РЕПУБЛИКА СРБИЈА
Министарство омладине и спорта
Број: 404-02-00066/2021-02
Датум: 29. октобар 2021. године
Б е о г р а д

ДОКУМЕНТАЦИЈА ЗА УЧЕШЋЕ У НАБАВЦИ БЕЗ ПРИМЕНЕ ЗАКОНА О ЈАВНИМ НАБАВКАМА Н 37/2021 – АКТ О ИНФОРМАЦИОНОЈ БЕЗБЕДНОСТИ

Београд, октобар 2021. године

На основу члана 92. а у вези са чланом 27. став 1. тачка 1) Закона о јавним набавкама ("Сл. гласник Републике Србије" број 91/19),

лице за спровођење поступка прикупљањем понуда, издаје

П О З И В
за достављање понуда ЈН 37-2021

ПОДАЦИ О НАРУЧИОЦУ:
Наручилац: Министарство омладине и спорта
Адреса: Булевар Михајла Пупина 2, Нови Београд
Интернет страница: www.mos.gov.rs
Врста Наручиоца: Јавни наручилац
Мат. бр. 17693719
ПИБ: 105004944
e-mail: javnenabavke@mos.gov.rs
Особа за контакт: Жељка Љубојевић

Позивамо вас да доставите понуду за набавку услуге акта о информационој безбедности Н 37/2021, а у складу са спецификацијом која се налази у прилогу овог позива.

Понуду доставити на обрасцу који се налази у прилогу овог позива. Обавезно попунити све податке у обрасцу и потписати.

Услови плаћања: на текући рачун испоручиоца у року од најдуже 45 дана од дана пружања услуге, а према испостављеној исправној фактури. Рачун се испоставља у динарима.

Критеријум за избор најповољније понуде је економски најповољнија понуда.

Рок за достављање понуда: **5. новембар 2021. године до 12,00 часова,** без обзира на начин подношења понуде.

Начин достављања понуда: електронским путем на е-маил адресу: javnenabavke@mos.gov.rs или на адресу: Министарство омладине и спорта, Булевар Михајла Пупина 2, Нови Београд

Наручилац ће потврдити пријем понуде електронским путем.

ПОПУЊАВА ПОНУЂАЧ
(понуду потписати и оверити печатом)

ОБРАЗАЦ ПОНУДЕ

број _____

ОПИС ПРЕДМЕТА НАБАВКЕ: акт о информационој безбедности

ОБРАЗАЦ ПОНУДЕ Н 37/2021

Понуђач подноси понуду: 1) САМОСТАЛНО; 2) ЗАЈЕДНИЧКИ; 3) СА ПОДИЗВОЂАЧЕМ

Пословно име и седиште понуђача:	
Деловодни број понуде и датум понуде:	
Име особе за контакт:	
e-mail:	
Телефон и факс:	
ПИБ: Матични број:	
Назив банке и број рачуна:	
Лице овлашћено за потпис уговора:	
Величина привредног субјекта (микро, мало, средње или велико привредно друштво):	
Рок важности понуде (не мање од 30 дана):	
Предмет понуде:	Акт о информационој безбедности
Укупно без ПДВ-а	
Укупно са ПДВ-ом	
Начин и рок плаћања у данима од дана пријема рачуна:	месечно, у року __ дана од дана испостављања рачуна и извештаја о извршеним услугама

Место: _____

Датум: _____

М.П.

Понуђач

_____

Напомена:
Образац понуде понуђач мора да попуни, овери печатом и потпише, чиме потврђује да су тачни подаци који су у обрасцу понуде наведени. Уколико понуђачи подносе заједничку понуду, група понуђача може да се определи да образац понуде потписују и печатом оверавају сви понуђачи из групе понуђача или група понуђача може да одреди једног понуђача из групе који ће попунити, потписати и печатом оверити образац понуду.

Техничка спецификација

Техничка спецификација и технички опис услуга:

Како су 24. новембра 2016. у Службеном гласнику Републике Србије број 94/2016 објављени:

- Уредба о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја;
- Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, те да је законски рок 90 дана за израду Акта о безбедности ИКТ система од посебног значаја у складу са тачком 8. Закона о инфрмационој безбедности (Сл. гласник РС бр. 07/2016) потребно је да Наручилац изради наведени Акт.

Израда акта треба да обухвати следеће активности:

1. GAP анализу усклађености са Законом о информационој безбедности и актуелног стања информационо-комуникационе (ИКТ) инфраструктуре Наручиоца.

2. Процену ризика по безбедност информација код Наручиоца и израду извештаја о процени ризика са одговарајућим препорукама за усклађивање са Законом о безбедности информација.

3. Израду Акта о безбедности ИКТ система Наручиоца у складу са чл. 8. став 1. Закона.

ДЕТАЉНИЈИ ОПИСИ ТАЧАКА

1. GAP анализа усклађености са Законом о информационој безбедности

GAP анализа утврђује који је степен усклађености система руковођења безбедношћу информација код Наручиоца са захтевима Закона о информационој безбедности, а у светлу захтева међународног стандарда ISO/EC 27001:2013.

GAP анализа треба да одговори на питање колики је степен уређености, управљивости и унапредивости система руковођења безбедношћу информација код Наручиоца, односно:

- Колико је постојећи систем прописан и подржан документованим доказима;
- Колико се ослања на најбољу светску праксу увођења, коришћења, одржавања и унапређивања система руковођења утврђену кроз захтеве међународног стандарда ISO/EC 27001:2013 и
- Колико се документовани докази користе за унутрашње проверавање система и спровођење мера отклањања грешки и мера за предупређење проблема.

