Србија Карго а.д.
Број: 4/2024-1712-431
Датум: 29.10.2024. године
Београд, Немањина 6

АКТ О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА

У Београду, октобар 2024. године

На основу члана 8. став 1. Закона о информационој безбедности („Службени гласник РС”, број 6/16 94/17 и 77/19), 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 29.10.2024. године донео

Акт о безбедности информационо-комуникационог система

Србија Карго а.д.

I ОСНОВНЕ ОДРЕДБЕ

Предмет Акта

Члан 1.

Актом о безбедности информационо-комуникационог система Србија Карго а.д. (у даљем тексту: Акт о безбедности), у складу са Законом о информационој безбедности („Службени гласник РС”, број 6/16, 94/17 и 77/19, у даљем тексту: Закон), ближе се уређују мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима информационо-комуникационог система Србија Карго а.д. (у даљем тексту: ИКТ систем).

Циљеви Акта о безбедности

Члан 2.

Циљеви доношења Акта о безбедности су:

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

Обавеза примене одредби Акта о безбедности

Члан 3.

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

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

Начелник и Саветник у Центру за ИТ Србија Карго а.д. одговорни су за праћење примене мера безбедности, као и за проверу да су подаци заштићени на начин који је утврђен овим актом и интерним процедурама.

Одговорност запослених

Члан 4.

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

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

Предмет заштите

Члан 5.

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

II МЕРЕ ЗАШТИТЕ

Сваки члан садржи опис мера заштите укључујући предлоге процедура, овлашћења и одговорности учесника у спровођењу мера.

Оператер ИКТ система од посебног значаја одговара за безбедност и предузимање мера заштите ИКТ система.

Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидената, односно превенција и смањење штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима.

Мере заштите ИКТ система се односе на:

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

2) постизање безбедности рада на даљину и употребе мобилних уређаја;

3) обезбеђивање да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који раде и разумеју своју одговорност;

4) заштиту од ризика који настају при променама послова или престанка радног ангажовања лица запослених код оператора ИКТ система;

5) идентификовање информационих добара и одређивање одговорности за њихову заштиту;

6) класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком из члана 3. овог закона;

7) заштиту носача података;

8) ограничење приступа подацима и средствима за обраду података;

9) одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа;

10) утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију;

11) предвиђање одговарајуће употребе криптозаштите ради заштите тајности, аутентичности и интегритета података;

12) физичку заштиту објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему;

13) заштиту од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава која чине ИКТ систем;

14) обезбеђивање исправног и безбедног функционисања средстава за обраду података;

15) заштиту података и средства за обраду података од злонамерног софтвера;

16) заштиту од губитка података;

17) чување података о догађајима који могу бити од значаја за безбедност ИКТ система;

18) обезбеђивање интегритета софтвера и оперативних система;

19) заштиту од злоупотребе техничких безбедносних слабости ИКТ система;

20) обезбеђивање да активности на ревизији ИКТ система имају што мањи утицај на функционисање система;

21) заштиту података у комуникационим мрежама укључујући уређаје и водове;

22) безбедност података који се преносе унутар оператора ИКТ система, као и између оператора ИКТ система и лица ван оператора ИКТ система;

23) испуњење захтева за информациону безбедност у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система;

24) заштиту података који се користе за потребе тестирања ИКТ система односно делова система;

25) заштиту средстава оператора ИКТ система која су доступна пружаоцима услуга;

26) одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга;

27) превенцију и реаговање на безбедносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама;

28) мере које обезбеђују континуитет обављања посла у ванредним околностима.

Влада, на предлог Надлежног органа, ближе уређује мере заштите ИКТ система уважавајући начела из члана 3. овог закона, националне и међународне стандарде и стандарде који се примењују у одговарајућим областима рада.

* Закона о информационој безбедности („Службени гласник РС", број 6/16 94/17 и 77/19)

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

Члан 6.

Србија Карго а.д. у оквиру организационе структуре утврђује послове и одговорности запослених у циљу управљања информационом безбедношћу.

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

- Правилник о организацији и систематизацији радних места;
- Уговори о раду;
- Изјаве о поверљивости;
- Уговори о пружању услуга који садрже одредбу о поверљивости.

Постизање безбедности рада на даљину и употребе мобилних уређаја

Члан 7.

Центар за ИТ Србија Карго а.д. дозвољава рад на даљину и употребу мобилних уређаја од стране запослених, 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.

Рад на даљину

Радни однос за обављање послова ван просторија послодавца обухвата:

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

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

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

VPN процедура дефинише правила и услове за повезивање на мрежу Србија Карго а.д. са удаљене локације. Правилном применом утврђеног поступка и начина приступа Србија Карго а.д. своди на минимум потенцијалну изложеност штети која може настати услед неауторизованог или неконтролисаног приступа мрежи.

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

Ауторизованим корисницима није дозвољено да користе мрежу Србија Карго а.д. за активности које нису у домену пословних активности, радних и других задатака у вези са послом и предметом рада појединачно запосленог.

Захтеви који морају бити испуњени и дефинисани у VPN, биће ближе уређени Процедуром **П.БИТС.01** ***Постизање безбедности рада на даљину и употребе мобилних уређаја.***

Рад на даљину запослених или других радно ангажованих (ангажованих за рад у просторијама послодавца) одобрава Начелник Центра за ИТ Србија Карго а.д.

Коришћење мобилних уређаја

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

Процедуром **П.БИТС.01** ***Постизање безбедности рада на даљину и употребе мобилних уређаја*** дефинише се начин физичке заштитите од крађе и активности које је неопходно предузети у случају крађе или губитка мобилних уређаја, односно безбедносног инцидента, како не би била нарушена безбедност.

Центар за ИТ Србија Карго а.д. спроводи обуку запослених који користе радне станице, у циљу подизања свести о додатним ризицима до којих долази услед оваквог начина рада.

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 Србија Карго а.д.

