АГЕНЦИЈА ЗА БАНКАРСТВО РЕПУБЛИКЕ СРПСКЕ

У П У Т С Т В О
О САДРЖАЈУ ПОЛИТИКЕ О УПОТРЕБИ ИКТ УСЛУГА

Бања Лука, октобар 2025. године

На основу члана 5. став 1. тачка б. и члана 22. став 1. тачка ђ. Закона о Агенцији за банкарство Републике Српске („Службени гласник Републике Српске" број 59/13 и 4/17), члана 6. став 1. тачка б. и члана 22. став 4. тачка л. Статута Агенције за банкарство Републике Српске („Службени гласник Републике Српске" број 63/17), те члана 53. Одлуке о управљању информационим системом и ризицима информационе и комуникационе технологије у банци („Службени гласник Републике Српске", број 42/25), директор Агенције за банкарство Републике Српске доноси

УПУТСТВО
О САДРЖАЈУ ПОЛИТИКЕ О УПОТРЕБИ ИКТ УСЛУГА

Предмет

Члан 1.

(1) Овим упутством се детаљније дефинише садржај политике о употреби ИКТ услуга које подржавају критичне функције или кључне пословне активности (у даљем тексту: Политика) у складу са чланом 22. став 3. Одлуке о управљању информационим системима и ризицима информационе и комуникационе технологије у банци (у даљем тексту: Одлука).

(2) Одредбе овог упутства примјењују се на банке са сједиштем у Републици Српској којима је Агенција за банкарство Републике Српске (у даљем тексту: Агенција) издала дозволу за рад.

Ризични профил банке и сложеност

Члан 2.

(1) Банка је дужна у оквиру Политике дефинисати елементе из члана 6. Одлуке о управљању екстернализацијом.

(2) Банка је дужна у оквиру Политике из става 1. овог члана узети у обзир величину и ризични профил банке, те природу, обим и сложеност њених услуга, активности и пословања, укључујући елементе који се односе на:

1) врсту ИКТ услуга укључених у уговор о употреби ИКТ услуга које подржавају критичне функције или кључне пословне активности између банке и пружаоца ИКТ услуга,
2) локацију пружаоца ИКТ услуга или његовог матичног друштва,
3) да ли се пружалац ИКТ услуга које подржавају критичне функције или кључне пословне активности налази у Босни и Херцеговини или изван ње, узимајући у обзир и локацију са које пружају ИКТ услуге и локацију на којој се подаци обрађују и складиште,
4) природу података који се размјењују са пружаоцем ИКТ услуга,
5) да ли је пружалац ИКТ услуга дио исте групе као и банка којој се пружају услуге,
6) ангажовање пружаоца ИКТ услуга који су овлашћени, регистровани или су под надзором надлежног органа унутар Босне и Херцеговине, те ангажовање осталих пружаоца ИКТ услуга,
7) ангажовање пружаоца ИКТ услуга који су добили овлашћени, регистровани или су под надзором надлежног органа изван Босне и Херцеговине, те ангажовање осталих пружаоца ИКТ услуга који то нису,
8) питање пружа ли ИКТ услуге које подржавају критичне функције или кључне пословне активности само један пружалац ИКТ услуга или мали број таквих пружаоца услуга,
9) преносивост ИКТ услуга којима се подржавају критичне функције или кључне пословне активности на другог пружаоца ИКТ услуга, узимајући у обзир технолошке специфичности и

10) потенцијални утицај поремећаја у пружању ИКТ услуга које подржавају критичне функције или кључне пословне активности на континуитет пословања и доступност услуга банке.

Примјена унутар групе

Члан 3.

Одредбе ове Политике банка је дужна примјењивати на појединачној и консолидованој основи.

Систем управљања

Члан 4.

(1) Банка је дужна да редовно, а најмање једном годишње, преиспитује и по потреби ажурира политику. Измјене треба благовремено имплементирати и што је могуће прије примијенити на релевантне уговоре, те документовати планиране рокове за провођење ових измјена.

(2) Банка је дужна Политиком дефинисати или упутити на методологију за одређивање ИКТ услуга и система којима се подржавају критичне функције или кључне пословне активности, те када се ова процјена проводи и преиспитује.

