На основу члана 17. Закона о Савјету министара Босне и Херцеговине ("Службени гласник БиХ", бр. 30/03, 42/03, 81/06, 76/07, 81/07, 94/07 и 24/08) и Поглавља 3. Одлуке о усвајању Политике управљања информационом безбједношћу у институцијама Босне и Херцеговине, за период од 2017. до 2022. године ("Службени гласник БиХ", број 38/17), на приједлог Министарства комуникација и транспорта Босне и Херцеговине, Савјет министара Босне и Херцеговине, на 3. сједници, одржаној 23. фебруара 2023. године, донио је

ОДЛУКУ
О УСВАЈАЊУ СМЈЕРНИЦА О КОНТРОЛИ ПРИСТУПА И БИЉЕЖЕЊУ ДОГАЂАЈА, СМЈЕРНИЦА О ФИЗИЧКОЈ ЗАШТИТИ ИНФОРМАЦИЈА И СМЈЕРНИЦА О КОРИШЋЕЊУ ПРЕНОСНИХ УРЕЂАЈА У ИНСТИТУЦИЈАМА БОСНЕ И ХЕРЦЕГОВИНЕ

Члан 1.
(Предмет Одлуке)

Овом одлуком усвајају се Смјернице о контроли приступа и биљежењу догађаја, Смјернице о физичкој заштити информација и Смјернице о коришћењу преносних уређаја у институцијама Босне и Херцеговине, које су дио ове одлуке.

Члан 2.
(Праћење реализовања)

За праћење реализовања ове одлуке задужују се Министарство комуникација и транспорта Босне и Херцеговине и Министарство безбједности Босне и Херцеговине.

Члан 3.
(Ступање на снагу)

Ова одлука ступа на снагу даном доношења и објављује се у "Службеном гласнику БиХ".

СМ број 71/23	Предсједавајућа
23. фебруара 2023. године	Савјета министара БиХ
Сарајево	**Борјана Кришто**, с. р.

СМЈЕРНИЦЕ
О КОНТРОЛИ ПРИСТУПА И БИЉЕЖЕЊУ ДОГАЂАЈА

1. СВРХА

Засигурно један од важнијих узрока проблема безбједности представљају овлашћени корисници. Они својим поступцима, било случајним или намјерним, угрожавају безбједност система у великој мјери.

Неки од узрока безбједносних инцидената које изазову овлашћени корисници су:

- знатижеља,
- доказивање,
- крађа идентитета од злонамјерног лица,
- случајни поступци (неедукованост корисника),
- прикупљање података у злонамјерне сврхе итд.

Наведене пријетње безбједности информационим системима разлог су због којих постоји потреба за контролом приступа, тј. забраном приступа оним ресурсима система којима корисник нема потребе приступати.

Осим контрола приступа, у сврху благовременог уочавања одступања од политике приступа и пружања доказа у случају безбједоносног инцидента, у систем је потребно увести безбједоносну контролу биљежење догађаја (надгледање).

2. КОНТРОЛА ПРИСТУПА

2.1. Права приступа у складу са потребама

Приступ информационим ресурсима потребно је одобрити уколико запослени или трећа страна има реалну потребу за приступ траженим ресурсима. Захтјев за додјелу права приступа на основу којег је донесена одлука о додјели права приступа треба бити документован.

Документ треба да садржи:

- идентификатор иницијатора захтјева,
- идентификатор лица коме је потребно додијелити права приступа,
- опис захтјева,
- датум подношења захтјева,
- укратко политику безбједности траженог ресурса - класификација ресурса, да ли постоје законске и уговорне обавезе и сл.,
- вријеме трајања права приступа - период у којем ће додијељена права вриједити (након његовог истека потребно је поновно предати захтјев за додјелу права приступа),
- одобриоца захтјева (ко је захтјев прегледао и одобрио).

2.2. Управљање приступом корисника

С циљем квалитетне контроле приступа информационим системима и сервисима потребно је успоставити одговарајуће процедуре. Те процедуре требају обухватити све стадије у животном циклусу корисничког приступа, од почетне регистрације новог корисника до коначног одјављивања корисника којем више није потребан приступ информационим ресурсима. Посебну пажњу треба посветити контроли додјеле привилегованих права приступа.