Право на коришћење преносних рачунара ван седишта Србија Карго а.д. се стиче на основу писаног захтева корисника упућеног Центру за ИТ Србија Карго а.д., односно одговорном лицу. Радне станице које се користе морају бити претходно одобрене и/или набављене од стране Србија Карго а.д. и оцењене као компатибилне са захтевима обезбеђивања адекватног степена заштите.

Рад на даљину може се остварити и коришћењем уређаја који нису мобилни (на пример, десктоп рачунари). Ови уређаји, при томе, морају имати примењене најмање исте безбедносне мере као и сродни уређаји који се налазе у оквиру мреже, док се за заштиту комуникације морају применити исте мере као и за заштиту комуникације преносних рачунара. Подешавање ових уређаја врши Стручни сарадник Центра за ИТ Србија Карго а.д. Корисници ових уређаја морају обезбедити довољно безбедан простор за њихов рад (засебна соба, положај екрана такав да се онемогући посматрање од стране неовлашћених особа и слично).

Главни координатор Центра за ИТ Србија Карго а.д. у оквиру дела послова рачунополагача одговоран је за вођење евиденције о свим уређајима намењеним за рад на даљину. Евиденција о уређајима садржи податке који су неопходни да би се уређај и/или корисник недвосмислено

идентификовали, као што су произвођач, модел, серијски број, инвентарски број, корисник који је задужио уређај и његов кадровски идентификациони број (КИБ).

Корисник мобилног уређаја у обавези је да сваки безбедносни инцидент одмах пријави Центру за ИТ Србија Карго а.д. путем електронске поште на дефинисану мејл адресу. 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. Начелник/Саветник у Центру за ИТ Србија Карго а.д. је у обавези да, по пријави безбедносног инцидента, неодложно блокира приступ несталом мобилном уређају ка информационом систему и кориснику промени креденцијале за приступ.

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

Члан 8.

Србија Карго а.д. се стара да запослени који управљају ИКТ системом, односно запослени који користе ИКТ систем имају адекватан степен образовања и способности, као и свест о значају послова које обављају. Њихове одговорности су утврђене уговором о раду или о ангажовању за рад ван радног односа и интерним актом.

Провера кандидата и услови запошљавања

Србија Карго а.д. спроводи радње у циљу провере испуњености услова сваког појединачног кандидата за запослење, у складу са одговарајућим прописима и етичким правилима, сразмерно пословним захтевима, класификацији информација којима ће имати приступ и сагледаним ризицима.

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

Обавезе у току запослења

Руководство Србија Карго а.д. је дужно да захтева од свих запослених и радно ангажованих лица да примењују мере заштите безбедности, у складу са овим актом и важећим процедурама.

Србија Карго а.д. у циљу развоја, имплементације и одржавања система заштите и безбедности података обезбеђује услове за интеграцију контролних механизама тако што:

- Обезбеђује да се поступци заштите спроводе на организован начин и у складу са процедурама и у континуитету;
- Штити информације и податке са сличним профилом осетљивости и карактеристикама на једнак начин у свим организационим јединицама;
- Спроводи програме заштите на конзистентан и уједначен начин у свим организационим јединицама;

- Координира безбедност и заштиту података у информационом систему са физичком заштитом истих.

Запослени који су надлежни за праћење, анализу, извештавање и предузимање активности на плану спровођења усвојене политике и процедура одређени су Решењем в.д. генералног директора и континуирано се обучавају у циљу унапређења техничког и технолошког знања. Ова лица су ауторизована 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

Запослени у Центру за ИТ Србија Карго а.д. 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. Информисање осталих запослених везано за безбедност информација спроводи се путем интерних и екстерних аката који су доступни у библиотеци објављеној на интернет страници друштва. Начелник Центра за ИТ Србија Карго а.д. процењује, уколико је потребно извршити додатне обуке одређеног броја запослених везано за безбедност информација када и на који начин ће се она обавити.

Дисциплински поступак

Дисциплински поступак се спроводи против запослених који су нарушили безбедност информација или на други начин извршили повреду правила и политике на снази и у примени код Србија Карго а.д.

Дисциплински поступак се покреће по предлогу Начелника Центра за ИТ Србија Карго а.д. након добијене пријаве о нарушеној безбедности информација.

Заштита од ризика који настају при променама послова или престанка радног ангажовања лица запослених у Србија Карго а.д.

Члан 9.

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

За поступање приликом престанка радног односа или ангажовања задужен је Сектор за правне послове и људске ресурсе који о томе доставља информацију Центру за ИТ Србија Карго а.д., у ком случају се предузимају активности у складу са Процедуром **П.БИТС.02** ***Раздужење и задужење ИТ опреме и пратеће документације.***

Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 10.

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

Пописивање имовине

Србија Карго а.д. врши идентификацију имовине која одговара животном циклусу информација и документује њен значај. Животни циклус информације обухвата креирање, обраду, складиштење, пренос, брисање и уништавање података. Србија Карго а.д. прави попис добара који је тачан, ажуран, конзистентан и усклађен са другом имовином.

Евиденцију о информационим добрима и средствима и имовини за обраду информационих добара води Главни координатор у Центру за ИТ Србија Карго а.д. у оквиру дела послова рачунополагача.

Власништво над имовином, прихватљиво коришћење имовине и њен повраћај

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

У оквиру ***Упутства о руковању имовином*** уређују се правила за прихватљиво коришћење имовине повезане са информацијама и опремом за обраду информација.

Запослени и екстерни корисници су обавезни да врате сву имовину Србија Карго а.д. коју поседују након престанка њиховог запослења, уговора или споразума о ангажовању на одређеним пословима и задацима.

Током отказног рока запослених, Србија Карго а.д. контролише њихово неовлашћено копирање, умножавање или преузимање релевантних заштићених информација.

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

Члан 11.

Класификовање податка је поступак утврђивања и појединачног додељивања нивоа тајности податка, у складу са њиховим значајем за Србија Карго а.д.

