На основу члана 15. став 1. и члана 63. став 3. Закона о Народној банци Србије („Службени гласник РС”, бр. 72/2003, 55/2004, 85/2005 – др. закон, 44/2010, 76/2012, 106/2012, 14/2015, 40/2015 – одлука УС и 44/2018), Извршни одбор Народне банке Србије доноси

О Д Л У К А
О МИНИМАЛНИМ СТАНДАРДИМА УПРАВЉАЊА ИНФОРМАЦИОНО-КОМУНИКАЦИОНИМ СИСТЕМОМ ФИНАНСИЈСКЕ ИНСТИТУЦИЈЕ

I. УВОДНЕ ОДРЕДБЕ

1. Овом одлуком утврђују се минимални стандарди и услови стабилног и сигурног пословања који се односе на управљање информационо-комуникационим системима у банкама, друштвима за осигурање, даваоцима финансијског лизинга, друштвима за управљање добровољним пензијским фондовима, као и платним институцијама, институцијама електронског новца и јавном поштанском оператору у делу њиховог пословања који се односи на пружање платних услуга и/или издавање електронског новца (у даљем тексту: финансијска институција).

Овом одлуком уређују се и минимални стандарди за управљање континуитетом пословања и опоравак активности у случају катастрофа у финансијској институцији.

Ова одлука примењује се на све финансијске институције, осим ако појединим њеним одредбама није друкчије утврђено.

2. Поједини појмови, у смислу ове одлуке, имају следеће значење:

1) *информационо-комуникациони систем* је свеобухватни скуп технолошке инфраструктуре (хардверске и софтверске компоненте), организације, људи и поступака за прикупљање, смештање, обраду, чување, пренос, приказивање и коришћење података и информација;

2) *ресурси информационо-комуникационог система* обухватају софтверске компоненте, хардверске компоненте, мрежне компоненте и информациона добра;

3) *софтверске компоненте* обухватају све типове системског и апликативног софтвера, софтверске развојне алате, као и остали софтвер;

4) *хардверске компоненте* обухватају рачунарску опрему, комуникациону опрему, медије за чување података, као и осталу техничку опрему која служи као подршка функционисању информационог система;

5) *електронско-комуникациона мрежа* има значење утврђено законом којим се уређују електронске комуникације;

6) *информациона добра* обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште акте, процедуре и сл.;

7) *информациона технологија (ИТ)* је комбинација хардверске и софтверске имовине која омогућава аутоматизовано генерисање, прикупљање, обраду, чување, пренос, приказивање и/или коришћење информација;

8) *ИТ систем* је информациона технологија уређена као део механизма или међусобно повезане мреже која пружа подршку пословању финансијске институције;

9) *ИТ сервис* је услуга коју ИТ систем пружа унутрашњим или спољним корисницима;

10) *корисници информационо-комуникационог система* су сва лица која су овлашћена да користе информациони-комуникациони систем (запослени у финансијској институцији, запослени у другим лицима који приступају информационо-комуникационом систему финансијске институције, клијенти финансијске институције који информационом систему финансијске институције приступају преко електронских интерактивних комуникационих канала и др.);

11) *ризик информационо-комуникационог система* је могућност настанка негативних ефеката на финансијски резултат и капитал, остваривање пословних циљева, пословање у складу с прописима и репутацију финансијске институције услед неадекватног управљања информационим системом или друге слабости у том систему која негативно утиче на његову функционалност или безбедност, односно угрожава континуитет пословања финансијске институције;

12) *склоност ка преузимању ризика* (engl. risk appetite) је ниво и врсте ризика које је финансијска институција спремна да преузме у оквиру своје способности подношења ризика како би остварила своје стратешке циљеве.

13) *контроле* су политике, процедуре, праксе, технологије и организационе структуре које се односе на информационо-комуникациони систем, утврђене да би се обезбедило разумно уверење да ће пословни циљеви финансијске институције бити остварени и да ће нежељени догађаји бити спречени или откривени, а могу се разликовати према начину примене (управљачке, техничке и физичке) и намени (превентивне, детективне и корективне);

14) *управљачке контроле* обухватају доношење и примену политика, стандарда, планова, процедура и других унутрашњих аката, као

и успостављање одговарајуће организационе структуре, а ради постизања и одржавања адекватног нивоа функционалности и безбедности информационо-комуникационог система;

15) *техничке контроле* су контроле примењене у хардверским и софтверским компонентама информационо-комуникационог система;

16) *физичке контроле* су контроле којима се ресурси информационо-комуникационог система штите од неовлашћеног физичког приступа, крађе, физичког оштећења или уништења;

17) *превентивне контроле* су контроле намењене спречавању настанка проблема и инцидената;

18) *детективне контроле* су контроле намењене откривању и препознавању проблема и инцидената и указивању на настале проблеме и инциденте;

19) *корективне контроле* су контроле намењене ограничавању и отклањању проблема и последица инцидената;

20) *инцидент* је сваки непланирани и нежељени догађај који може нарушити безбедност или функционалност информационо-комуникационог система;

21) *ИКТ инцидент* је догађај или низ повезаних догађаја које финансијска институција није планирала и који угрожавају сигурност мрежних и информацијских система и негативно утичу на доступност, аутентичност, интегритет или поверљивост података, или на услуге које пружа финансијска институција.

22) *безбедност информационо-комуникациог система* подразумева очување поверљивости, интегритета, расположивости, аутентичности, доказивости, непорецивости и поузданости у информационо-комуникационом систему;

23) *оперативни или сигурносни инцидент* је један или више повезаних догађаја који нису планирани, а који су или могу имати негативан утицај на интегритет, доступност, поверљивост и/или аутентичност података или на услуге повезане с плаћањем у смислу закона којим се уређују платне услуге;

24) сајбер претња је сваки догађај или радња која може узроковати штету или поремећај мрежних и информационих система, процеса и услуга а које укључују хакерске нападе, диструбуцију злонамерног кода, неовлашћени приступ мрежама и базама података као и друге врсте напада;

25) *поверљивост* означава да подаци и информације нису откривени или доступни неовлашћеним лицима;

26) *интегритет* означава да су подаци, информације и процеси заштићени од неовлашћеног или непредвиђеног мењања, односно да евентуалне такве промене не остају неопажене;

27) *расположивост* означава да су подаци, информације и процеси доступни и употребљиви на захтев овлашћеног лица;

28) *доступност* означава да су услуге које пружа финансијска институција и услуге повезане са пружањем платних услуга клијентима у потпуности доступне и употребљиве, у складу са прихватљивим нивоима које је унапред утврдила финасијска институција;

29) *аутентичност* означава да је идентитет лица заиста онај за који се тврди да јесте;

30) *доказивост* означава да свака активност у информационо-комуникационом систему може бити једнозначно праћена до њеног извора;

31) *непорецивост* означава немогућност порицања активности извршене у информационо-комуникационом систему или пријема информације;

32) *поузданост* означава да информациони-комуникациони систем доследно и очекивано врши предвиђене функције и пружа тачне информације;

33) *ауторизација* је процес доделе права приступа корисницима информационо-комуникационог система;

34) *идентификација* је процес представљања корисника информационо-комуникационог система приликом пријаве и у току извођења активности у том систему;

35) *аутентификација* је процес провере и потврде корисничког идентитета коришћењем једног од следећих елемената или њихове комбинације:

– нешто што само корисник зна (нпр. лозинка, лични идентификациони број и сл.),

– нешто што само корисник поседује (нпр. магнетна картица, чип картица, токен, криптографски кључ и сл.),

– нешто што само корисник јесте (биометријске карактеристике као што су отисак прста, очна дужица, глас, рукопис и сл.);

36) *повлашћени приступ информационо-комуникацоином систему* је приступ ресурсима информационо-комуникационог система који овлашћеним корисницима (администратори системског софтвера, администратори мреже, администратори база података и сл.) омогућава заобилажење техничких контрола;

37) *удаљени приступ информационо-комуникационом систему* је приступ ресурсима информационо-комуникационог система са удаљене локације посредством телекомуникационе инфраструктуре над којом финансијска институција нема потпуну контролу;

38) *оперативни и системски записи* означавају хронолошке записе о догађајима и активностима на ресурсима информационо-комуникационог система (записи оперативних система, апликативног софтвера, база података, мрежних уређаја и сл.);