2.3. Регистрација корисника

Да би појединим кориснику била додијељена права приступа информационом систему и сервисима потребно је дефинисати поступке регистрације у и одјаве из система. Приступ треба контролисати кроз процес регистрације корисника који укључује:

- коришћење корисничких имена које је додијелио администратор система или за то одговорно лице,
- корисничка имена требају бити јединствена како би се корисници могли повезати са њиховим активностима,
- провјеру аутентификације корисника преко лозинке,
- провјеру права приступа за коришћење информационих ресурса према корисничком имену,
- замрзавање корисниковог рачуна у случају планираног дужег изостанка са посла,
- тренутно укидање свих права кориснику уколико он престане бити запослен или дође до раскида уговара с трећом страном.

2.4. Управљање корисничким лозинкама

Лозинке служе како би се путем мреже провјерило да ли је корисник који се представља корисничком лозинком управо тај корисник. Стога је потребно безбједносним механизмима омогућити максималну безбједност лозинки у смислу њихове тајности. Осим политике безбједности намијењене корисницима у којој се јасно дефинише на који начин руковати лозинкама, лице одговорно за безбједност дужно је држати се сљедећих правила приликом расподјеле лозинки:

- корисници су дужни приликом преузимања лозинки потписати изјаву у којој се обавезују руковати лозинкама према правилима дефинисаним у Правилнику о информатичкој безбједности радног мјеста,
- приликом додјеле лозинке корисницима прво им се додјељује привремена лозинка коју у што краћем року, при првој пријави на систем, морају промијенити, при чему систем треба подесити тако да не дозвољава пријаву привременом лозинком,
- лозинке се корисницима смију прослиједити искључиво на безбједан начин, никако не електронском поштом, телефоном или преко треће стране,
- лозинке се не смију похрањивати на рачунару у незаштићеном облику.

2.5. Одговорност корисника

2.5.1. Употреба лозинки

Од корисника је потребно захтијевати да при одабиру и руковању лозинкама слиједе безбједносне упуте дефинисане Правилником о информатичкој безбједности радног мјеста. Кориснике треба савјетовати да:

- чувају повјерљивост лозинки,
- не биљеже лозинке на папире,
- лозинке мијењају искључиво након пријаве на систем,
- бирају квалитетне лозинке, дугачке минимално 6 знакова, максимално 10,
- лозинке буду лако памтљиве,
- лозинке садрже бројеве и слова, по потреби и специјалне знакове,
- лозинке не представљају имена, презимена, градове, датуме рођења, надимке и сл. ријечи,
- редовно мијењају лозинке,
- не користе већ употребљаване лозинке,
- не користе лозинке које већ користе на другим системима.

2.5.2. Надгледана корисничка опрема

Кориснике је потребно едуковати о потреби заштите опреме када нису у њеној близини. Многи корисници нису ни свјесни могућности злоупотребе рачунара, мобитела, али и других комуникационих уређаја уколико на кратко вријеме остану без надзора. Сваки корисник мора бити свјестан своје одговорности, безбједносних захтјева и поступака за заштиту ненадгледане опреме.

Кориснике треба савјетовати да:

- се одјаве са система или заштите рачунар посебним програмима (нпр. чувар екрана) уколико рачунар остављају без надзора,
- рачунар одјаве са система након завршетка посла,
- уколико је потребно, рачунаре и другу опрему закључају када је не користе.

2.5.3. Контрола приступа мрежи

Сви интерни и екстерни мрежни сервиси морају бити контролисани у сврху заштите ресурса од корисника који имају приступ мрежи и мрежним ресурсима. Контрола приступа мрежи треба садржавати сљедеће контроле:

- корисници смију приступити само оним мрежним сервисима за које имају дефинисане експлицитне овласти,
- контроле управљања и процедуре за заштиту приступа мрежи требају бити јасно дефинисане,
- у сврху смањења ризика неауторизованог приступа потребно је одредити "прописани пут",
- кориснике који приступају ресурсима са удаљених локација потребно је аутентификовати посебним методама које обезбјеђују одговарајући ниво заштите.