Србија Карго а.д. означава типове и локације података као ограничене, поверљиве, интерне или јавне. Имовина се означава уз помоћ идентификационих налепница које носе одговарајућу класификациону ознаку.

Србија Карго а.д. 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 угрожава опстанак.

Србија Карго а.д. врши класификацију ради:

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

Класификација документа мора да буде усклађена са правилима контроле приступа.

Србија Карго а.д. поступа у складу са усвојеном Шемом класификовања података. У оквиру процедуре **П.БИТС.03** ***Поступање са имовином*** (класификовање података и радње за поступање, обраду, складиштење и пренос података) се дефинишу радње за поступање, обраду, складиштење и пренос података.

Заштита носача података

Члан 12.

Центар за ИТ Србија Карго а.д. обезбеђује спречавање неовлашћеног откривања, модификовања, уклањања или уништења података који се чувају на носачима података.

Евиденцију носача на којима су снимљени подаци, води Главни координатор у оквиру дела послова рачунополагача у Центру за ИТ Србија Карго а.д.

Управљање преносним носачима података (медијума)

Србија Карго а.д. је дужан да развија и имплементира процедуру о управљању преносним носачима, у складу са усвојеном Шемом класификовања података.

Ближе се дефинише у Процедури **П.БИТС.04** ***Заштита носача података.***

Расходовање носача података (медијума)

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

Расходовање медијума на безбедан начин Србија Карго а.д. врши свођењем на минимум ризика од могућег преузимања осељивих података од стране неовлашћених особа.

Процедуром за безбедно расходовање медијума који садрже поверљиве податке утврђују се различити начини процеса расходовања, а у складу са осетљивошћу података.

Процедуром **П.БИТС.04** ***Заштита носача података*** се дефинишу правила о расходовању носача података (медијума).

Физички пренос носача података (медијума)

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

Процедуром **П.БИТС.04** ***Заштита носача података*** се дефинишу правила физичког преноса носача података (медијума).

У случају транспорта носача података са информацијама, Начелник Центра за ИТ Србија Карго а.д. одређује лице које ће вршити транспорт и начин транспорта.

Ограничење приступа подацима и средствима за обраду података

Члан 13.

Подацима и средствима за обраду података је неопходно ограничити приступ у складу са утврђеним степеном тајности података и усвојеном Шемом класификовања података према члану 11. овог Акта.

Центар за ИТ Србија Карго а.д. је формирао Контролну листу приступа која садржи попис свих информационих објеката и субјекте који им могу приступити.

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

Ближе се дефинише Процедуром **П.БИТС.05** ***Приступ мрежи и мрежним уређајима***.

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

Члан 14.

Центар за ИТ Србија Карго а.д. управља приступом ИКТ систему и услугама кроз употребу корисничких налога.

Управљање корисничким налозима врши се уз поштовање следећих принципа:

- кориснички налози су јединствени, тако да се корисници могу везати уз њих и учинити одговорним за своје активности;
- коришћење заједничких налога 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 налози;
- периодично идентификовање и уклањање или онемогућавање вишеструких корисничких налога;
- вишеструки налози 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 (администраторских) права за приступ врши се на основу одлуке одговорног лица Начелника Центра за ИТ Србија Карго а.д.

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

Привилегована права за приступ која треба доделити корисничком налогу другачија су од оних која се користе за редовне активности. Редовне пословне активности не треба вршити из привилегованих корисничких налога. Компетенције корисника са привилегованим правима за приступ се редовно преиспитују ради провере да ли су у складу са њиховим обавезама.

Забрањено је неовлашћено коришћење општих корисничких налога администратора.

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

Центар за ИТ Србија Карго а.д. врши ажурирање права корисника за приступ након сваке промене (унапређење, разрешење и крај запослења).

Запосленима, другим радно ангажованим и трећим лицима по престанку запослења или истеку уговора укида се право за приступ ИКТ систему.

Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију

Члан 15.

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 када примете да постоји било какав наговештај могућег компромитовања.

Шифре морају да:

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

Шифре не заснивати на личним подацима корисника, као што су име, телефонски број или датум рођења и не смеју садржати више од 3 узастопна идентична бројчана или словна знака.

Корисници су дужни да привремене шифре промене приликом првог пријављивања.

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

Члан 16.

У циљу заштите података Србија Карго а.д. развија и имплементира политику коришћења криптографских контрола.

Криптозаштита обезбеђује:

- Аутентификацију (идентификацију корисника и других системских ентитета који захтевају приступ или одобрење акције корисника);
- Непорецивост (примена криптографских техника, најчешће дигиталног потписа, како би се добила потврда о извршавању или неизвршавању неке акције од стране појединачног корисника);

Поверљивост (применом шифровања врши се заштита осетљивих или критичних информација које се складиште или преносе);

- Интегритет (непроменљивост података који се преносе).

Поступак криптографске контроле обухвата:

- анализу и процене потреба примене криптографије у пословним процесима укључујући опште принципе према којима би пословне информације требало да се штите;
- ниво заштите се одређује узимањем у обзир типа алгоритма за криптовање података, јачине и квалитета криптографског алгоритма;
- примену шифровања за заштиту осетљивих података приликом преноса мобилним или другим медијумима, уређајима или преко комуникационих водова.

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

Члан 17.

Србија Карго а.д. је дужан да предузме мере ради спречавања неовлашћеног физичког приступа просторијама, у којима се налазе средства и документи ИКТ система, као и спречавање оштећења и ометања информација. У Центру за ИТ Србија Карго а.д. одређена је посебна канцеларија за складиштење и чување ИТ документације.