(3) Политиком се јасно додјељују одговорности за одобравање, управљање, контролу и документовање релевантних уговора, те осигурава да се унутар банке одржавају адекватне вјештине, искуство и знање за ефикасан надзор над тим уговорима, укључујући ИКТ услуге које се пружају на основу тих уговора.

(4) Не доводећи у питање коначну одговорност банке за ефикасан надзор релевантних уговора, политиком се прописује обавеза процјене пружаоца ИКТ услуга, ради утврђивања да располаже довољним ресурсима, којима се обезбјеђује усклађеност банке са правним и регулаторним захтјевима у вези са ИКТ услугама које подржавају критичне функције или кључне пословне активности банке.

(5) Банка је дужна у оквиру Политике јасно утврдити функцију одговорног за праћење уговора о употреби ИКТ услуга склопљених са пружаоцима ИКТ услуга или члана вишег руководства, те дефинисати начин на који та функција или члан вишег руководства сарађује са контролним функцијама (осим ако је њихов дио), линије извјештавања према Управи банке, укључујући врсту информација о којима се извјештава, документе који се достављају, те учесталост/периодичност извјештавања.

(6) Банка је дужна Политиком обезбиједити да су уговори у складу са сљедећим:

1) оквиром за управљање ИКТ ризицима из члана 12. Одлуке,
2) политиком информационе безбједности члан 17. став 4. тачка 1. Одлуке,
3) планом континуитета пословања у подручју ИКТ-а из члана 40. Одлуке и
4) захтјевима за извјештавање о инцидентима из члана 34. Одлуке.

(7) Политиком се јасно дефинише обавеза да ИКТ услуге које подржавају критичне функције или кључне пословне активности, а које пружају треће стране, подлијежу независном преиспитивању, те да су укључене у план ревизије, а у складу са чланом 12. Одлуке о управљању екстернализацијом.

(8) У Политици се изричито наводи да се уговором:

1) банка и њени органи управљања не ослобађају регулаторних обавеза и одговорности према клијентима;
2) не спрјечава ефикасан надзор банке нити крше релевантна регулаторна ограничења у погледу пружања услуга и обављања активности;
3) од пружаоца ИКТ услуга захтијева сарадња са надлежним органима;
4) садрже одредбе које обезбјеђују да банка, њени ревизори и надлежни органи имају правовремен, неограничен и несметан приступ подацима и просторијама који се односе на коришћење ИКТ услуга које подржавају критичне функције или кључне пословне активности.

(9) Политиком се утврђују захтјеви, укључујући правила, одговорности и процесе за сваку главну фазу животног циклуса уговора, обухватајући најмање сљедеће:

1) одговорности органа управљања, укључујући по потреби њихово учешће у процесу доношења одлука у вези са употребом ИКТ услуга које подржавају критичне функције или кључне пословне активности, а које се повјеравају пружаоцима ИКТ услуга;
2) планирање уговора, укључујући процјену ризика, дубинску анализу у складу са члановима 5. и 6, те поступак одобравања нових уговора или значајних измјена у постојећим уговорима у складу са чланом 8. став 4. овог Упутства;
3) учешће пословних јединица, интерних контрола и других релевантних јединица у вези са уговорима;
4) провођење, праћење и управљање уговорима у складу са члановима 7, 8. и 9,
5) документовање и вођење евиденције, узимајући у обзир захтјеве у вези са регистром информација у складу са чланом 23. Одлуке;
6) излазне стратегије и поступак раскида у складу са чланом 10. овог Упутства.

Процјена ризика прије склапања уговора

Члан 5.

(1) Банка је дужна Политиком обухватити и активности дефинисања пословних потреба банке и провођења процјене ризика прије склапања уговора, узимајући у обзир одредбе члана 24. Одлуке.

(2) У оквиру процјене ризика из става 1. овог члана, банка је дужна узети у обзир одредбе дефинисане чланом 8. Одлуке о управљању екстернализацијом у банци, примјењујући их на све ИКТ услуге којима се подржавају критичне функције или кључне пословне активности, а које су повјерене пружаоцима ИКТ услуга.

