са лиценцом за коришћење било ког софтвера, или електронске публикације;
- се користе у сврхе које су противзаконите и у супротности са Актом о безбедности ИКТ система или другим актима или пословним интересима Друштва.

У циљу провере функционалности ИКТ система и унапређења безбедности и заштите ИКТ система, дозвољава се надгледање, контрола рада крајњих корисника и радњи у функцији одржавања нивоа безбедности, само овлашћеним администраторима Сектора за ИКТ.

Сви корисници ИКТ система имају обавезу да користе ИКТ систем на професионалан и моралан начин, у складу са законом.

У случају откривања злоупотребе коришћења ИКТ система, угрожавања безбедности података функционисања ИКТ система, носилац ИКТ функције је овлашћен да без упозорења делимично или потпуно, привремено или трајно искључи са рачунарске мреже Друштва сваку радну станицу или ИКТ ресурс, или да онемогући приступ кориснику ИКТ за кога се утврди, или се сумња да се преко њега врши злоупореба, или да постоји опасност по податке, или функционисање ИКТ система.

Корисник ИКТ система који злоупотребљава овлашћења у коришћењу ИКТ система и не понаша се у складу са одредбама Акта о безбедности ИКТ система и другим актима Друштва, одговоран је у складу са законом и овим актом.

У случају доказаног нарушавања безбедности ИКТ система и поверљивих информација или уколико корисник ИКТ система на други начин изврши повреду правила и безбедносне политике, против одговорних лица се спроводи поступак за утврђивање повреде радне обавезе.

Поступак из става 14. овог члана, се покреће по предлогу надлежног овлашћеног лица. За утврђену повреду радне обавезе изриче се мера у складу са причињеном штетом, нарушеном безбедношћу и ризиком коме су ИКТ и подаци били изложени.

Обезбеђивање адекватне оспособљености лица која користе ИКТ систем и потпуног разумања одговорност и мере везане за промену послова или престанак радног ангажовања запослених

Члан 7.

У циљу безбедног и функционалног руковања опремом и ресурсима ИКТ система, Друштво има обавезу и стара се да запослени који управљају ИКТ системом (носиоци ИКТ функције), односно запослени који користе ИКТ систем (крајњи корисници) имају адекватан степен образовања и способности, као и свест о значају послова које обављају.

Друштво је обавезно да запослене у Сектору за ИКТ континуирано обучава у циљу унапређења техничког и технолошког нивоа знања. Друштво, има обавезу едукације и усавршавања информатичког кадра, да би се пратио корак брзог раста и развоја хардвера, софтвера и информатичких технологија, који су услов рада, развоја и опстанка Друштва у савременим условима пословања.

Запослени Сектора за ИКТ морају бити оспособљени за предузимање хитних и неодложних мера у случају постојања непосредне опасности за опрему и ресурсе ИКТ система, податке и документацију који су под мерама заштите.

Небрига о оспособљености информатичког кадра, и довођење у ситуацију да неедукован кадар рукује опремом ИКТ система озбиљно угрожава безбедност и функционисање ИКТ система и података Друштва.

Запослени у Сектору ИКТ су у обавези да прођу одговарајућу обуку и редовно стичу нова и обнављају постојећа знања о имплементацији, одржавању и коришћењу ИКТ система, чиме се обезбеђује адекватан ниво функционисања и безбедности ИКТ система и података, на начин који одговара њиховом пословном ангажовању и радном месту.

Запослени који користе ИКТ систем за редовно обављање посла, а не припадају Сектору за ИКТ (у даљем тексту: крајњи корисници ИКТ система) су у обавези да прођу одговарајућу обуку за крајње кориснике ИКТ система на начин који одговара њиховом пословном ангажовању и радном месту.

Запослени или лица ангажована по другом основу, 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 радног односа или ангажовања задужен је Сектор за људске ресурсе и опште послове, непосредни руководилац и Носилац ИКТ система, који предузимају следеће активности:

- проверава испуњеност свих услова у погледу раздужења опреме
- преузима од запосленог електронске и друге мобилне уређаје,
- проверава враћене мобилне уређаје и уређаје за преношење података,
- даје налог за укидање налога електронске поште и свих других права приступа рачунарској мрежи на дан престанка радног односа или другог основа ангажовања бившег запосленог,
- прегледа све налоге за приступ, прикупља приступне шифре и кодове са циљем укидања/промене истих на дан престанка радног односа односно ангажовања,
- преузима картице или друге уређаје којима се омогућава приступ пословним просторијама и опреми Друштва.

Аутентификација и идентификација лица која приступају ИКТ систему и овлашћења приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа

Члан 8.

Друштво управља приступом ИКТ систему и рачунарској мрежи и услугама кроз употребу корисничких идентификатора, односно налога за приступ рачунарској мрежи.

Аутентификација 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 увек када постоји било какав наговештај могућег компромитовања.

Шифре морају да:

- садрже најмање 7 алфанумеричких карактера;
- садрже најмање једно велико и једно мало слово;
- садрже најмање 1 број (0-9).