Зона раздвајања и успостављање система физичке безбедности

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

У складу са проценом ризика дефинисане су следеће зоне раздвајања:

- зоне раздвајања на примарној и секундарној (ДР) локацији Дата центара су физички исправне и заштићене од неовлашћеног приступа помоћу аларма, брава и видео надзора. На обе локације су монтирана сигурносна врата а прозори су обезбеђени видео надзором;

- на примарној локацији Дата центра, у пословној згради, постоји пријавница са особљем за контролу физичког приступа у зграду; приступ примарном Дата центру је ограничен само на овлашћена лица;
- Дата центар на примарној локацији је обезбеђен блиндираном заштитом од влаге, пожара и поплава;
- зоне раздвајања на удаљеним локацијама су физички исправне и у закључаним просторијама.

Контрола физичког уласка

Безбедносне области су заштићене одговарајућим контролама уласка како би се осигурало да је само овлашћеним појединцима којима је дозвољен приступ одобрен од стране Начелника Центра за ИТ Србија Карго а.д:

- евидентирање датума и времена уласка и изласка посетилаца се врши путем електронске коресподенције. Сви посетиоци којима је приступ одобрен, могу физички ући у просторију Дата центра само уз присуство овлашћеног лица Центра за ИТ Србија Карго а.д.
- приступ областима у којима се обрађују или чувају поверљиве информације је ограничен само на овлашћена лица Центра за ИТ Србија Карго а.д.
- права приступа безбедносним областима редовно се ажурирају.

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

Србија Карго а.д. 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 информација, активностима споља. Физичка заштита се мора планирати и за случајеве природних катастрофа, непријатељских напада или несрећа.

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

Члан 18.

Постављање и заштита опреме

Опрема је постављена и штити се на начин којим се смањује ризик од претњи и опасности из окружења, као и могућношћу неовлашћеног приступа:

- Опрема је постављена на месту које је обезбеђено од неовлашћеног приступа;
- Опрема за обраду информација је постављена 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 се редовно чисте од прашине;
- Забрањено је конзумирање хране и пића и пушење у близини опреме за обраду информација;

- Редовно се прате температура и влажност ваздуха;
- Опрема је заштићена од атмосферских падавина.

Главни координатор/Начелник одељења/Стручни сарадник у Центру за ИТ Србија Карго а.д. редовно прати услове околине, као што су температура и влажност, који би могли негативно да утичу на рад опреме за обраду информација.

Помоћне функције за подршку

Опрема се штити од прекида напајања, тако што се:

- помоћна опрема за напајање одржава у складу са спецификацијама опреме произвођача и прописима;
- капацитет помоћне опреме редовно процењује;
- редовно прегледа и испитује у погледу правилног функционисања и врши поправка кварова;
- обезбеђује вишеструко напајање са различитих траса.

Безбедносни елементи приликом постављања каблова

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 до зграде;
- каблови за напајање се одвајају од комуникационих каблова да би се спречиле сметње;
- приступ до разводних табли и у просторије са кабловима се контролише.

Одржавање опреме

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

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

Измештање и премештање имовине

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

- Овлашћена лица Центра за ИТ Србија Карго а.д. и пружаоци услуга врше измештање имовине за коју добијају одобрење од стране Центра за ИТ Србија Карго а.д;

- Унапред се одређује временски рок за измештање опреме и проверава се усклађеност приликом повратка;
- Обострано потписаним документом потврђује се идентитет и улога лица које користи или поступа са имовином приликом премештања и ова документација мора бити враћена са опремом, информацијама или софтвером.

Безбедност опреме корисника без надзора

Корисници треба да обезбеде да опрема која је без надзора има одговарајућу заштиту, у циљу онемогућавања приступа заштићеним информацијама и подацима.
Ближе се дефинише Процедуром **П.БИТС.03** ***Поступање са имовином***.

Остављање осетљивих и поверљивих докумената и материјала

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 или када се документа и материјали не користе.

Ближе се дефинише Процедуром **П.БИТС.06** ***Остављање осетљивих и поверљивих докумената и материјала.***

Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 19.

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

Центар за ИТ Србија Карго а.д. за одређене процесе, успоставља радне процедуре, које садрже инструкције за детаљно извршење следећих послова:

а) инсталација и конфигурација система:
- планирање инсталације - пре инсталације, израђује се план који укључује захтеве система и безбедносне стандарде, у сарадњи са спољним консултантима
- избор софтвера и хардвера - избор поузданих компоненти и софтвера који су у складу са актуелним безбедносним прописима, уз савете консултаната
- процедура инсталације - инсталација се врши уз непосредну сарадњу овлашћених техничара и спољних консултаната, поштујући све безбедносне процедуре
- конфигурација безбедности - систем се конфигурише у складу са безбедносним политикама, укључујући корисничке акције, права приступа и шифровање података, уз стручну подршку консултаната
- тестирање и верификација - након конфигурације, спроводе се тестови функционалности и безбедности у сарадњи са консултантима, како би се осигурала исправност и заштита система

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

Ближе се дефинише Процедуром **П.БИТС.01** ***Постизање безбедности рада на даљину и употребе мобилних уређаја***, **П.БИТС.05** ***Приступ мрежи и мрежним уређајима*** и **П.БИТС.09** ***Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга.***

в) израда резервних копија врши се аутоматски свакодневно и то: Veeam backup и на магнетне траке које се чувају у специјално обезбеђеној просторији на секундарној удаљеној локацији - ДР локација. Месечни бекап уписан на магнетну траку се чува у сефу у просторијама Центра за ИТ. Такође се уписује и годишњи бекап на магнетне траке који се чува у сефу у просторијама Центра за ИТ.