39) *малициозни програмски кôд* је било који облик програмског кôда створен с намером да се неовлашћено оствари приступ ресурсима информационо-комуникационог система, прикупе информације, изазове

неочекивано понашање или прекид у функционисању овог система, односно да се на други начин потенцијално наруши поверљивост, интегритет или расположивост тих ресурса (нпр. рачунарски вируси, црви, тројански коњи и др.);

40) *критични/кључни пословни процеси* су пословни процеси или функције чије неадекватно функционисање може значајније угрозити пословање финансијске институције;

41) *најдужи прихватљив прекид* (*MAO – Maximum Acceptable Outage*) означава најдужи прихватљив период нерасположивости пословног процеса, односно критично време за опоравак тог процеса;

42) *циљни ниво активности* (*SDO – Service Delivery Objective*) означава одговарајући ниво опоравка пословног процеса који треба да буде постигнут током циљног времена опоравка;

43) *циљно време опоравка* (*RTO – Recovery Time Objective*) означава период, односно фазе у том периоду током којих треба да буде постигнут одговарајући ниво опоравка пословног процеса;

44) *циљна тачка опоравка (RPO – Recovery Point Objective*) означава најдужи прихватљив период од последње резервне копије података до наступања нерасположивости пословног процеса, односно најдужи прихватљив период за који подаци могу бити изгубљени;

45) *резервна копија података* представља копију најмање оних изворних података (софтверске компоненте и информациона добра) који су потребни за опоравак, односно за поновно успостављање пословних процеса;

II. ОКВИР ЗА УПРАВЉАЊЕ ИНФОРМАЦИОНО-КОМУНИКАЦИОНИМ СИСТЕМОМ

3. Финансијска институција је дужна да, у складу с природом, обимом и сложеношћу пословања, успостави адекватан информационо-комуникациони систем, који испуњава најмање следеће услове:

1) поседује функционалности, капацитете и перформансе који омогућавају пружање одговарајуће подршке пословним процесима;

2) обезбеђује благовремене, тачне и потпуне информације значајне за доношење пословних одлука, ефикасно обављање пословних активности и управљање ризицима, односно за сигурно и стабилно пословање финансијске институције;

3) пројектован је са одговарајућим контролама за валидацију података на улазу, у току процеса обраде, као и на излазу из тог система, ради спречавања нетачности и неконзистентности у подацима и информацијама.

Финансијска институција је дужна да обезбеди да сви пословно значајни системи за обраду података, као и систем извештавања, буду интегрални део информационо-комуникационог система.

4. Финансијска институција је дужна да, у складу с природом, обимом и сложеношћу пословања, као и сложеношћу информационо-комуникационог система, успостави, надзире, редовно ревидира и унапређује процес управљања овим системом ради смањења изложености ризицима и очувања безбедности и функционалности тог система, као и да унутрашњим општим актом, у складу са законом, утврди овлашћења и одговорности својих органа управљања и надзора који се односе на ове послове.

5. Финансијска институција је дужна да, у складу са стратегијом пословања, као и с природом, обимом и сложеношћу пословања, донесе стратегију развоја информационо-комуникационог система, за временски период који није краћи од три године.

Стратегијом развоја информационо-комуникационог система дефинишу се:

1) начин на који треба да се развија информационо-комуникациони систем како би ефикасно обезбедио подршку и учешће у стратегији пословања, укључујући развој његове организационе структуре, промене у том систему као и кључне зависности од трећих лица;

2) развој архитектуре информационо-комуникационог система, која укључује зависност од трећих лица;

3) јасни циљеви безбедности информационо-комуникационог система.

У складу са стратегијом развоја информационо-комуникационог система, финансијска институција дужна је да донесе одговарајуће стратегијске и оперативне планове, који садрже мере за реализацију циљева дефинисаних у стратегији информационо-комуникационог система. Оперативни план активности треба, као минимум, да садржи опис активности и пројеката из тачке 8. ове одлуке, извођаче, одговорна лица, буџет и рокове за извршење планираних активности.

Финансијска институција је дужна да, успостави процес редовног преиспитивања спровођења стратегије из става 1. ове тачке и по потреби, мења ту стратегију ако то захтевају одговарајуће измене и/или допуне стратегије пословања.

Финансијска институција је дужна да обезбеди финансијска средства довољна за спровођење стратегије из става 1. ове тачке.

Финансијска институција је дужна да о свакој измени и/или допуни стратегије развоја информационо-комуникационог система обавести Народну банку Србије у року од 15 дана од дана њеног усвајања.

6. Финансијска институција је дужна да, ради адекватног управљања информационо-комуникационим системом, обезбеди одговарајућу организациону структуру, с јасно утврђеном поделом послова и дужности запослених, односно са утврђеним унутрашњим контролама којима се спречава сукоб интереса.

Финансијска институција је у оквиру организационе структуреиз става 1. ове тачке нарочито дужна да јасно утврди послове и дужности запослених који су у непосредној вези са ефикасним и одговарајућим управљањем безбедношћу информационо-комуникационог система.

7. Финансијска институција је дужна да обезбеди примену свих унутрашњих општих аката и процедура у вези са информационо-комуникационим системом, као и да обезбеди да сви корисници овог система буду упознати са садржајем тих аката и процедура, у складу с њиховим овлашћењима, одговорностима и потребама.

8. Финансијска институција доноси методологију којом утврђује критеријуме, начин и поступке управљања пројектима информационо комуникационих система Пројекат информационо комуникационих система је сваки пројекат или његов део у којем се ови системи или сервиси успостављају, мењају, замењују, стављају ван употребе или имплементирају и може бити део ширих пројектних програма или пројектних програма трансформације пословања;

9. Финансијска институција је дужна да утврди критеријуме, начин и поступке извештавања свог надлежног органа о релевантним чињеницама у вези с функционалношћу и безбедношћу информационог система.

III. УПРАВЉАЊЕ РИЗИКОМ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА

10. Одредбе прописа којима се уређују општи услови и начин управљања ризицима у пословању финансијских институција примењују се и на управљање ризиком информационо-комуникационог система, осим ако овом одлуком није друкчије уређено.

11. Финансијска институција је дужна да, у оквиру свеобухватног система управљања ризицима, успостави процес управљања ризиком информационо-комуникационог система који обухвата идентификовање и

мерење, односно процену тог ризика, као и његово ублажавање, праћење и контролу.

Финансијска институција је дужна да, у складу са с природом, обимом и сложеношћу пословања, обезбеди независност и објективност организационог дела и/или лица која су непосредно одговорна за праћење и контролу ризика из става 1. ове тачке, односно организационог дела и/или лица која не обављају оперативне послове у којима настаје ризик информационо-комуникационог система а нарочито не учествују и не обављају послове и активности за које је задужен организациони део за ИТ операције.

Финансијска институција је дужна да унутрашњим општим актима уреди начин, динамику и достављање извештаја надлежним органима о ризицима у информационо-комуникационом систему, на такав начин да организациони део и/или лица из става 2. ове тачке извештава о изложености финансијске институције ризицима у информационо-комуникационом систему, као и о свим редовним и ванредним активностима везаним за управљање тим ризицима.

12. Финансијска институција је дужна да ризиком информационо-комуникационог система управља тако да омогући несметано управљање безбедношћу овог система и управљање континуитетом пословања финансијске институције.

Управљање ризиком информационо-комуникационог система мора да обухвати целокупан информациони систем финансијске институције и да буде интегрисано у све фазе развоја тог система.