Није препоручљиво да шифре буду засноване на личним подацима особе, као што су име, телефонски број или датум рођења. У себи не смеју да садрже више од 3 узастопна идентична бројчана или словна знака.

Коришћење или покушај злоупотребе туђег корисничког налога, представља повреду радне обавезе и повлачи одговорност запосленог.

Управљање корисничким идентификаторима врши се поштујући следеће принципе:

- кориснички идентификатори (Username и Password) су јединствени, тако да се корисници могу везати уз њих и учинити одговорним за своје активности;
- ради повећања нивоа безбедности неопходно је да крајњи корисници корисничку лозинку (Password) мењају сваког месеца;
- корисницима којима је престао радни однос или период ангажовања тренутно се онемогућавају или уклањају кориснички идентификатори;
- коришћење заједничких идентификатора дозвољава се само онда када је то неопходно за обављање посла уз претходно одобрење непосредно надлежних као и Сектора за ИКТ;
- вишеструки кориснички идентификатори се периодично проверавају и уклањају или онемогућавају по потреби;
- вишеструки идентификатори неког корисника се не издају другим корисницима који немају потребе и овлашћења за коришћење.

Сваком крајњем 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 потреба послова имплементације и одржавања ИКТ система запосленима у Сектору за ИКТ.

Привилегована (администраторска) 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.

Забрањено је неовлашћено коришћење туђих корисничких идентификатора или корисничких идентификатора администратора, у сврху администрирања ИКТ система. Шифре за приступ општим корисничким идентификаторима администратора мењају се променом корисника.

Запосленима лицима и екстерним корисницима информација и опреме за обраду информација по престанку радног односа или истеку уговора, укида се право на приступ ИКТ систему.

Исправно и безбедно коришћења и функционисања ИКТ система, података и средстава за обраду података и радног окружења

Члан 9.

Планирање и управљање расположивим капацитетима, као и коришћење ресурса ИКТ система и података се пројектује, подешава, усклађује и надгледа, у складу са пројектованим и захтеваним капацитетима за наредни период, од стране носилаца ИКТ система (Сектора за ИКТ) или професионалних стручних служби, уз активно учешће носилаца ИКТ система, како би се осигурало да захтеване перформансе система буду усклађене и оптимално и безбедно функционишу са постојећим ресурсима.

У складу са усвојеним плановима и пројектима ресурса и капацитета ИКТ система, врши се набавка неоходних компоненти (hardware) и апликација (software) уз консултовање и сагласност Сектора за ИКТ, ради обезбеђења компатибилности са постојећим ресурсима ИКТ система и постизања очекиваног нивоа безбедности.

Овлашћени администратори ИКТ система (запослени Сектора за ИКТ), управљају радом сервера и мрежних уређаја водећи рачуна о потребним капацитетима, саобраћају података и меилова, чувању потребних и брисању непотребних података и апликација са сервера и рачунара крајњих корисника.

Друштво задржава право по сопственој дискрецији, да изврши проверу и измену неког електронског податка и/или поруке, односно датотеке у којима су ти подаци забележени, било да се налази на серверима, централном рачунару, комуникационој опреми или на радним станицама, до оне мере до које је неопходно да се обезбеди да ИКТ систем и сервиси безбедно и несметано функционишу и користе се у складу са Актом о безбедности ИКТ система Друштво.

У циљу оптималног коришћења и одржавања неопходног нивоа безбедности ИКТ система, периодично, носиоци ИКТ функције спроводе активности:

- проверу и оптимизацију ИКТ капацитета са потребама за обраду, складиштење и размену података;
- брисање застарелих података (простора на диску);
- повлачење из употребе сувишних и неадекватних апликација, система, база података или виртуалних окружења;
- оптимизацију процеса и распореда коришћења података;
- одбијање или ограничавање пропусног опсега услуга захтеваних у погледу ресурса, ако оне нису неопходне за пословање.

Крајњи корисници су одговорни за одржавање свог радног простора у рачунару и података неопходних за обављање свакодневних радних задатака. Такође су обавезни да периодично и по потреби бришу непотребне електронске документе и меилове, чиме ослобађају неопходан простор за нова радна документа.

Корисници ИКТ система не смеју самостално да преузимају никакве мере и активности да применом ИКТ система Друштва, шифрирају и скривају податке по сопственом нахођењу.

Неопходно је окружења за развој, испитивање и рад софтвера међусобно раздвојити, како би се обезбедила безбедност радног окружења и како би се смањио ризик од грешака, губитка података, неовлашћеног приступа или промена у радном окружењу.

У циљу заштите поменутих окружења треба применити следеће смернице:

- развојни и оперативни софтвери треба да се извршавају на различитим системима или рачунарским процесима, као и у различитим виртуалним окружењима, доменима или директоријумима;
- промене у оперативним системима и апликацијама треба испитивати у окружењу за испитивање или режиму одржавања пре него што се примене на оперативне и функционалне системе;
- да би се смањио ризик од грешке, корисници треба да примењују различите корисничке профиле за оперативне и испитне системе, а менији треба да приказују одговарајуће идентификационе поруке;
- осетљиве податке не треба копирати у системско испитно окружење, осим ако нису обезбеђене еквивалентне контроле за систем за испитивање.