2.5.4. Контрола приступа оперативном систему

Приступ корисника оперативним системима потребно је контролисати путем уграђених механизама с циљем спречавања неовлашћеног приступа. Механизам контроле приступа оперативном систему треба садржавати:

- приликом пријаве на систем корисник треба унијети своје корисничко име и лозинку, на основу чега се ради провјера идентитета,
- провјеру да ли је период ваљаности лозинке истекао; уколико јесте (свака 3 мјесеца), обавијестити корисника да је потребно направити измјену,
- систем мора биљежити приступ информационом систему и покушаје приступа,
- рад корисника на клијентским радним станицама треба додатно контролисати на начин да се прати вријеме неактивности; уколико је клијентска радна станица неактиван дуже од 10 минута, треба направити аутоматску одјаву са система,
- уколико је потребно, контролу са које се локације приступа систему,
- број могућих пријава на систем треба ограничити на 3 пријаве.

3. ЗАКЉУЧАК

У складу са Политиком и Смјерницама о контроли приступа и биљежењу догађаја препоручује се институцијама БиХ да донесу свој интерни акт у којем ће дефинисати **правило/процедуру о контроли приступа и биљежењу догађаја.**

ЛИТЕРАТУРА:

1. Политика управљања информационом безбједношћу у институцијама Босне и Херцеговине за период 2017-2022. године ("Службени гласник БиХ", број 38/17)
2. Стандард ISO/IEC 27001 - Безбједносне технике - Системи за управљање безбједношћу информација - Захтјеви
3. Стандард ISO/IEC 27002 - Безбједносне технике - Правило добре праксе за контроле безбједности информација
4. Закон о заштити тајних података ("Службени гласник БиХ", бр. 54/05 и 12/09)

СМЈЕРНИЦЕ
О ФИЗИЧКОЈ ЗАШТИТИ ИНФОРМАЦИЈА

1. СВРХА

Информациони системи често су основа пословања институције који садрже врло важне информације из надлежности и овлашћења институције. Нарушавање њихове безбједности може водити до откривања осјетљивих података. Један од аспеката безбједности информационог система представља и физичка безбједност, тј. скуп мјера које спречавају недозвољен физички приступ информацијама и ресурсима. Пријетње физичкој безбједности долазе од природних непогода попут поплава и потреса те људских рањивости попут непослушности, намјере за саботажом или крађом. Такође, постоје неке пријетње које су резултат непредвиђених околности као што је пожар или неке врсте кварова на разним системима. Како би се смањила штета након појављивања неке од споменутих пријетњи, потребно

је увести адекватне мјере заштите. Под тим се подразумијева обезбјеђење околине и просторија објеката те спровођење контроле приступа. Такође, потребно је увести заштиту опреме и уређаја путем доступних технологија. Разни системи развијени су за успостављање и побољшање физичке безбједности. Неки од њих су алармни системи те системи за надзор, контролу приступа или закључавање вриједних уређаја.

Сврха физичке заштите информационог система је превентивним методама обезбиједити заштиту система од намјерних или случајних деструктивних радњи. Физичком заштитом жели се:

- спријечити неовлашћен приступ,
- спријечити ометање пословних просторија,
- спријечити непотребан приступ корисника осјетљивој опреми,
- обезбиједити заштита опреме од природних утицаја,
- обезбиједити сигурност инсталација,
- обезбиједити одржавање опреме.