Финансијска институција је дужна да у унутрашњим општим актима утврди правила за управљање ризицима информационо-комуникационог система која посебно садрже:

– склоност ка преузимању ризика у информационо-комуникационом систему;
– методе и параметре за процену ризика информационо-комуникационог система на основу којих се идентификује и мери тај ризик (нпр. претња, рањивост, вероватноћа, утицај и сл.);
– поступке за дефинисање мера за контролисање ризика информационо-комуникационог система, укључујући увођење нових и/или модификацију постојећих контрола у циљу ублажавања тог ризика и предузимања радњи за прилагођавање тих мера када је то потребно;
– поступке за праћења реализације и ефикасности примењених мера за контролисање ризика информационо-комуникационог система,

– поступке праћења броја утврђених оперативних или безбедносних инцидената, укључујући и инциденте који су пријављени Народној банци Србије,;

– обавезу да се, пре доношења одлуке о спровођењу промена у информационо-комуникационом систему, идентификују и мере, односно процењују ризици релевантног дела информационо-комуникационог система који произлазе из било каквих већих промена у том систему, услугама и/или процесу управљања тим системом;

– обавезу идентификације, мерења, односно процене ризика релевантног дела информационо-комуникационог система након сваког значајнијег оперативног или безбедносног инцидента;

– временски оквир за спровођење редовног, свеобухватног утврђивања и процене ризика информационо-комуникационог система, а најмање једном годишње;

– овлашћења и одговорности органа и запослених у финансијској институцији за управљање ризицима информационо-комуникационог система за све нивое пословног процеса и одлучивања, на начин којим се спречава сукоб интереса.

Финансијска институција приликом вршења процене ризика информационо-комуникационог система узима у обзир класификацију информационих добара из тачке 24. став 1. Одлуке, односно узима у обзир осетљивост и критичност тих добара.

13. Финансијска институција је дужна да, на основу резултата процене ризика информационо-комуникационог система, у складу са склоношћу ка преузимању тог ризика, утврди које је мере потребно применити како би се ови ризици свели на прихватљив ниво, и по потреби изврши промене постојећих пословних процеса, контролних мера, ИТ система и/или ИТ сервиса.

Финансијска институција процењује време потребно за спровођење измена из става 1. ове тачке и, у складу са склоношћу преузимања ризика информационо-комуникационог система, по потреби, дефинише привремене мере за смањење тог ризика које ће се примењивати до спровођења планираних измена.

14. Пружалац платних услуга у смислу закона којим се уређују платне услуге, дужан је да резултате свеобухватне процене ризика информационо-комуникационог система као и оперативних и сигурносних ризика повезаних са платним услугама достави Народној банци Србије једном годишње или након значајних промена или инцидената у информационо-комуникационом систему.

15. Финансијска институција је дужна да адекватно управља ризицима који произлазе из уговорних односа с правним и физичким лицима чије се активности односе на њен информационо-комуникациони систем.

Финансијска институција је дужна да континуирано надзире начин и квалитет уговорених активности из става 1. ове тачке.

IV. УНУТРАШЊА РЕВИЗИЈА ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА

16. Финансијска институција је дужна да, у складу с природом, обимом и сложеношћу пословања, као и сложеношћу информационо-комуникационог система, методологијом рада унутрашње ревизије обухвати критеријуме, начин и поступке унутрашње ревизије тог система засноване на резултатима процене ризика.

Финансијска институција је дужна да обезбеди да ревизију из става 1. ове тачке изврши ревизор који има знање и искуство у области у вези ризика информационо-комуникационог система. Учесталост и предмет ревизије из става 1. ове тачке треба да буду сразмерни процењеним ризицима информационо-комуникационог система којима је финансијска институција изложена.

Финансијска институција је дужна да успостави процес праћења спровођења мера за отклањање неправилности, слабости и недостатака утврђених ревизијом из става 1. ове тачке.

17. Унутрашња ревизија информационо-комуникационог система обавља се у складу с прописима којима се уређује пословање финансијских институција.

V. БЕЗБЕДНОСТ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА

18. Финансијска институција је дужна да, у складу са сложеношћу информационо-комуникационог система, донесе унутрашњи општи акт којим ће се успоставити оквир за управљање безбедношћу тог система (у даљем тексту: политика безбедности информационог система).

Политиком безбедности информационо-комуникационог система нарочито се уређују принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности овог система, као и овлашћења и одговорности у вези са овом безбедношћу и ресурсима тог система.

Финансијска институција је дужна да политику безбедности информационо-комуникационог система усклађује с променама у

окружењу и у самом информационо-комуникационом систему, као и у случајевима нарушавања безбедности и процене ризика тог система.

Финансијска институција је дужна да политиком безбедности обезбеди поверљивост, интегритет и доступност логичких и физичких ресурса информационо-комуникационог система у складу са њиховом критичношћу, као и осетљивошћу података, независно од тога да ли се налазе у стању мировања, преноса или у употреби.

19. Финансијска институција је дужна да процес управљања безбедношћу информационо-комуникационог система успостави као континуирани процес идентификовања потреба за овом безбедношћу и постизања и одржавања адекватног нивоа те безбедности

Финансијска институција је дужна да у вези процеса из става 1. ове тачке успостави систем за откривање догађаја који могу утицати на безбедност информационо-комуникационог система, као и да на одговарајући начин одговори на те догађаје.

У оквиру процеса из става 1. ове тачке, финансијска институција је дужна да имплементира ефикасне контроле за откривање физичких и логичких упада и нарушавања поверљивости, интегритета и доступности информација, као и контроле за откривање догађаја као што су нежељени одлив информација, присуство малициозног софтвера и коришћење софтвера који садржи техничке рањивости.

20. Финансијска институција је дужна да, у складу с природом, обимом и сложеношћу пословања, као и сложеношћу информационо-комуникационог система:

1) поделу послова у вези са безбедношћу тог система изврши тако да се у унутрашњим актима којима се уређује организација њеног пословања јасно могу утврдити послови и дужности запослених у вези с том безбедношћу;

2) одреди кључне запослене задужене за безбедност информационо-комуникационог система водећи рачуна о томе да њихова позиција има значајан утицај на активности и доношење одлука у вези с том безбедношћу;

3) у управљање безбедношћу информационо-комуникационог система укључи довољан број запослених који имају одговарајућу стручност и професионално искуство.

Лица из става 1. ове тачке су дужна да континуирано прате безбедносне и оперативне претње које би могле значајно да утичу на способност финансијске институције да пружа услуге, и да прате развој

технологија и трендова у безбедности информационо-комуникационог система како би били свесни потенцијалних безбедносних ризика.

Лица из става 1. ове тачке су дужна да благовремено извештавају надлежне органе финансијске институције о редовним и ванредним активностима спроведеним у циљу праћења информационе безбедности, а нарочито о откривеним догађајима који су утицали или могу утицати на информациону безбедност финансијске институције.

21. Финансијска институција је дужна да идентификује и прати потребе за безбедношћу информационо-комуникационог система, и то најмање на основу резултата процене ризика тог система и обавеза које произлазе из прописа, унутрашњих општих аката, уговорних односа и сл.

22. Финансијска институција је дужна да, ради постизања и одржавања адекватног нивоа безбедности информационо-комуникационог система, успостави одговарајуће контроле.

Финансијска институција је дужна да континуирано прати промене у постојећем оперативном окружењу, процењује њихов утицај на ефикасност постојећих мера безбедности, и по потреби уводи додатне мере за ублажавање ризика информационо-комуникационог система.

23. Финансијска институција је дужна, да у складу с природом, обимом и сложеношћу пословања, као и сложеношћу информационо-комуникационог система, унутрашњим општим актима уреди начин тестирања безбедности тог система како би се утврдила поузданост и ефикасност успостављених мера безбедности.

Финансијска институција је дужна, да у складу с природом, обимом и сложеношћу пословања, као и сложеношћу информационо-комуникационог система тестирање из става 1. ове тачке изводи у складу са проценом нивоа ризика безбедности информационо-комуникационог система (нпр. пенетрационо тестирање, скенирање рањивости, тестирање безбедности мреже и апликација и др), и да обезбеди да та тестирања спроводе лица која поседују довољно знања, вештина и искуства у вези са тим тестирањем.

Финансијска институција је дужна, да у складу с природом, обимом и сложеношћу пословања, и сложеношћу информационо-комуникационог система као и у складу са процењеним ризицима периодично понавља тестирање из става 1. ове тачке.

Пружалац платних услуга у смислу закона којим се уређују платне услуге, је дужан да најмање једном годишње врши тестирања из става 1.

ове тачке за све критичне ресурсе информационо-комуникационог система, односно најмање једном у три године за ресурсе који се не сматрају критичним.

Финансијска институција је дужна да у случају промена на ресурсима информационо-комуникационог система, значајним процесима и процедурама, увођења нових или значајних промена постојећих критичних апликација доступних на интернету као и након значајних оперативних или безбедносних инцидената врши одговарајућа ванредна тестирања безбедности информационо-комуникационог система.