Администратори Центра за ИТ се обавештавају о извршеном бекапу свакодневно путем аутоматског мејла на дефинисану мејл групу;

г) обрада захтева за временски распоред активности: дефинисан је план за израду дневних, месечних и годишњих резервних копија;

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

Начелник/Саветник Центра за ИТ се обавештавају у случају грешака или ванредне ситуације од стране запослених Србија Карга а.д. који су упознати да морају исте да пријаве у најкраћем року телефоном и мејлом. Начелник/Саветник Центра за ИТ су задужени за пријављивање грешака или других ванредних ситуација спољним сарадницима, који затим пружају додатне инструкције и подршку у поступању. Ово укључује ограничења у коришћењу системских помоћних функција у складу са добијеним смерницама

ђ) листа контаката за подршку и ескалацију (укључујући екстерне контакте за подршку) у случају неочекиваних оперативних или техничких потешкоћа;
Листу контаката за подршку и ескалацију води и ажурира Начелник/Саветник Центра за ИТ

е) израда инструкција за управљање поверљивим подацима:

Ближе се дефинише Процедуром **П.БИТС.03** ***Поступање са имовином***, **П.БИТС.06** ***Остављање осетљивих и поверљивих докумената и материјала***, **П.БИТС.04** ***Заштита носача података*** и **П.БИТС.09** ***Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга*;**

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

Администраотри Центра за ИТ врше поновно покретање и опоравак у ИТ система у сарадњи са спољним сарадницима који пружају додатне инструкције и подршку у поступању,

з) управљање системским записима (логовима):

Управљање системским записима (логовима) врше Администратори у Центру за ИТ. Они осигуравају правилно управљање системским записима, укључујући идентификацију и пријаву потенцијалних безбедносних инцидената. У случају потребе додатну подршку врше спољни сарадници, који пружају додатне инструкције у поступању.

и) поступак за надгледање се врши на дневном нивоу праћењем стања на дефинисаним порталима ИТ система (сервери, бекап, комуникациона и мрежна опрема, уређаји за безбедност система)

За усвајање, измене и допуне радних процедура овлашћен је Начелник Центра за ИТ, Србија Карго а.д.

Управљање расположивим капацитетима

Коришћење ресурса се континуирано надгледа, подешава и пројектује у складу са захтеваним капацитетима, како би се осигурале неопходне перформансе 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

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

а) дефинисана су правила за преношење софтвера из развојног статуса у продукциони статус;

б) развојни и продукциони радови на софтверима се извршавају на различитим системима или рачунарским процесорима, као и у различитим доменима или директоријумима;

в) промене на продукционим софтверима се испитују у окружењу за тестирање пре него што се примене на продукционе системе;

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

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

ђ) да би се смањио ризик од грешке, корисници треба да примењују различите корисничке профиле за продукционе и системе за тестирање;

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

За обезбеђивање исправног и безбедног функционисања средстава за обраду података и примену радних процедура задужен је Саветник Центра за ИТ Србија Карго а.д.

Заштита података и средстава за обраду података од злонамерног софтвера

Члан 20.

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

као и на одговарајућим контролама приступа систему и управљању захтеваним и потребним променама.

Поступак контроле и предузимање мера против злонамерног софтвера

Центар за ИТ Србија Карго а.д. одређује и примењује контроле откривања, спречавања и опоравка, ради заштите од злонамерног софтвера.

Процедуре о заштити од злонамерног софтвера са Листом провера које се спроводе дефинишу се Процедуром **П.БИТС.07** ***Поступак контроле и предузимање мера против злонамерног софтвера***.

У случају да корисник примети необично понашање рачунара, запажање треба одмах пријавити на дефинисану мејл адресу.

У циљу заштите од упада у ИКТ систем, Начелник одељења у Центру за ИТ Србија Карго а.д је дужан да одржава систем за спречавање упада.

Корисницима који су прикључени на ИКТ систем у случају доказане злоупотребе Интернета Начелник одељења/Стручни сарадник у Центру за ИТ Србија Карго а.д. укида приступ.

Заштита од губитка података

Члан 21.

Центар за ИТ Србија Карго а.д. врши израду резервних копија које обухватају системске информације, апликације и податке који су неопходни за опоравак целокупог система у случају наступања последица изазваних ванредним околностима.

Резервне копије информација и података

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

Заштитне копије корисницима обезбеђују податке који се налазе на серверима, 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 сервера, конфигурационих и log фајлова, критичних фајлова за функционисање оперативних система (серверских и комуникационих) или целих оперативних система, апликација, сервиса и базе података.

Заштитне копије омогућавају брзо и ефикасно враћање у функцију система у случају нежељених догађаја и праве се у време када се не умањује расположивост сервиса, апликација, база података и комуникационих капацитета ИКТ система. За чување заштитних копија користе се магнетне траке.

Центар за ИТ Србија Карго а.д. извршава следеће задатке:

- процењује осетљиве и критичне податке за које је потребно правити резервне копије;
- креира план прављења резервних копија;
- 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.

План израде резервних копија информација обухвата следеће:

- тачне и потпуне записе о резервним копијама;
- обим и учесталост израде резервних копија;
- резервне копије одражавају пословне потребе организације;
- резервне копије се складиште на локацији на довољној удаљености (ДР локацији), како би се избегло свако оштећење на примарној локацији;
- резервне копије информација су физички заштићене и обезбеђене од утицаја околине;
- медијуми са резервним копијама редовно се проверавају, ради сигурности њихове употребе у ванредним ситуацијама и када је то неопходно;
- у ситуацијама у којима је важна поверљивост, резервне копије се штите помоћу шифровања.

За заштиту од губитка података одговоран је Главни координатор у Центру за ИТ Србија Карго а.д.

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

Члан 22.

У ИКТ систему Центра за ИТ Србија Карго а.д. формирају се записи о догађајима (логови) у вези са активностима корисника, грешкама и догађајима у вези са информационом безбедношћу.

Записивање догађаја

Центар за ИТ Србија Карго а.д. прави записе о догађајима и бележи активности корисника, грешке и догађаје у вези са информационом безбедношћу, који се морају чувати и редовно преиспитивати. Администратори система немају дозволу да бришу логове о сопственим активностима.
Записи о догађајима садрже:

- налоге 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 подацима и другим 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.

Заштита информација у записима

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

Забрањено је неовлашћено уношење следећих измена:

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

Записи администратора и корисника

Активности администратора и корисника система се записују, а записи штите и редовно преиспитују. Кориснички налози са администраторским правима управљају записима на опреми за обраду информација која је под њиховом директном контролом.