Заштита од губитка података

Члан 10.

Пожељно је да крајњи корисници врше израду копија података и докумената неопходних за обављање редовних послова како би осигурали континуитет пословања у случају квара или нежељеног брисања података, под условом да израда копија не нарушава безбедност и интегритет ИКТ система.

Сектор за ИКТ врши израду резервних копија података који обухватају системске информације, апликације и податке са сервера који су неопходни за опоравак целокупог система у случају наступања последица изазваних ванредним околностима.

За чување заштитних копија користе се магнетне траке, екстерни хард дискови, USB Flash меморије и CD/DVD медији.

Резервне копије (Back Up) информација, софтвера и дупликати система сервера се редовно израђују и испитују по стандардима ИКТ система, у складу са Актом о безбедности.

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 и log 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.

У циљу заштите података Сектор за ИКТ извршава следеће задатке:

- процењује осетљиве и критичне податке за које је потребно правити резервне копије;
- прави заштитне копије серверског оперативног система и података, комуникационог оперативног система и конфигурационих фајлова, апликација, сервиса и база података;
- верификује успешно прављење резервних копија;
- води евиденцију урађених резервних копија;
- одлаже копије на безбедно место;
- тестира исправност резервних копија и процедуре за прављење заштитних копија;
- рестаурира податке са резервних копија.

Заштита носача података и безбедно одлагање поверљивих података и докумената

Члан 11.

Носилац ИКТ система обезбеђује услове за безбедно коришћење носача података и преносне меморије (CD/DVD, USB Flash меморије, екстених HDD...), инсталацијом и ажурирањем Антивирус програма.

Корисник ИКТ система је одговоран за употребу носача података, у складу са следећим:

- неопходно је све носаче података и преносне медије, приликом повезивања на матични рачунар скенирати званичним Антивирус програмом;
- 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;
- спречити неовлашћено модификовање, уклањање или уништење података, информација и садржаја неопходних за рад Друштва, а који се чувају на носачима података.
- носаче података који садрже информације треба штитити од неовлашћеног приступа, злоупотребе или оштећења приликом транспорта.

Када више нису потребни, медијуми за пренос података се расходују на безбедан начин, уз свођење на минимум ризика од доласка осетљивих информација до неовлашћених особа.

Сва осетљива и поверљива документа и материјали морају да буду уклоњени са радне површине и одложени на место где су физички обезбеђена, у периоду када запослени није присутан на свом радном месту или када се не користе.

Документа и радни материјали чувају се према следећој процедури:

- Све осетљиве и поверљиве информације у штампаном или електронском облику запослени морају одложити на сигурно место ван домашаја неовлашћених лица на крају радног дана или када нису присутни на свом радном месту.
- У одсуству запосленог рачунари морају бити угашени и осигурани.
- Ормари и фиоке у којима се чувају поверљиви подаци морају бити закључани, а кључеви не смеју бити остављени на приступачном месту без надзора.
- Лаптопови морају бити обезбеђени уз помоћ одговарајуће опреме или закључани у фиоци. Таблети и остали преносни уређаји морају бити закључани у фиоци.
- Носиоци података као што су дискови и flash меморија морају бити одложени и закључани.
- Шифре за приступ не смеју бити написане и остављене на приступачном месту.
- Штампани материјал који садржи осетљиве информације се мора одмах преузети са штампача приликом штампања.
- Материјал који је намењен за бацање треба адекватно уништити или одложити на место које се закључава, а које је намењено за одлагање такве врсте материјала.

Крајњи корисник ИКТ система дужан је да поштује утврђене мере безбедног коришћења носача података.

Обезбеђење интегритета софтвера и оперативних система

Члан 12.

На ИКТ систему и опреми Друштва може бити инсталиран само софтвер који је регистрован и одобрен од стране Сектора за ИКТ, произвођача или испоручиоца софтвера или опреме.

Инсталацију и подешавање софтвера може да врши искључиво Носилац ИКТ функције, односно администратор који има овлашћење за то, произвођач или испоручиоц софтвера или опреме.

Софтвер у ИКТ систему, може да буде преинсталиран само од стране овлашћеног администратора, произвођача или испоручиоца опреме, а касније инсталирање софтвера је дозвољено само овлашћеним лицима испоручиоца софтвера уз присуство и надзор овлашћених лица носиоца ИКТ функције.