Финансијска институција је дужна да у складу са резултатима спроведених тестирања из става 1. ове тачке прилагоди мере безбедности информационо-комуникационог система, а у случају критичних ресурса информационо-комуникационог система да то уради без одлагања.

24. Финансијска институција је дужна да унутрашњим општим актима утврди ближе критеријуме, начин и поступке за класификацију информационих добара према степену осетљивости и критичности – с обзиром на могуће последице нарушавања њихове поверљивости, интегритета и расположивости, да доследно примењује ту класификацију, као и да у складу с тим обезбеди адекватан ниво заштите ових добара.

Финансијска институција је дужна да именује лице, односно лица запослена у тој институцији која ће бити одговорна за управљање информационим добрима, те за класификацију и заштиту ових добара.

25. Финансијска институција је дужна да спроводи одговарајућу контролу приступа ресурсима информационо-комуникационог система, као и да с тим у вези успостави адекватан систем управљања корисничким правима приступа.

Системом управљања корисничким правима приступа нарочито се обухватају процеси евидентирања корисника информационо-комуникационог система, ауторизације, идентификације и аутентификације, као и надзор над корисничким правима приступа.

Финансијска институција је дужна да обезбеди да ауторизација корисника информационо-комуникационог система буде заснована на принципу:

– неопходности приступа информацијама (енгл. *need to know),* укључујући и приступ информацијама*;*

– доделе најмањих могућих права приступа ресурсима тог система која омогућују ефикасно обављање послова;

– адекватне сегрегације дужности, односно да корисницима није додељена комбинација права приступа која им омогућава заобилажење контрола;

– да су корисницима информационо-комуникационог система, где је то могуће, додељени персонализовани кориснички налози по којима их је лако идентификовати, и да један налог користи само један корисник како би се активности које се спроводе у том систему могле јасно повезати са тим корисником и како би могла да се утврди одговорност;

– да је коришћење привилегованог приступа строго контролисано тако што се ограничавају и пажљиво прате активности налога са повишеним правима приступа (као што су налози администратора система), и да се привилеговани удаљени приступ одобрава само на основу принципа неопходности приступа информацијама уз употребу решења за поуздану аутентификацију (као што је провера која се заснива на коришћењу два фактора);

– да се активности корисника, а нарочито све активности привилегованих корисничких налога, евидентирају у системским и оперативним записима и да се ти записи израђују, прате и чувају у складу са утврђеном критичношћу ресурса информационо-комуникационог система из тачке 24. став 1. одлуке, у сврху благовременог откривања неовлашћених приступа и радњи на информационо-комуникационом систему.

Финансијска институција је дужна да периодично и по потреби, а најмање једном годишње, ревидира корисничка права приступа како би се осигурало да корисници тих права не поседују претеране привилегије и да се оне повуку када више нису потребне.

При управљању корисничким правима приступа, финансијска институција је дужна да посебно уреди повлашћени и удаљени приступ информационо-комуникационом систему.

26. Финансијска институција је дужна да, на основу резултата процене ризика информационо-комуникационог система, успостави адекватан систем надгледања тог система и генерисања оперативних и системских записа.

Финансијска институција је дужна да обезбеди одговарајућу заштиту записа из става 1. ове тачке, као и да утврди време чувања, те учесталост, опсег и начин праћења тих записа.

Записи из става 1. ове тачке морају садржати довољну количину информација ради идентификовања проблема, реконструисања догађаја

и откривања неовлашћених приступа и активности на ресурсима информационог система, као и ради утврђивања одговорности.

27. Финансијска институција је дужна да унутрашњим општим актима дефинише и примени одговарајуће контроле физичке безбедности ресурса информационо-комуникационог система и других система који су подршка функционисању тог система у циљу заштите просторија, рачунарских центара и осетљивих подручја од неовлашћеног физичког приступа, од крађе, као и од физичког оштећења или уништења изазваног људским или природним фактором (статички електрицитет, висока температура, пожар, поплава, итд).

Финансијска институција је дужна да обезбеди да се прати физички приступ информационо-комуникационом систему као и да омогући приступ само овлашћеним лицима, а у складу са њиховим задацима и задужењима. Физичка права приступа се редовно преиспитују како би се, без одлагања, обезбедило повлачење тих права када за њима престане потреба.

28. Финансијска институција је дужна да, применом одговарајућих контрола, ресурсе информационо-комуникационог система заштити од малициозног програмског кôда.

VI. УПРАВЉАЊЕ КОНТИНУИТЕТОМ ПОСЛОВАЊА И ОПОРАВАК АКТИВНОСТИ У СЛУЧАЈУ КАТАСТРОФА

29. Финансијска институција је дужна да, ради обезбеђивања несметаног и континуираног функционисања свих својих значајних система и процеса, као и ограничавања губитака у ванредним ситуацијама, успостави процес управљања континуитетом пословања.

30. Финансијска институција је дужна да обезбеди да управљање континуитетом пословања буде засновано на анализи утицаја на пословање и на процени ризика, које нарочито обухватају:

1) утврђивање ресурса и система потребних за одвијање појединачних пословних процеса, као и њихове међузависности и повезаности;

2) процену ризика у вези с појединачним пословним процесима, укључујући и вероватноћу настанка нежељених догађаја и њихов потенцијални утицај на континуитет пословања, финансијско стање и репутацију финансијске институције;

3) утврђивање прихватљивих нивоа ризика и техника за ублажавање идентификованих ризика;

4) утврђивање најдужег прихватљивог прекида (*MAO*) појединачних пословних процеса;

5) утврђивање критичних/кључних пословних процеса и активности.

Финансијска институција је дужна да, у складу са спроведеним активностима из става 1. ове тачке, усвоји стратегију опоравка коју ће применити у случају прекида пословања, а која нарочито садржи:

1) приоритете опоравка пословних процеса, као и ресурса и система потребних за њихово одвијање;
2) циљне нивое активности (*SDO*);
3) циљна времена опоравка (*RTO*);
4) циљне тачке опоравка (*RPO*).

Финансијска институција је дужна да обезбеди да информационо-комуникациони систем и услуге које пружа уз помоћ тог система буду у складу са анализом утицаја на пословање, и с тим у вези успостави редундантност одређених критичних компоненти тог система како би се спречили прекиди изазвани догађајима који утичу на те компоненте.

31. Управни одбор банке и даваоца финансијског лизинга, односно надлежни орган друштва за осигурање, друштва за управљање добровољним пензијским фондом, платне институције, институције електронског новца и јавног поштанског оператора дужан је да, на основу активности спроведених у складу с тачком 30. ове одлуке, донесе план континуитета пословања (Business Continuity Plan), као и план опоравка активности у случају катастрофа (Disaster Recovery Plan) којим се превасходно уређује стварање услова за опоравак и расположивост ресурса информационо-комуникационог система потребних за одвијање критичних/кључних пословних процеса.

План континуитета пословања нарочито садржи:

1) опис процедура у случају прекида пословања;
2) ажуран списак свих ресурса неопходних за поновно успостављање континуитета пословања;
3) списак приоритета по којима ће се поступити у случају да је потребно опоравити више пословних активности;
4) податке о тимовима који ће бити одговорни за поновно успостављање пословања у случају настанка непредвиђених догађаја и о именованим члановима тих тимова, укључујући и њихове јасно утврђене дужности и одговорности, као и план унутрашњих и спољних линија комуникације;

5) резервну локацију – у случају прекида пословања и немогућности поновног успостављања пословних процеса на примарној локацији.

План опоравка активности у случају катастрофа нарочито садржи:

1) процедуре за опоравак информационо-комуникационог система кад наступе катастрофални догађаји;
2) услови који морају бити испуњени за примену плана опоравка активности
3) приоритете опоравка ресурса информационо-комуникационог система;
4) податке о тимовима који ће бити одговорни за опоравак информационо-комуникационог система и о именованим члановима тих тимова, укључујући и њихове јасно утврђене дужности и одговорности;
5) податке о кључним пружаоцима услуга;
6) податке о резервним локацијама за опоравак информационо-комуникационог система, односно локације резервних рачунарских центара.