Сатови свих одговарајућих система за обраду информација заштите морају бити синхронизовани према UTC (Coordinated Universal Time) времену, како би се обезбедила тачност свих логова, јер ће можда бити коришћени приликом истраге неког инцидента.

Обезбеђивање интегритета софтвера и оперативних система

Члан 23.

Центар за ИТ Србија Карго а.д. спроводи процедуре којима се обезбеђује контрола интегритета инсталираног софтвера и оперативних система, у складу са 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;
- апликације се имплементирају после успешно спроведеног испитивања, а спроводе се на засебним системима, односно тестним окружењима;
- све одговарајуће библиотеке изворних програма се ажурирају;
- пре имплементације било каквих промена, успоставља се стратегија повратка на претходно стање;
- приликом свих ажурирања на библиотекама оперативних програма, треба одржавати записе за проверу;
- као меру предострожности за неочекиване ситуације треба сачувати претходне верзије апликативног софтвера;

Инсталацију и подешавање софтвера врши Начелник одељења/Стручни сарадник у Центру за ИТ Србија Карго а.д., односно запослени који има овлашћење за то.

Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 24.

Центар за ИТ Србија Карго а.д. 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

Центар за ИТ Србија Карго а.д. благовремено прикупља информације о техничким рањивостима информационих система који се користе, вреднује изложеност тим рањивостима и предузима одговарајуће мере, узимањем у обзир припадајућих ризика.

- дефинише и успоставља улоге и одговорности у вези са управљањем техничким рањивостима;
- најмање једном месечно, а по потреби и чешће, врши анализу дневника активности (activitylog, history, securitylog, transactionlog и др) у циљу идентификације потенцијалних слабости ИКТ система;
- за софтверске и друге технологије се одређују информациони ресурси за идентификовање одговарајућих техничких рањивости и за одржавање свести о истима;
- реаговање без одлагања на обавештење о могућим техничким рањивостима;
- када је могућа техничка рањивост идентификована, препознају се припадајући ризици и активности које треба предузети;
- најпре се узимају у разматрање системи са високим ризиком;
- ефективан процес управљања техничким рањивостима се усклађује са активностима које се односе на управљање инцидентима, тако да обезбеди техничке процедуре које треба спровести ако се догоди неки инцидент.

Уколико се идентификују рањивости које могу да угрозе безбедност ИКТ система, Начелник одељења/Стручни сарадник у Центру за ИТ Србија Карго а.д. односно запослени који има овлашћење је дужан да одмах изврши подешавања и инсталира софтвер који ће отклонити уочене рањивости.

Ограничења у погледу инсталације софтвера

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

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

Члан 25.

Приликом спровођења ревизије ИКТ система, Србија Карго а.д. обезбеђује да ревизија има што мањи утицај на фукционисање система.

Поступак контроле информационих система:

- Са руководством се договарају захтеви за проверу приступа систему и подацима;
- Предмет и подручје испитивања за проверу су унапред договорени и строго контролисани;
- Испитивања за проверу су ограничена на приступ читањем;
- Приступ који није ограничен само на читање дозвољен је само на издвојеним копијама системских датотекама, које се по завршеној провери бришу;
- 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 врши Центар за интерну ревизију Србија Карго а.д. а спољну ревизију по захтеву руководства Србија Карго а.д.

Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 26.

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

Мрежне услуге обухватају обезбеђивање прикључака, услуге на приватним мрежама и мреже са додатним функцијама, као и решења за управљање безбедношћу (заштита и системи за откривање упада).

Начелник одељења у Центру за ИТ Србија Карго а.д. је дужан/а да стално врши контролни преглед мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности.

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

Члан 27.

Заштита података који се преносе комуникационим средствима унутар Србија Карго а.д. између Центра за ИТ и лица ван Центра за ИТ, обезбеђује се утврђивањем одговарајућих правила, процедура, потписивањем уговора и споразума, као и применом адекватних контрола.

- Правила коришћења електронске поште

Употреба електронске поште мора бити у складу са успостављеним процедурама и адекватним контролама над спровођењем истих. Електронска пошта се користи за пословне потребе; сви подаци садржани у порукама или њиховом прилогу морају бити у складу са стандардима заштите података.

- Правила коришћења Интернета

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

- Правила коришћења информационих ресурса

Информациони ресурси се користе у пословне сврхе, на раду или у вези са радом. Другу намену коришћења посебно одобрава Начелник/Саветник Центра за ИТ, на образложени писани захтев корисника.

Споразуми о преносу информација

Безбедан пренос пословних информација између организације и трећег лица обезбеђује се поштовањем Уредби које доноси Влада Републике Србије.

Ово ће се примењивати само ако то безбедоносна ситуација налаже (пример у случају природних катастрофа и слично).

Размена електронских порука

Заштита информација укључених у размену електронских порука се регулише процедуром **П.БИТС.08** ***Размена електронских порука.***

Споразуми о поверљивости или неоткривању

Споразуми о поверљивости или неоткривању имају за циљ заштиту Србија Карго а.д. 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 које треба заштитити;
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 информације;
6. процес за обавештавање и извештавање о неовлашћеном откривању или приступу поверљивим информацијама;
7. радње које треба предузети у случају кршења овог споразума.

Питања информационе безбедности у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система

Члан 28.

У оквиру животног циклуса ИКТ система који укључује фазе конципирања, спецификације, пројектовања, развијања, тестирања, имплементације, коришћења, одржавања и на крају

повлачења из употребе, Центар за ИТ Србија Карго а.д. 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.

Начелник/Саветник/Главни координатор у Центру за ИТ Србија Карго а.д. је задужен за технички надзор над реализацијом од стране извођача, односно испоручиоца.

О успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова ИКТ система Начелник/Саветник/Главни координатор у Центру за ИТ Србија Карго а.д. води документацију.

Анализа и спецификација захтева за информациону безбедност

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, непорецивост 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 се примењује за све купљене производе.