Носилац ИКТ функције спроводи поступке којима се обезбеђује контрола интегритета инсталираног софтвера и оперативних система у складу са следећим смерницама за контролу промена и инсталацију софтвера:

- ажурирање оперативног софтвера, апликација и програмских библиотека могу да обављају само оспособљени администратори, по добијању одговарајућег овлашћења од руководиоца и Носилаца ИКТ функције;
- оперативни системи треба да садрже само одобрене извршне кодове, а не и развојне кодове;
- апликације и оперативни системски софтвер треба имплементирати тек после обимног и успешно спроведеног испитивања, које обухвата испитивање безбедности, применљивости, компатибилности, утицаја на друге системе и погодности за коришћење, а треба их спроводити на засебним системима, односно тестним окружењима;
- треба осигурати да све одговарајуће библиотеке изворних програма буду редовно и адекватно ажуриране;
- пре имплементације било каквих промена, треба успоставити стратегију повратка на претходно стање;
- као меру предострожности за неочекиване ситуације треба сачувати претходне верзије апликацијског софтвера;
- старије верзије софтвера треба архивирати, заједно са свим потребним информацијама и параметрима, процедурама, детаљима конфигурације и софтвером за подршку, све док се подаци држе у архиви.

Приступ ресурсима и подацима другог лица и/или друге компаније или особе, у погледу копирања, коришћења, преправљања и/или прослеђивања података, врши се искључиво уз дозволу власника.

Изричито је забрањено инсталирање софтвера на уређајима, који могу довести до изложености ИКТ система безбедносним опасностима.

Заштита ИКТ система, софтвера и података од злонамерног кода и софтвера (''вируса'')

Члан 13.

Злонамерни софтвер (компијутерски "Вирус") подразумева све програме који су направљени у намери да онемогуће, отежају рад неке апликације, софтверског система, или оштете неки фајл, податке или рачунар.

Заштита од злонамерног софтвера се заснива на софтверу за откривање злонамерног софтвера (у даљем тексту: Антивирус програм) и отклањање штете, на спровођењу

мера које доприносе безбедности информација, као и на одговарајућим контролама приступа систему и управљања захтеваним и потребним променама.

У циљу заштите од упада у ИКТ систем са интернета, Сектор за ИКТ је дужан да активира и одржава антивирус систем за заштиту од злонамерног кода и софтвера.

У циљу спречавања ширења злонамерног кода ("вируса") преко ИКТ система Друштва, строго је забрањено преузимање било којег софтвера или материјала са Интернета или са непроверених или нескенираних екстерних носача података, као и отварање меилова од непознатих пошиљаоца са сумњивим пратећим фајловима и материјалом (Attachment-ом).

У случају да корисник примети неуобичајан и неправилан рад рачунара, запажање треба без одлагања да пријави Сектору за ИКТ.

Мере контроле откривања, спречавања и опоравка, ради заштите од злонамерног софтвера обухватају следеће:

- инсталирање и редовно ажурирање софтвера за откривање непријатеског софтвера и опоравак (антивирус програм) ради претраживања рачунара и медијума као контролу из предострожности;
- имплементација контрола које спречавају или откривају коришћење неовлашћеног софтвера;
- имплементација контрола које спречавају или откривају коришћење познатих или сумњивих компромитованих веб-сајтова;
- успостављање политике заштите од ризика повезаних са добијањем софтвера од или преко спољних мрежа, или на било ком другом медијуму;
- смањење рањивости које може да експлоатише непријатељски софтвер, нпр. кроз управљање техничким рањивостима;
- спровођење редовних преиспитивања софтвера и садржаја података у системима који подржавају критичне пословне процесе, присуство било каквих неодобрених датотека или неауторизованих допуна треба формално истражити;
- формална забрана коришћења неауторизованих софтвера.

Листа провера које се спроводе ради заштите од злонамерних софтвера:

- проверу и скенирање, пре коришћења, свих датотека на електронским или оптичким медијумима, као и датотека примљених преко мрежа, да ли садрже злонамерни софтвер;
- проверу и скенирање, пре коришћења, садржаја придружених порукама електронске поште и преузетих садржаја, да ли садрже злонамерни софтвер на серверима за електронску пошту, на персоналним рачунарима или приликом приступа на рачунарску мрежу Друштва;
- проверу постојања злонамерних софтвера на веб-страницама;
- правилно поступање и коришћење заштите од злонамерног софтвера у системима, као и извештавање и опоравак од напада злонамерним софтвером;
- припрему за континуитет пословања приликом опоравка од напада непријатељским софтвером, укључујући све неопходне резервне копије података и софтвера и механизме за опоравак;
- редовно прикупљање информација, и провера веб-страница на којима се дају информације о новим злонамерним софтверима;

- имплементацију процедура за верификовање информација о злонамерним софтверима и обезбеђење да су упозоравајући извештаји тачни и информативни; сви корисници треба да буду свесни проблема појаве злонамерних обмана и онога што треба да раде после њиховог пријема.

Сектор за ИКТ, кориснику који је повезан на ИКТ систем, у случају доказане злоупотребе и повезаности за активирањем и ширењем компијутерског "вируса", укида приступ ИКТ систему и он сноси одговорност за евентуално насталу штету.

Безбедан рад на даљину и употреба мобилних уређаја

Члан 14.