Финансијска институција је дужна да, ради ефикасног спровођења планова из става 1. ове тачке, обезбеди да сви запослени буду упознати са својим улогама и одговорностима у случају наступања ванредних ситуација.

Финансијска институција је дужна да предузима све неопходне активности ради усклађивања планова из става 1. ове тачке с пословним променама, укључујући и промене у производима, активностима, процесима и системима, с променама у окружењу, с пословном политиком и стратегијом пословања као и са искуством из претходних инцидената и новим идентификованим ризицима и претњама.

Финансијска институција је дужна да, периодично и после настанка значајних промена, а најмање једном годишње, тестира планове из става 1. ове тачке, као и да документује резултате тих тестирања и обезбеди њихово укључивање у извештавање надлежног органа финансијске институције.

Финансијска институција је дужна да, тестирањем из става 6. ове тачке утврди да ли може успешно прећи на алтернативни начин обављања критичних пословних активности из окружења предвиђеног за опоравак од катастрофе, и да ли може такав режим рада одржати довољно дуг временски период и након тога поново успоставити редовно пословање и стабилан рад информационо-комуникационог система.

За спровођење планова из става 1. ове тачке, као и одредаба ст. од 4. до 7. те тачке, одговоран је извршни одбор банке и даваоца финансијског лизинга, односно надлежни орган друштва за осигурање, друштва за управљање добровољним пензијским фондом, платне институције, институције електронског новца и јавног поштанског оператора који, у складу са законом, води послове друштва.

32. Финансијска институција је дужна да, при управљању континуитетом пословања, узме у обзир и активности поверене трећим лицима и зависност од услуга тих лица.

33. Финансијска институција је дужна да, у случају настанка околности које захтевају примену плана континуитета пословања и плана опоравка активности у случају катастрофа, обавести о томе Народну банку Србије, и то најкасније наредног дана од дана настанка тих околности. Народна банка Србије може захтевати додатну документацију у вези с релевантним чињеницама о овим околностима и одредити рок за достављање те документације.

Финансијска институција је дужна да, у случају настанка околности које захтевају примену плана континуитета пословања и плана опоравка активности у случају катастрофа о томе информише све релевантне интерне и спољне актере и одржава комуникацију са њима.

34. Финансијска институција је дужна да успостави процес управљања резервним копијама података, те да у ту сврху утврди детаљне процедуре и одговорности.

Процедуре из става 1. ове тачке треба да садрже врсту, обим, начин и учесталост израде резервних копија података, начин тестирања и начин и учесталост одлагања на удаљену локацију, период чувања резервних копија података, као и начин вођења евиденције о њима.

Управљање резервним копијама података мора да обухвати поступке израде, чувања и тестирања ових копија, као и опоравка података и софтверских компонената, како би се омогућило поновно успостављање пословних процеса у оквиру циљног времена опоравка.

Финансијска институција је дужна да обезбеди да су резервне копије података ажурне и адекватно заштићене, а поступци опоравка тестирани и успешни.

Најмање једна ажурна и комплетна резервна копија података мора бити адекватно ускладиштена на одговарајућој удаљености од примарне локације – на основу резултата процене ризика информационо-

комуникационог система и уз узимање у обзир потребе за избегавањем утицаја истих ризика на обе локације.

35. Финансијска институција је дужна да, на основу активности спроведених у складу с тачком 30. ове одлуке, обезбеди расположивост резервног рачунарског центра и његову адекватну опремљеност, функционалност и ниво безбедности, као и његову одговарајућу удаљеност од примарног рачунарског центра, уз узимање у обзир потребе за избегавањем утицаја истих ризика на обе локације.

VII. УПРАВЉАЊЕ ИКТ ИНЦИДЕНТИМА И ИЗВЕШТАВАЊЕ О ИКТ ИНЦИДЕНТИМА

36. Финансијска институција је дужна да успостави и спроводи процес управљања ИКТ инцидентима који омогућава благовремен и ефикасан одговор у случају нарушавања безбедности или функционалности ресурса информационо-комуникационог система.

37. Финансијска институција је дужна да унутрашњим општим актима утврди начин класификације значајних ИКТ инцидента, начин на који о тим инцидентима обавештава Народну банку Србије и критеријуме на основу којих процењује значај.

38. Финансијска институција је дужна да у значајне ИКТ инциденте укључи и инциденте који су настали код лица повезаних с финансијском институцијом имовинским и/или управљачким односима (лица са учешћем, чланице групе друштава којој та институција припада и др.) која послују у Републици Србији или у иностранству, као и инциденте настале код пружаоца услуга којима је финансијска институција поверила активности а који утичу на услуге које пружа финансијска институција и то:

1) директно, када услугу повезану са пружањем услуга пружа повезано лице или пружалац услуга који је захваћен инцидентом или
2) индиректно, када је, способност финансијске институције да настави да пружа услуге угрожена на други начин због инцидента код повезаног лица или пружаоца услуга.

39. Финансијска институција је дужна да успостави одговарајуће поступке и процесе за доследно и свеобухватно праћење, поступање и предузимање адекватних мера са ИКТ инцидентима, како би се осигурало утврђивање и документовање основних узрока (енг. Root cause) тих инцидената, у циљу спречавања појаве истог инцидента.

40. Финансијска институција је дужна да, у складу са природом, обимом и сложеношћу пословања у оквиру процеса управљања ИКТ инцидентима из тачке 36. ове одлуке:

1) успостави показатеље за рано упозоравање (енг. early warning indicators);

2) успостави поступке за утврђивање, праћење, евидентирање, категоризацију и класификацију ИКТ инцидената према њиховим приоритету и озбиљности и према критичности захваћених услуга, у складу с критеријима утврђеним у тачки 42. став 1. одлуке;

3) додели улоге и одговорности за различите типове и сценарије ИКТ инцидената;

4) утврди планове за комуникацију који обухватају запослене у финансијској институцији, лица повезана са финансијском институцијом (заинтересоване стране), јавност и медије у зависности од природе ИКТ инцидента;

5) утврди планове за обавештавање клијената у складу са поступком ескалације инцидента, што укључује приговоре корисника повезане са информационо-комуникационом системом;

6) осигура извештавање и информисање свог надлежног органа о значајним ИКТ инцидентима, последицама тих инцидената, одговора на њих као и додатних контрола које треба увести у циљу спречавања понављања истих;

7) успостави поступке одговора на ИКТ инциденте како би се ублажиле последице и обезбедило да услуге правовремено постану доступне и безбедне.

41. Финансијска институција је дужна да класификује као значајне оне ИКТ инциденте за које проценом из тачке 42. ове одлуке утврди да испуњавају:

1) један или више критеријума већег нивоа утицаја; или

2) три или више критеријума мањег нивоа утицаја.

Критеријуми већег и мањег нивоа утицаја из става 1. ове тачке дати су у Прилогу 1 који чини саставни део ове одлуке.

Финансијска институција је дужна да класификацију из става 1. ове тачке спроведе благовремено, а најкасније 24 сата од тренутка откривања инцидента и без непотребног одлагања након што информације потребне за класификацију инцидента постану доступне.

Изузетно од става 3. ове тачке, ако је финансијској институцији потребно више од 24 сата за класификацију одређеног инцидента од његовог откривања, дужна је да Народној банци Србије достави обавештење (почетни извештај) о насталом инциденту у складу са тачком. 44. став 1. ове одлуке.

42. Финансијска институција је дужна да спроводи процене ИКТ инцидената на основу следећих критеријума и њихових основних индикатора:

1) трансакције или услуге захваћене инцидентом – финансијска институција утврђује укупну вредност трансакција које су захваћене инцидентом, као и процентуални удео компромитованих трансакција у редовном обиму пословања;

2) укупан број клијената, корисника услуга захваћени инцидентом – финансијска институција утврђује укупан број корисника који су обухваћени инцидентом и њихов процентуални удео у укупном броју корисника финансијске институције, при том узимајући у обзир поред броја клијената и њихов значај и, ако је то примењиво, број трансакција захваћених тим инцидентом. Број клијената односи се на број свих захваћених клијената, без обзира на то да ли су физичка или правне лица, која не могу или нису могла користити услугу коју финансијска институција пружа током инцидента или на које је инцидент негативно утицао.