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

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

Обезбеђивање апликативних услуга у јавним мрежама

Информације обухваћене апликативним услугама које пролазе кроз јавне мреже су заштићене од малверзација, неовлашћеног откривања података и модификовања. Дефинисани су идентитети корисника и извршена подела овлашћења и одговорности за постављање садржаја, електронског потписивања или обављања трансакција.

Заштита трансакција апликативних услуга

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

Трансакције морају да подрже следеће услове:

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

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

Члан 29.

Под тестирањем ИКТ система, као 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 очекивана 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, Србија Карго а.д. избегава коришћење оперативних података који садрже личне податке или било које друге поверљиве податке и информације на основу којих је могуће идентификовати појединачног добављача, купца, запосленог или др. Уколико се за сврху испитивања користе лични подаци или неке друге поверљиве информације, онда се сви поверљиви подаци и информације пре коришћења штите анонимизацијом личних података, уклањањем садржаја или изменом текста садржаја у предметном делу.

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

- за свако копирање оперативних података у тестно окружење се издаје посебно овлашћење;
- приликом тестирања апликативних система примењују се процедуре за контролу приступа које се примењују и на продукционим системима.

За податке који су означени ознаком тајности, односно службености као поверљиви подаци, или су подаци о личности коришћени приликом тестирања система, одговорна су лица која имају отворене корисничке налоге за унос и ажурирање података у информационе апликације Србија Карго а.д., у складу са прописима којима је дефинисана употреба и заштита такве врсте података.

За потребе тестирања ИКТ система односно делова система Администратор у Центару за ИТ Србија Карго а.д. може да користи 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 неовлашћених приступа, а које се примењују и на оперативним системима. Скуп криптографских мера које ће бити примењене за заштиту података утврђује Администратор у Центару за ИТ Србија Карго а.д., узимајући у обзир њихову поузданост и сврсисходност.

Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга

Члан 30.

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

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

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

Србија Карго а.д. успоставља контролу безбедности информација које се односе на процесе и процедуре које ће спроводити пружаоци услуга, што се дефинише Процедуром **П.БИТС.09** ***Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга.***

Уговарање обавезе обезбеђивања безбедности у споразумима са пружаоцима услуга

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

Пример: "Сви подаци и информације садржани 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 у складу са овим уговором и обавезом извршења уговорених послова и обавеза, буду стављене на располагање и увид запосленима, уколико је то неопходно ради извршења обавеза из овог уговора.

Уговорне стране се нарочито обавезују да поступају обазриво са подацима о личности до којих могу доћи у поступку извршења услуга за оператора ИКТ система, 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 Србија Карго а.д. у погледу безбедности информација прошире и на своје подуговараче за додатне услуге или производе.

Начелник/Саветник/Главни координатор у Центру за ИТ Србија Карго а.д. је одговоран за контролу приступа и надзор над извршењем уговорених обавеза, као и за поштовање одредби правилника којима су такве активности дефинисане.

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

Члан 31.

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

Праћење и преиспитивање извршења уговорених обавеза пружаоца услуга

Начелник/Саветник/Главни координатор у Центру за ИТ Србија Карго а.д. редовно прати, анализира, преиспитује и проверава извршене услуге и усаглашеност са уговореним услугама, на следећи начин:

1. Надгледање и преиспитивање услуга се може вршити 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 уговорну обавезу да организује и припреми периодичне састанаке који ће обезбедити редовно извештавање Србија Карго а.д. и унапредити квалитет уговорених услуга, односно умањити потенцијалну штету или инциденте који могу настати у поступку извршења услуге или након почетка примене;
5. Начелник/Саветник/Главни координатор у Центру за ИТ Србија Карго а.д.одржава потпуну контролу над спровођењем услуга и осигурава увид у све осетљиве или критичне безбедносне информације и друга средства за обраду информација којима трећа страна приступа, које процесуира или којима управља;
6. Начелник/Саветник/Главни координатор у Центру за ИТ Србија Карго а.д. одржава увид у безбедносне активности кроз јасно дефинисан процес извештавања;
7. Преиспитује трагове провере и записа 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 Србија Карго а.д. у поступку извршења уговорених услуга и извршити оцену извршених услуга и квалитета 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 Србија Карго а.д.

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, крајњих, 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 пружаоца услуга

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

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 Србија Карго а.д. ради имплементације нове или промењене апликације, система, контрола или процедура у циљу побољшања безбедности.

Превенција и реаговање на безбедносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама

Члан 32.

Одговорност појединаца и поступак одговора на инциденте

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

Начелник у Центру за ИТ Србија Карго а.д., одређује Администраторе у оквиру Центра за ИТ чији је задатак да придржавајући се процедура одређених овим чланом, планирају, детектују, анализирају и информишу надлежне у току и након инцидента.

Администратор у Центру за ИТ Србија Карго а.д. подразумева одговарајућа техничка знања како би на најбржи и одговарајући начин могао да одговори на безбедносне инциденте.

Администратор у Центру за ИТ Србија Карго а.д. 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, запослени је дужан да о томе одмах обавести Начелника/Саветника у Центру за ИТ Србија Карго а.д. или на дефинисану мејл адресу.

Начин поступања у случају инцидената детаљно се описује Поступком одговора на инциденте.

Извештавање о догађајима у вези са безбедношћу информација

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

Главни координатор у Центру за ИТ Србија Карго а.д. је дужан да припреми план и неколико метода комуникације које би могле да се примене у зависности од инцидента. Могуће методе комуникације су: електорнска 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.

Процедура:

1. Запослени који сматра да је дошло до напада или злоупотребе података мора одмах припремити опис проблема и послати га електронском поштом Центру за ИТ (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 врши проверу пријављеног инцидента и даље поступа по одговарајућој процедури.

Када је индетификован инцидент запослени је дужан да одмах обавести Начелника/Саветника у Центару за ИТ Србија Карго а.д. на дефинисану мејл адресу и предузме мере у циљу заштите ресурса ИКТ система.