(3) Банка је дужна приликом процјене ризика, узети у обзир и сљедеће:

1) оперативне ризике,
2) правне ризике,
3) ИКТ ризике,
4) репутационе ризике,
5) ризике повезане са заштитом повјерљивих или личних података,
6) ризике повезане са доступношћу података,
7) ризике повезане са локацијом на којем се подаци обрађују и складиште,
8) ризике повезане са локацијом пружаоца ИКТ услуга и
9) ризике од концентрације ИКТ услуга код истог пружаоца ИКТ услуга на нивоу банке.

Дубинска анализа

Члан 6.

(1) Банка је дужна Политиком дефинисати адекватан и сразмјеран поступак за избор и процјену потенцијалних пружалаца ИКТ услуга, а прије склапања уговора.

(2) Приликом процјене из става 1. овог члана, банка је дужна узети у обзир одредбе члана 8. Одлуке о управљању екстернализацијом и члана 24. став 1. тачка 4. Одлуке, те процијенити да ли пружалац ИКТ услуга:

1) има пословну репутацију, довољне способности, стручна знања и адекватне финансијске, људске и техничке ресурсе, стандарде у области информационе безбједности, одговарајућу организациону структуру, поступке управљања ризицима и интерне контроле, те уколико је примјењиво, потребна одобрења или уписе у регистре код надлежних органа за пружање ИКТ услуга које подржавају критичне функције или кључне пословне активности на поуздан и професионалан начин,

2) има способност да прати релевантна технолошка достигнућа и препозна најбоље праксе у области ИКТ безбједности, те их примјењује, ако је то потребно, у циљу успостављања ефикасног и поузданог оквира за дигиталну оперативну отпорност,
3) ангажује или намјерава да ангажује подизвођаче за пружање ИКТ услуга које подржавају критичне функције или кључне пословне активности или њихових битних дијелова;
4) налази се, или обрађује или складишти податке у изван Босне и Херцеговине земљи и ако је то случај, да ли таква пракса повећава ниво оперативних ризика, репутационих ризика или ризика од утицаја рестриктивних мјера, укључујући ембарго и санкције, који могу утицати на способност пружаоца ИКТ услуга да пружа услуге или способност банке да их прима;
5) пристаје ли на уговорне одредбе које омогућавају ефикасно провођење ревизије, укључујући и ревизије на лицу мјеста, од стране банке, Агенција или трећих страна које су оне именовале
6) поступа ли на етички и друштвено одговоран начин, поштује ли људска права и права дјеце, укључујући забрану рада дјеце, поштује ли релевантна начела заштите животне средине и обезбјеђује ли одговарајуће радне услове.

(3) Банка је дужна Политиком дефинисати потребан ниво увјерења у погледу ефикасности оквира за управљање ризицима пружалаца ИКТ услуга, за ИКТ услуге којима се подржавају критичне функције или кључне пословне активности које пружалац ИКТ услуга треба да пружи. Политиком се захтијева да поступак дубинске анализе укључује оцјену постојања мјера за ублажавање ризика и очување континуитета пословања, као и начина на који је њихова примјена обезбијеђена код пружаоца ИКТ услуга.

(4) Политиком се утврђује начин провођења дубинске анализе за избор и процјену потенцијалних пружалаца ИКТ услуга и наводи се који од сљедећих елемената се користе за потребан ниво увјерења у погледу рада пружаоца ИКТ услуга:
1) ревизија или независна процјена које проводи сама банка или се проводе у њено име;
2) извјештаји о независној ревизији које пружалац ИКТ услуга доставља на захтјев;
3) извјештаји о ревизији које је сачинила интерна ревизија пружаоца ИКТ услуга;
4) одговарајући сертификати трећих страна;
5) друге релевантне информације које су доступне банци или које је доставио пружалац ИКТ услуга.

(5) Банка је дужна обезбиједити одговарајући ниво осигурања у погледу рада пружаоца ИКТ услуга, узимајући у обзир елементе из става 4. овог члана. У складу са процјеном ризика, банка је дужна употребљавати више елемената из става 4. овог члана.