3) нарушавање сигурности мреже или информационо-комуникационог система – финансијска институција утврђује да ли је злонамерна активност угрозила сигурност мреже или информационо-комуникационог система, повезаних са пружањем услуга;

4) дужина прекида пружања услуге – финансијска институција утврђује временски период у којем ће услуга вероватно бити недоступна клијенту или кориснику услуга или током којег пружалац платних услуга неће моћи да изврши налог за плаћање, при том узимајући у обзир дужину трајања ИКТ инцидента, време прекида рада ИКТ система или његовог дела или застоја у раду или застоја/прекида пружања услуге. Дужина прекида се мери од тренутка његова настанка, односно од тренутка његовог откривања до тренутка његовог решавања.

5) економски утицај – финансијска институција свеобухватно утврђује трошкове повезане са ИКТ инцидентом и узима у обзир његов апсолутни износ и, када је применљиво, релативни значај тих трошкова у односу на величину финансијске институције, односно на њен основни капитал, ово се односи на директне и индиректне трошкове и губитке. Финансијска институција нарочито узима у обзир одузета новчана средства или ресурсе, трошкове замене хардверских или софтверских компоненти, остале трошкове за спровођење форензичких и корективних радњи, трошкове правне заштите и накнаде клијентима, накнаде због неиспуњавања уговорних обавеза, казне, друге обавезе и пропуштене приходе.

6) висок ниво интерне ескалације – финансијска институција утврђује да ли су чланови њених органа управљања о том инциденту обавештени или ће вероватно бити обавештени;

7) друге финансијске институције или релевантна инфраструктура потенцијално захваћени инцидентом – финансијска

институција утврђује системске последице које ће инцидент вероватно имати, односно потенцијал инцидента да се прошири са финансијске институције који је иницијално захваћен инцидентом на друге финансијске институције, инфраструктуре финансијског тржишта и/или платне шеме; Финансијска институција нарочито процењује да ли се инцидент проширио или ће се вероватно проширити на друге финансијске институције, да ли је утицао или ће вероватно утицати на несметано функционисање инфраструктура финансијског тржишта и да ли је угрозио или ће вероватно угрозити исправно функционисање финансијског система као целине.

8) репутациони утицај – финансијска институција утврђује како инцидент може нарушити поверење корисника услуга према финансијској институцији или тржишту у целини. Финансијска институција сматра да је до репутационог утицаја дошло ако је испуњен барем један од следећих критеријума: инцидент се спомињао у медијима, инцидент је довео до више притужби различитих клијената на услуге или критичне/кључне пословне односе, финансијска институција неће моћи или вероватно неће моћи испунити регулаторне захтеве због инцидента, инцидент је довео до кршења уговорних обавеза које за последицу имају објављивање информација о покретању правних радњи против финансијске институције и финансијска институција ће због инцидента изгубити или ће вероватно изгубити клијенте који имају значајан утицај на њено пословање.

Финансијска институција је дужна да поред наведених критеријума класификације ИКТ инциденте размотри и следеће:

1) географска распрострањеност инцидента у смислу подручја које је ИКТ инцидент захватио, посебно ако је захватио више од две државе у којима финансијска институција послује или поверава активности трећим лицима укључујући и лица повезана са финансијском институцијом;

2) губитак података проузрокованог ИКТ инцидентом, у смислу:

– доступности података, односно да ли су подаци због инцидента привремено или трајно недоступни или неупотребљиви,

– аутентичности податка односно да ли је угрожена поузданост извора података,

– интегритета података односно да ли су извршене неодобрене измене података због којих су они постали нетачни или непотпуни и

– поверљивости података, односно да ли су неовлашћене стране или системи приступили подацима или да су подаци откривени.

3) критичност захваћених услуга, укључујући трансакције и пословање финансијске институције, том приликом финансијска институција процењује да ли ИКТ инцидент утиче на кључне или важне

функције финансијске институције, на финансијске услуге за које је потребно одобрење, регистрација или које надзире Народна банка Србије или да ли представља или је представљао успешан, злонамеран и неовлашћен приступ мрежним и информационим системима финансијске институције.

Инциденти који се понављају, а који се појединачно не сматрају значајним инцидентом у складу са ставом 1. ове тачке сматрају се једним значајним инцидентом ако испуњавају следеће услове:

1) догодили су се најмање два пута у шест месеци;
2) имају исти очити узрок проблема (енгл.root cause);
3) заједнички испуњавају критеријуме за значајни инцидент из става 1. ове тачке

Финансијска институција је дужна да сваки месец процењује да ли постоје инциденти који се понављају.

43. Финансијска институција је дужна да спроведе процену ИКТ инцидента тако што ће за сваки критеријум из тачке 42. став 1. ове одлуке утврдити да ли су прагови нивоа утицаја из Прилога 1 ове одлуке достигнути или ће вероватно бити достигнути пре решавања тог инцидента.

Финансијска институција је дужна да ради спровођења процене из става 1. ове тачке утврди вредност индикатора из тачке 42. став 1. ове одлуке.

Ако финансијска институција нема стварне податке на основу којих може проценити праг нивоа утицаја из става 1. ове тачке достигнут или ће пре решавања ИКТ инцидента вероватно бити достигнут, ту процену може утврдити на основу процењених података, нарочито у почетној фази истраге тог инцидента.

Финансијска институција је да дужна да процену из става 1. ове тачке спроводи континуирано током трајања ИКТ инцидента, како би утврдила да ли је дошло до промене статуса тог инцидента у смислу његовог значаја.

Финансијска институција је дужна да о свакој рекласификацији ИКТ инцидента из значајног у оперативни или сигурносни инцидент који није значајан без одлагања обавести Народну банку Србије, у складу са тачком 47. ст. 7, 8. и 9. ове одлуке.

44. Финансијска институција је дужна да Народну банку Србије обавести, односно достави почетни извештај о ИКТ инциденту, у случају инцидента који је озбиљно угрозио или нарушио њено пословање, односно који би могао озбиљно угрозити или нарушити њено пословање, и то:

1) ако је настао услед нарушавања функционалности ресурса информационог система – одмах по утврђивању околности о настанку тог инцидента;

2) ако је настао као последица нарушавања безбедности информационог система – одмах по сазнању о том инциденту;

3) ако је настао код пружаоца услуге, а имао је или је могао имати значајан утицај на информационо-комуникациони систем финансијске институције или континуитет услуга које пружа – одмах по утврђивању околности о настанку тог инцидента, односно сазнању о том инциденту.

Финансијска институција је дужна да Народној банци Србије, на захтев, без одлагања достави додатну документацију којом се допуњавају информације достављене у почетном, статусном-прелазном и завршном извештају и појашњења у вези са већ достављеном документацијом.

Финансијска институција је дужна да наведе све додатне информације садржане у документацији из става 2. ове тачке достављеној Народној банци Србије, без обзира да ли је документацију доставила самоиницијативно или на захтев Народне банке Србије.

Финансијска институција је дужна да у сваком тренутку очува поверљивост и интегритет информација које размењује са Народном банком Србије и да на прикладан начин потврди свој идентитет Народној банци Србије.

Народна банка Србије ће на својој интернет страници објавити електронске обрасце (почетни, статусни – прелазни и завршни извештај), као и упутство за попуњавање тих образаца.

45. Финансијска институција је дужна да достави почетни извештај о ИКТ инциденту Народној банци Србије у складу са тачком 44. став 1. ове одлуке и одмах након што је инцидент који није био значајан рекласификован у значајан ИКТ инцидент.

Почетни извештај из става 1. ове тачке садржи матични број финансијске институције, назив финансијске институције, податке о

лицу за контакт (име, презиме, телефон и имејла адреса), датум откривања ИКТ инцидента, информацију о томе да ли је инцидент у току, последице које је инцидент изазавао и друге информације које су доступне финансијској институцији у вези са ИКТ инцидентом.

Ако финансијска институције нема све релевантне податке о инциденту у тренутку креирања почетног извештаја из става 1. ове тачке може користити податке до којих је дошла на основу процене.

Ако је финансијској институцији за класификацију одређеног инцидента потребно више времена од тренутка његовог откривања до обавештења Народне банке Србије, дужна је да у почетном извештају из става 1. ове тачке наведе разлоге за то.