2. ПОДРУЧЈЕ ФИЗИЧКЕ ЗАШТИТЕ

Физичка безбједност описује мјере које спречавају неовлашћен приступ ресурсима или информацијама похрањеним на физичким медијима. Ради се о скупу смјерница за дизајнирање структуре која је отпорна на разне злонамјерне радње, а може укључивати једноставну примјену закључавања врата или запошљавање обезбјеђења. Физичка безбједност је најосновнији аспект заштите, а обухваћа контролу заштите просторија, постројења, зграда и друге имовине. Примјена физичке безбједности подразумијева процес употребе мјера заштите како би се спријечио неовлашћен приступ, оштећење или уништење добара. У основи, физичка безбједност односи се на спречавање оштећења било којег дијела некретнина, постројења, канцеларија, објеката или зграда. Такође, она доприноси заштити људи и информација, иако се на те групе примјењују и друге софистициране мјере заштите. Према томе, физичка безбједност чини дио свеукупне безбједности информационог система као основе на којој су све безбједносне мјере базиране. Мјере које укључује физичка безбједност, а служе за заштиту особља, опреме и имовине, могу се подијелити на:

1. *пасивне мјере* – ефективна употреба архитектуре, околине и освјетљавање за постизање боље безбједности кроз олакшану детекцију упада или потенцијалних пријетњи,
2. *активне мјере* – укључују употребу познатих система и техника дизајнираних за детекцију и реакцију на пријетње.

Да би се обезбиједила физичка заштита информационог система, институција је дужна спровести сљедеће тачке безбједности:

- потребно је јасно дефинисати и документовати ко је овлашћен приступити појединим просторијама под физичком заштитом,
- контролним механизмима потребно је спријечити сваки покушај неовлашћеног приступа; улазе у просторије које садрже сервере, медије за похрану података и остале осјетљиве ресурсе потребно је заштитити методама контроле уласка (картице, кључ и сл.),
- врата на улазима у заштићена подручја морају бити отпорна на пожаре, поплаве и пробијања,
- улази у просторије које садрже осјетљиву опрему морају бити јасно означени,
- сви контролни механизми морају бити периодички прегледавани како би се на вријеме уочили недостаци заштите или покушаји неовлашћеног приступа.

3. БЕЗБЈЕДНОСТ ОПРЕМЕ

Најважнији аспект код физичке заштите информационог система представља правилна заштита опреме и уређаја. Сваком уређају треба дефинисати посебне мјере заштите с обзиром на његову намјену и вриједност. Такве мјере требају спријечити све пријетње, укључујући пријетње од природних непогода или људске пријетње. Већина организација спроводи само основне мјере заштите опреме које често нису довољне, а односе се на заштиту сервера и персоналних рачунара. Разлог томе је што наведени елементи садрже највише осјетљивих података па њихово оштећење може довести до озбиљних посљедица. Ипак, потребно је спровести додатне безбједносне мјере при руковању опремом, као што су:

- закључавање уређаја након употребе (нпр. факс уређаја),
- смјештај уређаја на безбједна мјеста,
- похрана преносних медија на безбједна мјеста,
- адекватно уништавање старих преносних медија.

Сврха обезбјеђивања опреме је спријечити губитке, штету или компромитовање имовине и прекид пословних активности. Опрема треба бити заштићена од пријетњи и опасности из околине. Заштита опреме је неопходна како би се смањио ризик неовлашћеног приступа подацима те како не би дошло до губљења и оштећења имовине.

3.1. Смјештај и заштита опреме

3.1.1. Заштита сервера

Сервери представљају врло важан аспект за пословање сваке организације јер могу садржавати врло важне информације, а запослени их свакодневно користе. Због таквих намјена, најбоља пракса је раздвајање свакодневних функција од сервера. То значи да се један сервер не би требао користити за обављање свакодневних задатака. Још један од важних елемената заштите представља правилан смјештај сервера. Најбоље би било сервере издвојити у посебну просторију коју је могуће добро надзирати. Такође, смјештај треба организовати тако да се спријечи помицање и премјештање сервера. Тиме се спрјечава оштећење и узроковање кварова, али се може постићи и боља заштита од неких природних пријетњи (нпр. потрес).

3.1.2. Заштита персоналних рачунара

Најосновнији начин заштите персоналних рачунара укључује добру едукацију запослених. Уколико су запослени упознати са правилним начином руковања рачунаром, ризик од разних пријетњи знатно је умањен. Запосленима је потребно јасно дефинисати правила у облику безбједносних политика те их представити на једноставан начин. У склопу безбједносне политике треба навести правилно опхођење према рачунарима у случају неког квара или природне непогоде. Такође, треба дефинисати заштиту од крађе, шпијунаже и других пријетњи које доносе људи, а односе се на физичку безбједност. Употреба надзора у облику постављања камера и обезбјеђења може спријечити запослене при покушају оштећивања или крађе рачунара. Надзорне камере потребно је поставити на кључна мјеста која су у близини вриједних уређаја или рачунара.