Сукоб интереса

Члан 7.

(1) Банка је дужна Политиком дефинисати одговарајуће мјере за идентификовање, спречавање и управљање стварним или потенцијалним сукобима интереса који произлазе из ангажовања пружалаца ИКТ услуга, које треба предузети прије склапања уговора, те обезбиједити континуирано праћење таквих сукоба интереса.

(2) У оквиру дефинисаних мјера из става 1. овог члана, банка је дужна узети у обзир и одредбе члана 8. став 1. тачка 7. Одлуке о управљању екстернализацијом.

(3) Ако се ИКТ услуге, којима се подржавају критичне функције или кључне пословне активности, повјеравају пружаоцу ИКТ услуга унутар исте групе, банка је дужна у Политици навести да се одлуке о условима пружања тих услуга, укључујући и финансијске услове, доносе на објективан начин.

Уговорне одредбе

Члан 8.

(1) Банка је дужна Политиком дефинисати да уговори са пружаоцима ИКТ услуга морају бити у писаној форми и да морају обухватити све елементе из члана 27. Одлуке. Политика мора да обухвати и елементе који се односе на:

1) управљањем ризиком информационе и комуникационе технологије (ИКТ),
2) извјештавање о значајним ИКТ инцидентима и обавјештавање Агенције о значајним сајбер пријетњама,
3) обавјештавање клијената и партнера, најмање о значајним ИКТ инцидентима или рањивостима,
4) тестирање дигиталне оперативне отпорности,
5) размјену информација и података о сајбер пријетњама и рањивостима и
6) мјере за добро управљање ИКТ ризиком повезаним с трећим странама.

(2) Банка је дужна Политиком дефинисати да уговорне одредбе укључују право банке на приступ подацима, провођење надзора и ревизија, те провођење тестирања ИКТ система. У ту сврху, не доводећи у питање коначну одговорност банке, банка је дужна Политиком дефинисати примјену сљедећих метода:

1) властите интерне ревизије или ревизије које проводе именоване треће стране,
2) према потреби, групне ревизије и заједничка тестирања ИКТ система, укључујући пенетрационо тестирање вођено пријетњама, које може организовати заједно са другим банкама или клијентима истог пружаоца ИКТ услуга и које проводе те банке наручиоци односно трећа страна коју су они именовали,
3) према потреби, сертификате трећих страна и
4) према потреби, извјештаје о ревизији које је сачинио пружалац ИКТ услуга или трећа страна, а који су стављени на располагање.

(3) Банка се не треба дугорочно ослањати искључиво на сертификате из става 2. тачка 3. овог члана или извјештаје о ревизији из става 2. тачка 4. овог члана. Политика треба да дозволи коришћење метода наведених у ставу 2. тачке 3. и 4. само уколико је банка:

1) задовољна планом ревизије пружаоца ИКТ услуга у вези са релевантним уговорима,
2) обезбиједила да обухват сертификације или извјештаја о ревизији укључује системе и контроле које је банка утврдила као кључне, као и усклађеност са релевантним регулаторним захтјевима,
3) обезбиједила детаљан и континуиран преглед садржаја извјештаја о ревизији и обухват сертификата, те провјерава да наведени извјештаји или сертификати нису застарјели, тј. да су и даље релевантни,
4) обезбиједила да су кључни системи и контроле обухваћени и наредним верзијама сертификата или извјештаја о ревизији,
5) задовољна оспособљеношћу треће стране која издаје сертификате или проводи ревизију,
6) утврдила да се сертификати издају и ревизије проводе у складу са релевантним професионалним стандардима, те укључују тестирање оперативне ефикасности постојећих кључних контрола,
7) дефинисала уговорно право да затражи проширење обухвата сертификације или извјештаја о ревизији на друге релевантне системе и контроле, при чему је број и учесталост таквих захтјева разумна и оправдана са становишта управљања ризицима и
8) задржала уговорно право да према властитој одлуци обавља појединачне и групне ревизије у вези са релевантним уговорима и та права остварује у договореној учесталости.

(4) Банка је дужна Политиком обезбиједити да се значајне измјене релевантних уговора документују у писаној форми, која је датирана и коју су потписале све стране, као и да је у Политици дефинисан поступак обнављања уговора.