Изузетно од става 1. ове тачке, ако финансијска институција није у могућности да достави почетни извештај у предвиђеном року из разлога што канали за извештавање нису доступни или функционални, дужна је да достави почетни извештај без одлагања када ти канали поново постану доступни и/или функционални, а да Народну банку Србије обавести о значајном инциденту доступним каналима комуникације.

46. Након обавештења из тачке 45. ове одлуке, финансијска институција је дужна да Народну банку Србије континуирано обавештава о битним догађајима и другим релевантним информацијама у вези са инцидентом (статус инцидента-прелазни извештај), као и о активностима предузетим ради ублажавања инцидента и његовим последицама. Ово обавештење садржи и детаљан опис инцидента, информације о процени броја корисника на које је инцидент утицао, оквирно време потребно да се инцидент реши, потенцијални утицај на друге финансијске институције, као и битне догађаје и друге релевантне информације од настанка инцидента (нпр. информације о томе да ли је инцидент ескалирао, да ли су откривени нови узроци и о ефикасности примењених активности)

Финансијска институција је дужна да достави прелазни извештај о ИКТ инциденту Народној банци Србије:

1) одмах након опоравка редовних активности и поновног успостављања редовног пословања;
2) у року од најдуже три радна дана од дана достављања почетног извештаја, ако у том периоду није дошло до поновног успостављања редовног пословања финансијске институције.

Финансијска институција је дужна да ажурира информације из почетног и статусног-прелазног извештаја да их, без одлагања, достави Народној банци Србије:

1) након достављања претходних извештаја Народној банци Србје, када настану значајне промене у вези са ИКТ инцидентом, укључујући откривање додатних узрока тог инцидента или предузимање додатних радњи за решавање проблема;

2) када ИКТ инцидент није решен у року од три радна дана од тренутка откривања;

3) на захтев Народне банке Србије.

Ако финансијска институција нема све релевантне податке о ИКТ инциденту у тренутку креирања и/или ажурирања извештаја из ст. 2. и 3. ове тачке може користити податке до којих је дошла на основу процене.

Ако је редовно пословање финансијске институције поново успостављено у оквиру четири сата од тренутка када је ИКТ инцидент класификован као значајан, финансијска институција је дужна да у истом року, заједно са почетним извештајем достави и прелазни извештај, када је то могуће.

47. Финансијска институција је дужна да достави завршни извештај о значајном ИКТ инциденту Народној банци Србије у року од 15 дана од дана престанка инцидента, односно од дана када процени да су успостављени редовно пословање финансијске институције и стабилан рад информационог система, а након што изврши анализу основног узрока тог инцидента, без обзира да ли су мере за ублажавање ризика и последица спроведене и да ли је основни узрок инцидента у потпуности идентификован, и када утврди стварне податке којима се могу заменити подаци до којих је дошао на основу процена из тачке 45. став 3. и тачке 46. став 5. ове одлуке.

Завршни извештај садржи коначне информације о инциденту – датум почетка и датум окончања инцидента, дужина трајања инцидента, врста инцидента (недоступност хардверских компоненти, проблеми у раду софтверских компоненти или безбедносни инцидент), опис инцидента, узроци настанка и последице инцидента, активности које је финансијска институција спроводила током инцидента, план активности којима ће превентивно деловати и спречити поновне појаве истог инцидента, број корисника на које је инцидент утицао, настали финансијски

трошкови повезани са инцидентом, утицај на друге финансијске институције и, по потреби, друге релевантне информације.

Изузетно од става 1. ове тачке, финансијска институција, којој је потребно продужење рока за достављање завршног извештаја дужна је да, пре истека тог рока, поднесе захтев за одлагање достављања завршног извештаја са детаљним образложењем разлога за одлагање и навођењем новог рока за његово достављање.

Финансијска институција је дужна да завршни извештај из става 1. ове тачке сачини на основу стварних података, и да на основу тих података ажурира информације које је раније доставила.

Ако је финансијска институција у могућности да Народној банци Србије достави све информације из завршног извештаја у оквиру четири сата од тренутка када је инцидент класификован као значајан, дужна је да истовремено достави почетни, прелазни и завршни извештај.

Финансијска институција је дужна да достави завршни извештај о ИКТ инциденту и када на основу континуиране процене инцидента из тачке 43. став 4. ове одлуке утврди да одређени инцидент, о којем је већ обавестила Народну банку Србије, више не испуњава критеријуме на основу којих би био класификован као значајан и да не очекује да ће их испунити пре него тај инцидент буде решен.

Финансијска институција је дужна да у случају из става 7. ове тачке, завршни извештај достави, без одлагања, након рекласификације инцидента, до истека рока за подношење следећег извештаја.

48. Финансијска институција обавештава Народну банку Србије о озбиљним сајбер претњама ако сматра да је та претња релевантна за финансијску институцију, кориснике услуга или клијенте. Народна банка Србије те информације може доставити другим релевантним телима.

49. Финансијска институција је дужна да, када настане значајан ИКТ инцидент који утиче на финансијске интересе клијената, чим постане свесна тог инцидента, без одлагања обавести своје клијенте о том инциденту и о мерама које су предузете како би се ублажио његов негативан утицај.

VIII. РАЗВОЈ И ОДРЖАВАЊЕ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА

50. Финансијска институција је дужна да успостави процес развоја информационо-комуникационог система у складу с релевантним променама унутар финансијске институције и у окружењу, како би се обезбедила континуирана адекватност тог система.

51. Финансијска институција процес развоја информационо-комуникационог система спроводи у складу са усвојеном стратегијом развоја тог система и методологијом управљања пројектима, уз узимање у обзир функционалних захтева и потреба за безбедношћу.

Финансијска институција је дужна да, током развоја информационо-комуникационог система унутар финансијске институције, успостави и документује процес тог развоја, који обухвата анализу и пројектовање, програмирање, тестирање и увођење у продукцију.

Финансијска институција је дужна да, у складу са сложеношћу информационо-комуникационог система, на одговарајући начин раздвоји продукционо окружење од других непродукционих окружења (нпр. развојног, тестног, припремног (енг. Staging) и др.).

52. Финансијска институција је дужна да успостави процес управљања хардверским и софтверским компонентама у свим фазама њиховог животног циклуса – од набавке или развоја до повлачења из употребе.

Финансијска институција је дужна да обезбеди да управљање хардверским и софтверским компонентама обухвати, између осталог, одржавање детаљне и ажурне евиденције ових компонената, именовање лица запосленог, односно запослених у финансијској институцији одговорних за управљање и заштиту тих компонената, као и утврђивање правила њиховог прихватљивог коришћења и безбедног одлагања при повлачењу из употребе.

53. Финансијска институција је дужна да обезбеди адекватно одржавање хардверских и софтверских компонената информационо-комуникационог система према препорукама произвођача и да чува записе о том одржавању, као и да се стара о томе да се притом не угрози безбедност или функционалност овог система.

Финансијска институција је дужна да успостави процес планирања и праћења перформанси и капацитета информационо-комуникационог система у циљу благовременог спречавања, откривања и отклањања

значајних проблема у раду овог система и недостатка капацитета тог система.

54. Финансијска институција је дужна да успостави процес управљања променама хардверских и софтверских компонената информационо-комуникационог система како би се избегло да оне доведу до неочекиваног и нежељеног понашања овог система, односно наруше његову безбедност или функционалност.

Управљање променама софтверских компонената информационо-комуникационог система обухвата нарочито следеће поступке:

1) утврђивање почетних верзија ових компонената;
2) иницирање, анализу и одобравање захтева за променом;
3) хронолошко документовање свих промена ових компонената и архитектуре база података, заједно с временом настанка промене;
4) информисање корисника информационо-комуникационог система о детаљима извршених промена.

Финансијска институција је дужна да обезбеди да све промене хардверских и софтверских компонената, укључујући и нове компоненте и системе, буду тестиране и одобрене пре пуштања у продукцијски рад, као и да утврди план враћања на претходно стање.

Финансијска институција је дужна да унутрашњим општим актом уреди процес управљања хитним променама хардверских и софтверских компонената информационо-комуникационог система.