Начелник у Центру за ИТ Србија Карго а.д. води евиденцију о свим инцидентима, као и пријавама инцидената, у складу са уредбом, на основу које, против одговорног лица, могу да се воде дисциплински, прекршајни или кривични поступци.

Извештавање о утврђеним слабостима система заштите

Сви запослени су у обавези да о уоченим и утврђеним слабостима ИКТ система известе Центар за ИТ Србија Карго а.д. на дефинисану мејл адресу у што краћем року, како би се инциденти нарушавања информационе безбедности спречили 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 безбедноости

Центар за ИТ Србија Карго а.д. 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 напада.

План за превенцију од безбедносних ризика:

- Информације које имају приоритет заштите према Класификационој шеми – детаљи о подацима који се налазе у систему, њихов ниво осетљивости и поверљивости дефинишу се процедуром **П.БИТС.03 - *Поступање са имовином*** и листи услуга (попис свих услуга које Центар за ИТ Србија Карго а.д. пружа, рангиране по важности)
  - одржавање и мониторинг Дата центара
  - одржавање и мониторинг ИТ мреже
  - корисничка подршка и отклањање сметњи на хардверу и софтверу
- Дефинисан је План за 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 поступак за restore података а према документу ***Veeam backup обука.***
- Одређена је одговорна особа задужена за односе са јавношћу, као и упутство које информације је дозвољено јавно објавити у случају напада.

У случају инцидента запослени су дужни да исти одмах пријаве Центру за ИТ.

Центар за ИТ је дужан да истражи инцидент и у случају потребе о томе обавести:

- Национални ЦЕРТ Републике Србије, Палмотићева 2, Београд
- Канцеларија за информационе технологије и електронску управу, Немањина 11, Београд
- Безбедносно информативна агенција – БИА, Улица краљице Ане бб, Београд
- Министарство унутрашњих послова Републике Србије, Булевар Михајла Пупина 2, Београд

Центар за ИТ поступа према препорукама горе контактираних служби а у зависности од врсте и тежине инцидента. Након предузетих мера за санирање последица инцидента, о томе је неопходно известити руководство Србија Карго а.д.

Прикупљено знање из анализе и решавања инцидената који су нарушили информациону безбедност, Центар за ИТ Србија Карго а.д. користи да би се идентификовали инциденти који се понављају и смањила вероватноћа и утицај будућих инцидената.

Прикупљање доказа

Центар за ИТ Србија Карго а.д. дефинише и примењује процедуре за идентификацију, сакупљање, набавку и чување информација које могу да служе као доказ у случају покретања дисциплинског, прекршајног или кривичног поступка.

Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 33.

Центар за ИТ Србија Карго а.д. примењује мере које обезбеђују континуитет обављања посла у ванредним околностима, како би ИКТ систем у што краћем року био у функционалном стању.

Планирање континуитета мера безбедности информација

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

При изради Плана за обезбеђење континуитета пословања за хардверске компоненте ИКТ система треба обухватити следеће:

- документацију за логички и физички дијаграм и копије пројеката;
- заштитне копије конфигурационих фајлова и оперативног система активних уређаја;
- постојање резервне опреме;
- унапред направљене конфигурације за различите сценарије;
- израду резервних копија.

При изради Плана опоравка од нежељених догађаја ИКТ система:

- проценити најкритичније апликације, податке, конфигурационе фајлове и системски софтвер за који треба направити резервне копије;
- одредити место чувања копије;
- одредити нову локацији 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; - одредити изворе непрекидног напајања електричном енергијом.

Такође, при изради Плана опоравка од нежељених догађаја ИКТ система потребно је предвидети:

- постојање документације за сервисе, апликације и базе података;
- процедуре инсталације и конфигурисања 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.

План опоравка од нежељених догађаја ИКТ система у Центру за ИТ Србија Карго а.д. се ближе дефинише у документу ***Опоравак продукционог окружења услед ДР сценарија.***

Имплементација континуитета безбедности информација

Да би се осигурао потребан ниво континуитета безбедности информација током ванредних ситуација, Начелник/Саветник у Центру за ИТ Србија Карго а.д. примењује процедуре и контроле описане у Плану за обезбеђење континуитета пословања.

Начелник/Саветник у Центру за ИТ Србија Карго а.д. редовно врши проверу усвојених процедура контроле континуитета безбедности информација, како би оне биле адекватне и ефективне током ванредних ситуација.

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

III ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Посебна обавеза Србија Карго а.д.

Члан 34.

Обавеза Србија Карго а.д. је 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 одговорности у ИКТ систему Србија Карго а.д.

В.д. генералног директора Србија Карго а.д ће на предлог Центра за ИТ донети посебне процедуре којима се ближе уређује постизање безбедности рада на даљину и употребе мобилних уређаја, заштита од ризика који настају при променама послова или престанка радног ангажовања лица запослених у Србија Карго а.д. (раздужење и задужење ИТ опреме и пратеће документације), поступање са имовином (класификовање података и радње за поступање, обраду, складиштење и пренос података), заштита носача података, приступ мрежи и мрежним уређајима, остављање осетљивих и поверљивих докумената и материјала, поступак контроле и предузимање мера против злонамерног софтвера, размена електронских порука, заштита средстава оператора ИКТ система која су доступна пружаоцима услуга и руковање имовином.

Ступање на снагу Акта о безбедности

Члан 35.

Овај Акт о безбедности информационо - комуникационог система Србија Карго а.д. ступа на снагу даном доношења и биће објављен у Службеном гласнику " Железнице Србије ".

Ступањем на снагу овог Акта престаје да важи Акт о безбедности информационо - комуникационог система Србија Карго а.д. број 4/2017-464-162 од 08.12.2017. године.

ОДБОР ДИРЕКТОРА

Наташа Млинар Лежаја, дипл.инж.саоб.

Горан Влајковић, маст.инж.маш.

Звездан Павићевић, дипл. економиста

Садржај