Како би се онемогућило злонамјерно руковање рачунаром неког запосленог потребно је рачунар закључати уколико није у употреби. Рачунар који остаје укључен посјетиоци могу злоупотријебити за откривање осјетљивих података или наношење друге штете. Смјештај рачунара

запослених такође представља важан аспект заштите. Рачунаре је потребно распоредити тако да нити један запослени нема приступ подацима другог запосленог. Како би се додатно спријечило откривање осјетљивих података, треба избјегавати да сви корисници употребљавају исти преносни уређај за похрану података. Спречавање крађе може се постићи и неким софистицираним уређајима. Неки од њих су системи за праћење и откривање локације украдених или изгубљених ствари. Такође, постоје посебни држачи за преносиве рачунаре који имају могућност закључавања. Уколико такви уређаји нису доступни, могуће је уградити ормариће са картицама за безбједну похрану мобилних рачунара. Безбједност информационог система додатно се може повећати закључавањем USB прикључака како би се спријечило преузимање података или онемогућило убацивање злонамјерних програма.

Сљедеће смјернице треба узети у обзир при физичкој заштити опреме:

- опрема мора бити смјештена тако да је непотребни приступ опреми минималан,
- јединице за обраду података морају бити смјештене тако да је смањена могућност посматрања неовлаштеним корисницима (примјер: постављање монитора под таквим углом да само особа за рачунаром види слику),
- контроле је потребно спроводити тако да минимизују ризик од потенцијалних пријетњи (крађа, пожар, дим, вода, вибрације, радијација итд.),
- забрањено је јести, пити и пушити у близини опреме,
- услови окружења (температура, влага) који могу утицати на рад јединица за обраду информација треба дефинисати одговорно лице а морају бити строго надзирани.

3.2. Безбједност инсталација

Јединице за обраду података морају бити заштићене од грешака које могу настати у снабдијевању енергијом, водом, одвођењем отпадних вода, гријањем/хлађењем итд. Све наведене инсталације морају бити благовремено прегледане и тестиране како би се на вријеме уочиле и исправиле грешке у раду.

Нестанак струје, поплаву, пожар или било коју другу пријетњу битно је алармирати звучним и свјетлосним сигналима како би се благовремено предузеле прописане акције у случају незгоде. Снабдијевање водом мора бити редовно контролисано како исправност уређаја за гашење пожара не би била упитна. Телекомуникациона опрема мора бити инсталирана тако да евентуалан прекид везе не утиче на комплетан прекид комуникације. Примјер рјешења овог проблема је прикључење комуникационих уређаја на више сервера.

3.3. Безбједност код каблирања

Каблови за снабдијевање електричном енергијом и телекомуникациони каблови морају бити адекватно заштићени од оштећења, прекида или прикључења неовлашћених корисника на мрежу, ако то услови на постојећој физичкој локацији дозвољавају. Прије каблирања треба бити размотрено сљедеће:

- каблови за напајање јединица за обраду података, уколико је могуће, морају бити положени подземно (алтернатива је адекватна физичка заштита),
- исто важи и за телекомуникационе каблове,
- каблови за напајање морају бити раздвојени од телекомуникационих како би се избјегло међудјеловање,
- означавање каблова посебним идентификационим ознакама спријечиће грешке у спајању (напомена: ознаке је потребно документовати).