55. Финансијска институција која планира миграцију података на нови систем главних пословних апликација (*core business application*) или у други рачунарски центар, односно која врши промену локације рачунарског центра, дужна је да о томе обавести Народну банку Србије најкасније 30 дана пре почетка тестирања планираног у вези с том миграцијом.

Обавештење из става 1. ове тачке нарочито садржи:

1) детаљне описе система између којих се подаци преносе;
2) план, динамику и опис активности у вези с миграцијом података, укључујући и методологију тестирања;
3) резултате процене ризика и опис контрола које ће се применити током миграције података с циљем очувања поверљивости, интегритета и расположивости података;

4) план враћања на стање пре миграције података, који укључује динамику тог враћања и опис активности, као и критеријуме за доношење одлуке за примену овог плана.

Изузетно од става 1. ове тачке, финансијска институција која планира миграцију података због статусне промене за коју је дужна да прибави сагласност, односно дозволу Народне банке Србије дужна је да, истовремено са захтевом за давање ове сагласности, односно дозволе, Народној банци Србије достави и обавештење с подацима из става 2. те тачке, а банка је дужна да достави и захтев за омогућавање функционисања привременог рачуна правног следбеника (у даљем тексту: захтев за привремени рачун) који мора потписати законски заступник правног следбеника – ради поступања Народне банке Србије по том захтеву у случајевима утврђеним овом тачком.

Привремени рачун правног следбеника представља рачун банке која престаје да постоји због статусне промене који је отворен у Народној банци Србије у складу с прописима, односно правилима рада платног система у којем та банка учествује а који због статусне промене преузима правни следбеник, ради његовог привременог функционисања у року утврђеном овом одлуком.

Финансијска институција која донесе одлуку о примени плана враћања на стање пре миграције података дужна је да о томе без одлагања обавести Народну банку Србије.

Ако донесе одлуку о примени плана враћања на стање пре миграције података због статусне промене, банка је дужна да о томе обавести Народну банку Србије најкасније наредног радног дана од дана када је започела миграцију података, и то најкасније један сат пре почетка периода утврђеног Дневним терминским планом рада RTGS платног система Народне банке Србије (у даљем тексту: RTGS НБС систем) за извршавање налога за пренос у том систему.

Народна банка Србије омогућава функционисање привременог рачуна из става 4. ове тачке у случају да банка донесе одлуку о примени плана враћања на стање пре миграције података.

Изузетно од става 7. ове тачке, ако постоје објективне околности услед којих могу бити угрожени интереси клијената банке која спроводи поступак миграције података због статусне промене, Народна банка Србије може, на образложени захтев који банка доставља уз документацију из става 3. ове тачке, посебно утврдити рок спровођења поступка миграције података и омогућити функционисање привременог рачуна у том року.

Финансијска институција је дужна да поступак миграције података због статусне промене спроведе најкасније у року од десет радних дана од дана почетка примене плана из става 5. ове тачке, односно у року који утврди Народна банка Србије у складу са ставом 8. ове тачке.

Привремени рачун правног следбеника из ове тачке, као и поступање Народне банке Србије у складу са захтевом за привремени рачун ближе се уређују правилима рада RTGS НБС система.

56. Финансијска институција је дужна да обезбеди израду, чување и редовно одржавање документације која се односи на информационо-комуникациони систем, како би та документација у сваком тренутку била тачна, потпуна и ажурна.

Финансијска институција је дужна да свим корисницима информационо-комуникационог система обезбеди приступ одговарајућим документима у складу с потребама посла.

57. Финансијска институција је дужна да обезбеди адекватно, континуирано стручно оспособљавање и обучавање запослених за коришћење информационо-комуникационог система и очување његове безбедности и функционалности, као и да донесе, спроводи и редовно ажурира програм подизања свести о безбедности информационо-комуникационог система, а у складу са актуелним трендовима.

Финансијска институција је дужна да обезбеди да се, у складу са програмом из става 1. ове тачке, сви запослени и друга лица ангажована код ње периодично, а најмање једном годишње, обучавају како би се обезбедило да су оспособљени за извршавање својих дужности и одговорности у складу са политиком безбедности у циљу смањења оперативних ризика и ризика безбедности информационо-комуникационог система.

IX. ЕЛЕКТРОНСКЕ УСЛУГЕ

58. Електронске услуге су услуге које друштва за осигурање, друштва за управљање добровољним пензијским фондовима и даваоци финансијског лизинга пружају корисницима са удаљене локације преко интернета (у даљем тексту: пружалац електронских услуга). Пружалац електронских услуга је дужан да, као саставни део управљања ризиком информационо-комуникационог система, успостави процес управљања ризицима који произлазе из пружања електронских услуга.

59. Пружалац електронских услуга дужан је да при пружању електронских услуга примени безбедне и ефикасне методе за проверу и потврду идентитета и овлашћења лица, процеса и система.

Пружалац електронских услуга дужан је да корисницима при коришћењу ових услуга обезбеди аутентификацију која укључује комбинацију најмање два међусобно независна елемента за потврђивање корисничког идентитета.

60. Пружалац електронских услуга дужан је да усвоји и примени правила којима се на одговарајући начин, у складу с тржишном праксом и проценом ризика, ограничава број покушаја пријаве на систем за пружање електронских услуга, односно покушаја аутентификације, да одреди најдуже време без активности корисника након пријаве на тај систем, као и да утврди рокове важења параметара аутентификације.

При коришћењу једнократних лозинки ради аутентификације (нпр. *One Time Password – OTP*), пружалац електронских услуга дужан је да обезбеди да временско важење те лозинке буде ограничено на период који је потребан за обављање аутентификације.

Пружалац електронских услуга дужан је да утврди највећи могући број неуспешних покушаја пријаве на систем за пружање електронских услуга након којих ће тај систем бити трајно или привремено блокиран, као и да успостави процедуре за безбедно поновно активирање овог система.

Пружалац електронских услуга дужан је да утврди најдуже могуће време без активности корисника на систему за пружање електронских услуга по пријављивању у тај систем, након којег долази до аутоматског одјављивања корисника из овог система (тзв. завршетак сесије).

Пружалац електронских услуга дужан је да обезбеди одговарајућу потврду свог идентитета на дистрибутивном каналу за пружање електронских услуга како би корисници могли да провере пружаоца електронске услуге.

Пружалац електронских услуга је дужан да обезбеди постојање оперативних и системских записа како би се у одговарајућој мери обезбедила непорецивост и доказивост радњи у вези са пружањем електронских услуга .

X. ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

61. Пружаоци платних услуга дужни су да своје унутрашње акте ускладе са одредбама ове одлуке најкасније месец дана пре почетка њене примене и да у том року Народној банци Србије доставе обавештење о томе, заједно са усклађеним унутрашњим актима.

62. Ова одлука не примењује се на банку која се припаја другој банци, ако је банка којој се банка припаја поднела Народној банци Србије уредан захтев за давање сагласности на то припајање најкасније до дана почетка примене ове одлуке а планирани датум регистрације статусне промене припајања је најкасније 31. децембар 2026. године.

На банку која је најкасније до дана почетка примене ове одлуке доставила Народној банци Србије обавештење и одлуку надлежног органа банке да планира миграцију података на нови систем главних пословних апликација у смислу одлуке којом се уређују минимални стандарди управљања информационим системом финансијске институције – одредбе ове одлуке примењиваће се од 30. јуна 2026. године.

63. Поступци обавештавања покренути до дана почетка примене ове одлуке окончаће се према одредбама Одлуке о минималним стандардима управљања информационим системом финансијске институције („Службени гласник РС“, бр. 23/2013, 113/2013, 2/2017, 88/2019, 37/2021 и 100/2023 – др. одлука).

64. Даном почетка примене ове одлуке престаје да важи Одлука о минималним стандардима управљања информационим системом финансијске институције („Службени гласник РС“, бр. 23/2013, 113/2013, 2/2017, 88/2019, 37/2021 и 100/2023 – др. одлука).

65. Ова одлука ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Србије“, а примењује се од 1. јануара 2026. године.

ИО НБС бр. 85
20. децембра 2024.
Б е о г р а д

Председавајућа
Извршног одбора Народне банке Србије
Г у в е р н е р
Народне банке Србије

Др Јоргованка Табаковић, с.р.