Друштво дозвољава рад на даљину и употребу мобилних уређаја од стране запослених лица, уколико је осигурана безбедност рада у случају обављања послова ван просторија послодавца, узимајући у обзир и ризике до којих може доћи услед неадекватног коришћења 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 садрже податке и имају могућност повезивања на мрежу. Приликом коришћења мобилних уређаја потребно је осигурати пословне информације од могућег компромитовања.

Право на коришћење мобилних уређаја ван седишта Друштва се стиче на основу писаног захтева корисника мобилног уређаја упућеног Сектору ИКТ, односно непосредном руководиоцу. Мобилни уређаји који се користе морају бити претходно одобрени и/или набављени од стране Друштва и оцењени као компатибилни са захтевима обезбеђивања адекватног степена заштите од стране Сектора за ИКТ. Рад на даљину одобрава непосредни руководилац уз сагласност и техничко одобрење Сектора ИКТ.

Ангажовање и омогућавање обављања неопходних послова на даљину се остварује уз поштовање мера безбедности за приступ VPN серверу и информационом систему Друштва.

Правилном применом утврђеног поступка за VPN конекцију и начина приступа VPN серверу и рачунарској мрежи, Друштво своди на минимум потенцијалну изложеност штети која може настати услед неауторизованог или неконтролисаног приступа мрежи. Неопходно је да сви уређаји који приступају VPN серверу и рачунарској мрежи имају инсталиран званичан лиценциран софтвер за заштиту од злонамерног кода (рачунарски Антивирус програм) одобрен од стране Сектора за ИКТ.

Правилно коришћење VPN конекције је обавезно за све запослене и сараднике који користе рачунаре или мобилне уређаје за повезивање на мрежу, у сврху обављања посла у име и за рачун Друштва, укључујући коришћење електронске поште и мрежних ресурса са удаљених локација.

Запосленима и ауторизованим корисницима није дозвољено да користе мрежу VPN конекцију и рачунарску мрежу Друштва за активности које нису у домену пословних

активности, радних и других задатака у вези са послом и предметом рада појединачно запосленог.

Одговорност за правилно коришћење мобилних уређаја односи се на све запослене и лица ангажована по другим основима, који имају приступ или користе мобилне уређаје у власништву Друштва.

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 физичког радног простора Друштва, док се за заштиту комуникације мобилних уређаја морају применити исте мере као и за заштиту комуникације у физичким просторијама Друштва. Подешавање ових уређаја врше Носиоци ИКТ функције. Корисници ових уређаја морају обезбедити безбедан простор за њихов рад.

Корисник мобилног уређаја дужан је да води рачуна о исправности повереног уређаја и да га чува на адекватан начин. У случају нестанка, у обавези је да крађу или губитак мобилног уређаја пријави без одлагања, и да достави писану изјаву о околностима губитка или крађе мобилног уређаја. Носиоц ИКТ функције је у обавези да, по пријави крађе или губитка мобилног уређаја, неодложно блокира несталом мобилном уређају приступ информационом систему и кориснику промени креденцијале за приступ. У случају да се пронађе мобилни уређај чији нестанак је пријављен, Носилац ИКТ функције извршиће преглед исправности уређаја и утврдити да ли он може бити поново коришћен за рад на даљину или не.

Безбедност и заштита података у рачунарској мрежи и коришћење записа о догађајима

Члан 15.

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

У рачунарским мрежама су међусобно раздвојене групе информационих услуга, корисника и информациони системи, а мрежни администратор је одговоран за управљање мрежом.

За све мрежне услуге треба применити и укључити механизме безбедности и различите нивое услуга и захтева за одређене корисничке профиле, било да се те услуге пружају унутар организације или из спољног извора. Мрежне услуге обухватају обезбеђивање прикључака, размене података, као и решења за управљање безбедности, као што су заштитна ограничења и системи за откривање неовлашћених упада.

ИКТ систем, укључујући у то и сервисе рачунарске мреже, морају да се користе на начин који неће да произведе загушење ИКТ мреже, ИКТ ресурса и ИКТ сервиса, нити да значајно смањи могућност другим корисницима ИКТ система да приступе и/или користе ИКТ ресурсе и сервисе на ИКТ мрежи.

Мрежни администратор је дужан да стално врши контролни преглед мрежне опреме и мрежних корисника, као и да благовремено предузима мере у циљу заштите и отклањања евентуалних сигурносних и безбедносних неправилности, рањивости и проблема.

У ИКТ систему формирају се записи о догађајима (логови) у вези са активностима корисника, грешкама и догађајима у вези са информационом безбедношћу. Средства за записивање и записане информације су заштићени од неовлашћеног мењања и приступа.

Активности корисника, администратора и оператора система се записују, а записи штите и редовно преиспитују. Власници привилегованих корисничких налога могу бити у стању да управљају записима на опреми за обраду информација која је под њиховом директном контролом, на који начин се штите и прегледају записи да би се одржала одговорност за привилеговане кориснике.

Носилац ИКТ система у оквиру ИКТ система прави записе о догађајима и бележи активности корисника, грешке и догађаје у вези са безбедношћу информација, који се морају чувати и редовно преиспитивати.