4. ОДРЖАВАЊЕ ОПРЕМЕ

Одржавање опреме треба редовно обављати стручњак како би се обезбиједила исправност, тј. непрекидан рад. При одржавању опреме треба се придржавати сљедећег:

- одржавање опреме мора бити у складу са препорукама произвођача, у одређеним временским интервалима и по задатим спецификацијама,
- само овлашћена лица смију сервисирати опрему,
- прије сервисирања опреме потребно је спровести одговарајуће сигурносне контроле, уколико за тим постоји потреба, те је потребно обрисати повјерљиве информације (потребе за оваквим мјерама настају уколико сервисирање извршавају спољни партнери или трећа страна),
- приступ спољних партнера опреми треба бити строго контролисан и документован,
- приступ спољних партнера опреми треба бити ограничен уговором.

5. ЗАКЉУЧАК

У складу са Политиком и Смјерницама о физичкој заштити информација препоручује се институцијама БиХ да донесу свој интерни акт у којем ће дефинисати **правила/процедуре о физичкој заштити информација.**

ЛИТЕРАТУРА:

1. Политика управљања информационом безбједношћу у институцијама Босне и Херцеговине за период 2017-2022. године ("Службени гласник БиХ", број 38/17)
2. Стандард ISO/IEC 27001 - Безбједносне технике - Системи за управљање безбједношћу информација - Захтјеви
3. Стандард ISO/IEC 27002 - Безбједносне технике - Правило добре праксе за контроле безбједности информација
4. Закон о заштити тајних података ("Службени гласник БиХ", бр. 54/05 и 12/09)

СМЈЕРНИЦЕ
О КОРИШЋЕЊУ ПРЕНОСНИХ УРЕЂАЈА

1. СВРХА

Преносни рачунари су све популарнији. Цјеновно близу, а практичношћу пуно испред десктоп рачунара, постали су чест избор при куповини рачунара, било да се ради о пословним или приватним корисницима.

Али, употреба преносних рачунара од запослених, партнера или других корисника доноси потребу за увођењем додатних безбједносних контрола. Оне морају спријечити сваку неовлашћену радњу која може да угрози безбједност информационог система.

2. ИДЕНТИФИКАЦИЈА ПРИЈЕТЊИ

Безбједност система употребом преносних рачунара можете да буде угрожена на сљедеће начине:

- случајни поступци овлашћеног корисника преносног рачунара,
- намјерни поступци овлашћеног корисника преносног рачунара,

- намјерни поступци неовлашћеног (злонамјерног) корисника,
- покретање малициозног кôда на преносном рачунару,
- крађа, губитак или мијењање података због неправилног руковања преносним рачунаром.

3. ФИЗИЧКА ЗАШТИТА ПРЕНОСНОГ РАЧУНАРА

3.1. Унутар просторија институције

Унутар просторија институције корисник је дужан да се придржава правила дефинисаних Правилником о информатичкој безбједности радног мјеста. То значи да рачунар ни у којем тренутку не смије оставити незаштићен без надзора. Код краћих одсуствовања рачунар је потребно заштитити неким од једноставнијих облика заштите (нпр. чуваром екрана са лозинком и сл.). Код дужих одсуствовања (годишњи одмор, боловање) корисник је дужан рачунар смјестити у простор под физичком заштитом (у закључани ормар или просторију).

3.2. Изван просторија институције

Уколико се преносни рачунар износи изван просторија институције (на путовање или сл.), потребно је придржавати се сљедећег:

- вријеме без надзора рачунара треба бити што краће,
- рачунар не треба остављати у аутомобилу на видљивом мјесту,
- рачунар не треба остављати без надзора у незакључаном простору,
- остављени преносни рачунар треба бити искључен, закључан у спремишту гдје није видљив.

4. СЕРВИС ОПРЕМЕ

4.1. Сервисирање

- уколико је могуће, прије сервисирања потребно је направити безбједносне копије свих (важних) података са рачунара у складу с *Правилником о безбједносним копијама*,
- ако сервисирање проводи трећа страна, податке са рачунара потребно је заштитити овисно о њиховој класификацији (неком од криптографских метода), а уколико постоји потреба, подаци са рачунара морају бити избрисани (након израде безбједносне копије података).

4.2. Повратак преносног рачунара са сервисирања

- све лозинке морају бити промијењене,
- све функционалности требају бити провјерене,
- све се мора подвргнути антивирусној провјери.