Праћење уговора

Члан 9.

(1) Банка је дужна да Политиком дефинише поступке праћења и надзора пружаоца ИКТ услуга узимајући у обзир одредбе члана 13. Одлуке о управљању екстернализацијом. То укључује и обавезу да се у уговорима са пружаоцима ИКТ услуга прецизирају мјере и кључни показатељи за континуирано праћење њиховог рада, укључујући мјере за надзор усклађености са захтјевима који се односе на повјерљивост, доступност, интегритет и аутентичност података и информација, као и мјере за надзор усклађености рада пружаоца услуга са релевантним политикама и процедурама банке. Политика такође треба да прецизира мјере које се примјењују када се не испуне уговорени нивои услуга, укључујући према потреби уговорне казне.

(2) Политиком се дефинише начин на који банка оцјењује да ли пружаоци ИКТ услуга који су ангажовани за пружање ИКТ услуга којима који подржавају критичне функције или кључне пословне активности, поштују одговарајуће стандарде рада и квалитета у складу са уговором и политикама банке. Банка је дужна Политиком посебно обезбиједити следеће:

1) да пружаоци ИКТ услуга достављају банци одговарајуће извјештаје о својим активностима и услугама, укључујући периодичне извјештаје, извјештаје о инцидентима, извјештаје о испоруци услуга, извјештаје о ИКТ безбједности, те извјештаје о мјерама и проведеним тестирањима у области континуитета пословања,
2) да се рад пружаоца ИКТ услуга оцјењује кључним показатељима успјешности, кључним показатељима контроле, ревизијама, самооцјењивањем и независним прегледима у складу са оквиром банке за управљање ИКТ ризицима,
3) да банка прима и друге релевантне информације од пружалаца ИКТ услуга,
4) да банка, према потреби, буде обавијештена о ИКТ инцидентима и оперативним или безбједносним инцидентима повезаним са пружањем услуга, и
5) да се проводе независне ревизије и прегледи којима се провјерава усклађеност са законским и подзаконским прописима и интерним политикама.

(3) Банка је дужна Политиком дефинисати да процјену из става 2. овог члана треба документовати, а резултате ове процјене употребљавати за ажурирање процјене ризика, а у складу са чланом 13. став 3. Одлуке о управљању екстернализацијом.

(4) Банка је дужна Политиком дефинисати одговарајуће мјере које треба предузети уколико утврди недостаци код пружаоца ИКТ услуга, укључујући ИКТ инциденте, као и оперативне или безбједносне инциденте у пружању ИКТ услуга којима се подржавају критичне функције или кључне пословне активности, као и усклађеност са уговорним одредбама или законским прописима. Такође, Политиком се дефинише и начин на који се прати провођење тих мјера како би се обезбиједило да се оне заиста поштују, узимајући у обзир значајност утврђених недостатака.

Излазна стратегија и раскид уговора

Члан 10.

(1) Банка је дужна Политиком дефинисати захтјеве за документованом излазном стратегијом за сваки уговор, као и захтјеве за периодични преглед и тестирање те стратегије узимајући у обзир одредбе члана 10. став 1. Одлуке о управљању екстернализацијом и члана 25. Одлуке. Приликом утврђивања излазне стратегије, банка је дужна узети у обзир и следеће:

1) непредвиђене и дуготрајни прекиде у пружању услуге,
2) неодговарајуће или неуспјешно пружање услуга и

3) неочекивани раскид уговора.

(2) Банка је дужна дефинисати излазну стратегију која треба да буде реалистична, изводљива, заснован на вјероватним сценаријима и разумним претпоставкама, те садржи планирани распоред провођења у складу са условима изласка и престанка који су утврђени у уговору.

Прелазне и завршне одредбе

Члан 11.

(1) Ово упутство ступа на снагу осмог дана од дана доношења и објављује се на службеној интернет страници Агенције.

(2) Банка је дужна ускладити своје пословање са одредбама овог упутства до 01.04.2026. године.

Број: Д-22/25

Дана, 30.10.2025. год.

Директор

Срђан Шучут