Записи о догађајима садрже:

- идентификаторе корисника;
- активности система;
- датуме, време и детаље кључних догађаја, нпр. пријављивања и одјављивања;
- идентитет или локацију уређаја, ако је могуће, и идентификатор система;
- записе о успешним и одбијеним покушајима приступа систему;
- записе о успешним и одбијеним покушајима приступа ИКТ ресурсима;
- промене у конфигурацији система;
- коришћење привилегија;
- 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.

Ради провере начина коришћења ИКТ система и рачунарске мреже, носиоци ИКТ функције рутински скупљају дневнике догађаја (log записа) електронских комуникација и надгледају кориснике ИКТ путем:

- анализе коришћења ресурса
- оптималне расподеле ресурса
- оптималног техничког управљања рада ИКТ ресурса
- актвности које могу да открију и укажу да поједини корисници ИКТ система, нарушавају ИКТ систем или да се баве незаконитим радњама.

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.

Безбедност података који се преносе унутар Друштва као и између Друштва и лица и система изван Друштва (пружаоцима услуга)

Члан 16.

Заштита података који се преносе комуникационим средствима унутар Друштва, између Друштва и система и лица ван Друштва ангажованих за пружање уговорених услуга (у даљем тексту: Пружаоци услуга), обезбеђује се поштовањем одговарајућих правила, преузетих уговорених обавеза и применом адекватних и неопходних контрола.

Правила коришћења информационих ресурса су:

- Информациони ресурси се користе искључиво у пословне сврхе за обављање редовних задатака. Другу намену коришћења посебно одобрава одговорно лице, на образложени писани захтев корисника;
- Употреба електронске поште мора бити сигурна и у складу са пословном праксом. Електронска пошта се може користити искључиво за пословне потребе; размена порука личног садржаја у име Друштва није дозвољена; сви подаци садржани у порукама или њиховом прилогу морају бити у складу са стандардима заштите података и интегритетом Друштва;
- Приступ садржајима на интернету је дозвољен искључиво за пословне намене. Носиоци ИКТ функције користе право контроле, надзора и ревизије логовања, како при повезивању на мрежу, тако и на пријему и слању меил порука;
- Пружаоц услуга је у обавези да и после обављеног посла штити интегритет и поштује правила безбедности информација и чува податке и расположиве информације о Друштву.

Информације обухваћене апликативним услугама које пролазе кроз јавне мреже треба заштити од малверзација, неовлашћеног откривања података и модификовања. Неопхнодно је потврдити идентитет корисника за постављање садржаја, електронског потписивања или обављања трансакција.

Информације укључене у апликативне услуге финансијских и вредносних трансакција 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 примене електронски потпис;
- Гарантовану приватност свих страна које учествују у трансакцији;
- На трансакционим комуникационим каналима мора бити примењено шифровање;
- Коришћење безбедносних протокола предвиђених за трансакције.

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

Приликом закључења уговора неопходно је јасно дефинисати квалитативне, оперативне и финансијске критеријуме контроле и оцене квалитета посла; утврдити поступак извештавања, праћења и поступања у складу са захтевима Друштва у поступку извршења уговорених услуга и извршити оцену извршених услуга и квалитета пружаоца услуга.

Пружаоци услуга имају право на приступ ресурсима ИКТ система и информацијама које су неопходне за пружање предметне уговорене услуге, уз поштовање безбедности ИКТ система и интегритета Друштва.

Друштво успоставља контролу безбедности информација које се односе на процесе и процедуре које ће спроводити пружаоци услуга:

- идентификовање и документовање врсте пружаоца услуга којима ће Друштво дозволити да приступ информацијама;
- стандардизовани процес за управљање односима према пружаоцима услуга;
- дефинисање врста информација које ће различитим типовима пружаоца услуга бити дозвољено ради приступања, праћења и контроле 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 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 пружаоца услуга;

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

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

Носилац ИКТ функције прати, анализира, преиспитује и проверава извршене услуге и усаглашеност са уговореним услугама, на следећи начин:

- 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, и омогући управљање на одговарајући начин;
- Одржава увид у безбедносне активности кроз јасно дефинисан процес извештавања;
- Врши оцену квалитета извршења и саобразности уговорене услуге;
- Пружалац услуге има уговорну обавезу да организује периодичне састанаке

који ће обезбедити редовно извештавање Носиоца ИКТ функције и унапредити квалитет уговорених услуга, односно умањити потенцијалну штету или инциденте који могу настати у поступку извршења услуге или након почетка примене;

- Одржава потпуну контролу над спровођењем услуга и осигурава увид у све осетљиве безбедносне информације и друга средства за обраду информација којима трећа страна приступа, процесира или којима управља;
- Преиспитује трагове, провере и записе о догађајима у вези са безбедношћу код пружаоца услуга, оперативним проблемима, отказима система, праћењу неисправности и сметњама у вези са испорученим услугама.

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 Друштва.