5. ЗАКЉУЧАК

У складу са Политиком и Смјерницама о коришћењу преносних уређаја препоручује се институцијама БиХ да донесу свој интерни акт у којем ће дефинисати **правила/процедуре о коришћењу преносних уређаја.**

ЛИТЕРАТУРА:

1. Политика управљања информационом безбједношћу у институцијама Босне и Херцеговине за период 2017-2022. године ("Службени гласник БиХ", број 38/17)
2. Стандард ISO/IEC 27001 - Безбједносне технике - Системи за управљање безбједношћу информација - Захтјеви
3. Стандард ISO/IEC 27002 - Безбједносне технике - Правило добре праксе за контроле безбједности информација
4. Закон о заштити тајних података ("Службени гласник БиХ", бр. 54/05 и 12/09)

385

Na osnovu člana 17. Zakona o Vijeću ministara Bosne i Hercegovine ("Službeni glasnik BiH", br. 30/03, 42/03, 81/06, 76/07, 81/07, 94/07 i 24/08), a u vezi sa članom 8. stav (2) tačka e) Zakona o finansiranju institucija Bosne i Hercegovine ("Službeni glasnik BiH", br. 61/04, 49/09, 42/12, 87/12, 32/13 i 38/22) i Uputstva o načinu planiranja, odobravanja i realiziranja višegodišnjih projekata u institucijama Bosne i Hercegovine ("Službeni glasnik BiH", br. 77/21), Vijeće ministara Bosne i Hercegovine na 3. sjednici, održanoj 23. februara 2023. godine donijelo je

ODLUKU
O ODOBRAVANJU VIŠEGODIŠNJEG PROJEKTA "IZGRADNJA GRANIČNIH PRIJELAZA ČEPIKUĆE I BROD"

Član 1.
(Predmet Odluke)

(1) Ovom Odlukom odabrava se višegodišnji projekat "Izgradnja graničnih prijelaza Čepikuće i Brod", procijenjene vrijednosti 2.000.000 KM.
(2) Sredstva iz stava (1) ovog člana će se realizirati kroz višegodišnji projekat "Izgradnja graničnih prijelaza Čepikuće i Brod" koji će se uvrstiti u Program višegodišnjih ulaganja za period 2023.-2024. godina u vrijednosti 2.000.000 KM i ista će se rasporediti na ekonomskom kodu 8212-nabavka objekata.

Član 2.
(Izvor flnansiranja i dinamika realizacije)

Projekat iz člana 1. ove Odluke finansirat će se iz sredstava Budžeta institucija Bosne i Hercegovine i međunarodnih obaveza Bosne i Hercegovine u sljedećim fazama:

a) 2023. godina 750.000 KM,
b) 2024. godina 1.250.000 KM,

i ista će se, u okviru višegodišnjeg projekta, rasporediti na budžetskoj poziciji 8212-nabavka građevina.

Član 3.
(Namjena sredstava)

Sredstva iz člana 1. ove odluke u ukupnom iznosu od 2.000.000 KM su namijenjena za:

a) Izgradnju graničnog prijelaza Čepikuće 1.000.000 KM,
b) Izgradnju graničnog prijelaza Brod 1.000.000 KM.

Član 4.
(Ažuriranje Pregleda višegodišnjih projekata, izvještavanje i praćenje realizacije)

(1) Uprava za indirektno oporezivanje će na osnovu ove Odluke sa Ministarstvom finansija i trezora Bosne i Hercegovine vršiti ažuriranje Pregleda višegodišnjih projekata u Budžetu institucija Bosne i Hercegovine i međunarodnih obaveza Bosne i Hercegovine svake godine.
(2) Praćenje realizacije ovog višegodišnjeg projekta vršit će se preko posebno otvorenog projektnog koda u Informacionom sistemu finansijskog upravljanja (ISFU).
(3) Po okončanju realiziranja projekta Uprava za indirektno oporezivanje konačan izvještaj o realizaciji projekta dostavit će Vijeću ministara Bosne i Hercegovine najkasnije 30 dana nakon završetka projekta, a Ministartsvu finansija i trezora uz godišnji izvještaj o izvršenju budžeta.