Уговором са пружаоцем услуга треба обезбедити могућност континуиране контроле и управљања променама уговорених услуга, укључујући одржавање и унапређење постојећих процедура и контролу безбедности информација и њиховог утицаја на безбедност ИКТ система.

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 Друштво, ради имплементације нове или промењене апликације, система, контрола или процедура у циљу побољшања безбедности.

Физичка заштита објеката, простора, просторија и средства, опреме и докумената ИКТ система Друштва

Члан 17.

Ради заштите и безбедности ИКТ система и информација Друштво предузима неопходне мере за спречавање неовлашћеног физичког приступа објекту и просторијама, у којима се налазе средства ИКТ система, као и за спречавање оштећења, ометања или крађе опреме за обраду информација.

Друштво пројектује и примењује инструменте за обезбеђивање физичке безбедности канцеларија, просторија и средстава, тако што се онемогућава јавни приступ кључној опреми, конфигурисањем средстава у циљу спречавања видљивости поверљивих информација и активности споља.

Технички и безбедносно осетљива опрема за обраду, пренос и складиштење информација се штити закључавањем у посебно припремљеним просторима или просторијама у којима су обезбеђени неопходни услови за њен рад.

У складу са проценом ризика дефинисане су следеће мере :

- 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, бравама, 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;
- сва пожарна врата у безбедносној зони раздвајања треба да имају алармни уређај, да буду под надзором и треба да функционишу у складу са локалним противпожарним стандардима у погледу осигурања од отказа;
- да би се надгледала сва спољна врата и доступни прозори, треба поставити погодне противпровалне алармне системе у складу са националним, регионалним или међународним стандардима;
- области без особља треба да буду под алармом у сваком тренутку;
- опрема за обраду информација којом управља организација треба да буде физички одвојена од оне којом управљају крајњи корисници ИКТ система;
- неопходно је обезбедити резервни извор електричне енергије (адекватан агрегат) којим се обезбеђује континуитет и несметан рад основних финкција ИКТ система.

Безбедне области од посебног значаја морају бити заштићене одговарајућим контролама уласка како би се осигурало да је само овлашћеним појединцима дозвољен приступ у складу са безбедносним овлашћењима.

Смернице за контролу физичког уласка:

- евидентирати датуме и време уласка и изласка посетилаца, са ограниченим приступом безбедносно ограниченим местима;
- приступ областима у којима се обрађују или чувају поверљиве информације треба да буде ограничен само на овлашћене особе, применом одговарајућих контрола приступа, нпр., као што су картице за приступ и тајни лични идентификациони број (PIN);
- одржавати, надгледати и контролисати физичку књигу записа приступа или електронски траг провере свих приступа;
- запосленима код пружаоца услуга треба одобрити ограничен приступ безбедним областима или опреми за обраду осетљивих информација и то само онда када је то неопходно, овакав приступ треба да буде одобрен и надгледан у сваком тренутку;
- права приступа безбедним областима треба редовно преиспитивати и ажурирати, као и укидати их по потреби.

Опрема ИКТ система се поставља и штити на начин којим се смањује ризик од претњи и опасности из окружења, као и могућности за неовлашћени приступ.

Смернице за безбедност опреме ИКТ система:

- 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 не места која нису видљива особама које нису овлашћене;

- Врши се редовна контрола система за обезбеђење, аларма, противпожарне заштите, као и инсталација за воду, струју, гас, електронске комуникације;
- Опрема мора бити заштићена од атмосферских падавина и осталих утицаја;
- Сервери, рутери и остала битна и технички и безбедносно осетљива опрема за пренос, обраду и складиштење података мора бити смештена у просторији са контролисаним атмосферским условима;
- Редовно се прате температура и влажност ваздуха и остали атмосферски параметри који утичу на рад опреме;
- Просторије са опремом треба редовно чистити од аеросола и прашине;
- Забрањено је конзумирање хране и пића, и пушење у близини опреме за обраду информација.

Опрема ИКТ система се штити од прекида напајања, тако што се:
- обезбеђује вишеструко напајање са различитих траса;
- 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 поправка кварова.

Каблови за напајање и телекомуникациони каблови који преносе податке или који представљају подршку информационим услугама штите се од ометања или оштећења на следећи начин:
- комуникациони мрежни каблови којима се преносе информације или који пружају подршку ИКТ систему морају бити заштићени од пресретања информација или оштећења;
- водови напајања и телекомуникациони водови који улазе у просторије где се налазе сервери и опрема 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 у преносу сигнала;
- за осетљиве или критичне системе се постављају оклопљени водови, користе закључане просторије или кутије ради заштите каблова;
- неовлашћено прикључење уређаја на каблове се контролише и открива техничким претраживањем и физичком провером;
- приступ до разводних табли и у просторије са кабловима се такође контролише.

Опрема ИКТ система се редовно и правилно 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;
- о свим сумњивим или стварним неисправностима, као и о целокупном превентивном и корективном одржавању се чувају записи;
- осетљиве информације периодично и по потреби треба избрисати из опреме;
- пре враћања опреме у рад након одржавања, треба је прегледати да би се уверили да није неовлашћено коришћена или оштећена.

Опрема ИКТ система, информације и подаци или софтвер се измештају само уз одобрење одговорних лица, непосредног руководиоца и стручних лица носиоца ИКТ функције.

Током измештања се примењују следећа правила:

- треба да се одреде логички и организациони разлози за измештање опреме;
- треба да се испитају техничке и логистичке могућности и да се обезбеде неопходни услови за функционисање опреме на новој локацији;
- треба на технички и безбедносно исправан начин поставити опрему и пустити у функцију на новој локацији;
- треба на старој локацији вратити техничку инсталацију и преосталу опрему у стање оптимално за несметани даљи рад и прихват нове опреме;
- осетљиве податке и лиценцирани софтвер избрисати пре уклањања опреме.

Заштита од ризика и рањивости, техничких и безбедносних слабости и превенција и реаговање на безбедносне инциденте и претње ИКТ систему

Члан 18.

Сви запослени су у обавези да извештавају о уоченим и утврђеним слабостима ИКТ система Носиоца ИКТ функкције, у што краћем року, како би се инциденти нарушавања безбедности информација спречили и спречио настанак штете. Догађаји у вези са безбедношћу информација се оцењују и у складу са тим се доноси одлука да ли је потребно да се класификују као инциденти нарушавања безбедности информација.

Носилац ИКТ функције благовремено прикупља информације о безбедносним ризицима, техничким рањивостима информационих система који се користе, вреднује изложеност тим ризицима и рањивостима и предузима одговарајуће мере, узимањем у обзир степен припадајућих ризика.

Носилац ИКТ функције 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 ризици и рањивости које могу да угрозе безбедност ИКТ система, Носилац ИКТ функције је дужан да одмах изврши подешавања, односно инсталира алат (софтвер) који ће отклонити уочене ризике и слабости.

Смернице за откривање безбедносно-техничких слабости и ризика су:

- 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;
- најпре се узимају у разматрање системи са високим ризиком;
- у зависности од тога колико хитно треба неку техничку рањивост узети у разматрање, предузете активност се спроводе у складу са контролама које су везане за управљање променама или спровођењем процедура за одговор на инциденте нарушавања безбедности;

- 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 контроле, као што су деактивирање услуга, прилагођавање или додавање контрола приступа или појачано надгледање како би се открили или спречили постојећи напади и утицало на повећање свести о ризицима и опасностима;

Сви запослени морају одмах известити Носиоца ИКТ функције о догађајима у вези са угроженом безбедношћу ИКТ система, података и информација. Могуће методе комуникације су: електоронска пошта, веб сајтови (интерни, екстерни, портали), телефонска комуникација, говорна порука, писмено извештавање, директан контакт.

У случају погрешног или отежаног функционисања компоненти ИКТ система, корисник извештава на исти начин као и у случају догађаја у вези са безбедношћу ИКТ система.

Процедура за извештавање:

- Запослени који сматра да је дошло до неисправности или безбедносне угрожености ИКТ система, напада или злоупотребе података мора одмах пријавити проблем лични, телефоном или уз опис истог послати поруку електронском поштом Носиоцу ИКТ функције;
- Када је индетификован инцидент запослени је дужан да одмах обавести Сектор за ИКТ, и предузме мере у циљу заштите ресурса ИКТ система;
- Носиоци ИКТ функције и овлашћени администратор врши проверу пријављеног инцидента и даље поступа по одговарајућој процедури.
- Друштво дефинише, идентификује и чува информације које могу да служе као доказ у случају покретања казнених мера унутар организације;
- Носилац ИКТ функције води евиденцију о свим инцидентима, као и пријавама инцидената, на основу које, против одговорног лица, могу да се воде дисциплински, прекршајни или кривични поступци.

Прикупљено знање из детектовања, анализе и решавања инцидената који су нарушили безбедност информација, Друштво користи да би се идентификовали инциденти који се понављају и смањила вероватноћа и утицај будућих инцидената.

Сви запослени су обавезни да се придржавају и спроводе одедбе Акта о безбедности и да свакодневно и доследно спроводе мере и воде бригу у циљу заштите система ИКТ система и безбедности информација.

Посебна обавеза

Члан 19.

Друштво је дужно да периодично, а најмање једном годишње, врши проверу ИКТ система и усклађивање Акта о безбедности, у циљу провере адекватности предвиђених мера заштите и утврђених процедура, овлашћења и одговорности са реалним стањем у ИКТ систему, о чему сачињава извештај.

III. ЗАВРШНА ОДРЕДБА

Ступање на снагу

Члан 20.

Акт о безбедности ступа на снагу даном доношења и објављује се у „Службеном гласнику Железнице Србије“.

ОДБОР ДИРЕКТОРА

Душан Гарибовић

Мира Вукмировић

Владимир Булатовић

АКЦИОНАРСКО ДРУШТВО ЗА ЖЕЛЕЗНИЧКИ ТРАНСПОРТ РОБЕ „СРБИЈА КАРГО“ БЕОГРАД