GAP анализа као један од резултата треба да прикаже време и неопходна средства за евентуално касније потврђивање (сертификовање) система руковођења безбедношћу информација према зхтевима међународног стандарда ISO/EC 27001:2013 од стране овлашћеног (акредитованог) тела према некој међународној шеми акредитације.

2. **Израда извештаја о процени ризика са одговарајућим препорукама за усклађивање са Законом о безбедности информација**

Извештај о процени ризика треба да садржи попис свих актуелних опасности по безбедност информација за сваку врсту делова ИКТ система Наручиоца уз оцену које су унутрашње и спољашње околности које су опредељујуће важне, утичу на постизање постављених циљева, као и опасности, тј. утицај с обзиром на: учинак, значај и изложеност опасности.

Извештај третира захтеве међународног стандарда ISO/IEC 27001:2013 у погледу:
(а) осигурања достизања планираних резултата,
(б) спречавања, односно смањења до прихватљивог нивоа, нежељених дејстава и
(в) постизања сталног побољшања;

На основу овог Извештаја и Извештаја GAP анализе Наручилац треба да добије препоруке које мере заштите треба да спроведе;

Извештај о процени ризика прати и План поступања са ризиком по безбедност информација обзиром на предложене мере заштите сагласно Додатку А стандарда ISO/IEC 27001:2013, односно чл. 7. Закона о информационој безбедности.

3. **Израда Акта о безбедности ИКТ система Наручица у складу са чл. 8. став 1. Закона о информационој безбедности**

Актом о безбедности ИКТ система од посебног значаја утврђују се мере, а нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система од посебног значаја.

Начела постизања и одржавања адекватног нивоа безбедности ИКТ система

Приликом израде Акта о безбедности ИКТ система треба се руководити следећим начелима:

1. **Начело управљања ризиком** - избор и ниво примене мера се заснива на процени ризика, потреби за превенцијом ризика и отклањања последица ризика који се остварио, укључујући све врсте ванредних околности;

2. **Начело свеобухватне заштите** - мере се примењују на свим организационим, физичким и техничко-технолошким нивоима, као и током целокупног животног циклуса ИКТ система;

3. **Начело стручности и добре праксе** - мере се примењују у складу са стручним и научним сазнањима и искуствима у области информационе безбедности;

4. **Начело свести и оспособљености** - сва лица која својим поступцима ефективно или потенцијално утичу на информациону безбедност треба да буду свесна ризика и поседују одговарајућа знања и вештине.

Акт о безбедности ИКТ система треба да попише које мере заштите ИКТ система се уводе код Наручиоца, а које се изузимају, уз образложење изузимања ако су изузете, и то за следеће области:

- Успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система;
- Постизање безбедности рада на даљину и употребе мобилних (преносивих) уређаја;
- Обезбеђивање да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који раде и разумеју своју одговорност;
- Заштита од ризика који настају при променама послова или престанка радног ангажовања лица запослених код оператора ИКТ система;
- Идентификовање информационих добара и одређивање одговорности за њихову заштиту;
- Класификовање података;
- Заштита носача података;
- Ограничење приступа подацима и средствима за обраду података;
- Одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа;
- Утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију;
- Предвиђање одговарајуће употребе криптозаштите ради заштите тајности, аутентичности односно интегритета података;
- Физичка заштита објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему;
- Заштита од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава која чине ИКТ систем;
- Обезбеђивање исправног и безбедног функционисања средстава за обраду података;
- Заштита података и средства за обраду података од злонамерног софтвера;
- Заштита од губитка података;
- Чување података о догађајима који могу бити од значаја за безбедност ИКТ система;
- Обезбеђивање интегритета софтвера и оперативних система;
- Заштита од злоупотребе безбедносних слабости ИКТ система;
- Обезбеђивање да активности на ревизији ИКТ система имају што мањи утицај на функционисање система;
- Заштита података у комуникационим мрежама укључујући уређаје и водове;
- Безбедност података који се преносе унутар оператора ИКТ система, као и између оператора ИКТ система и лица ван оператора ИКТ система;
- Питања информационе безбедности у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система;
- Заштита података који се користе за потребе тестирања ИКТ система односно делова система;
- Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга;
- Одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга;

- Превенција и реаговање на безбедносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама;
- Мере које обезбеђују континуитет обављања посла у ванредним околностима.

Рок плаћања: до _____ дана од дана извршења услуге;

Период на који се јавна набавка набавка врши: 12 месеци.

МОДЕЛ УГОВОРА
(попуњен, оверен и потписан)

НАРУЏБЕНИЦА Н 37/2021
УГОВОР
АКТ О ИНФОРМАЦИОНОЈ БЕЗБЕДНОСТИ

закључен дана _____ новембра 2021. године, у Београду, између:

1. Министарства омладине и спорта, Булевар Михајла Пупина 2, Нови Београд које заступа министар Вања Удовичић (у даљем тексту: наручилац), с једне стране

   и

2. _____ кога заступа _____ (у даљем тексту: добављач), с друге стране, како следи:

Члан 1.

Уговарачи констатују:

– да је наручилац, на основу члана 27. Закона о јавним набавкама („Службени гласник РС", број 91/19) спровео поступак прикупљања понуда;

– да је добављач доставио понуду, која у потпуности одговара спецификацијама из конкурсне документације;

Члан 2.

Предмет Уговора су – услуге акта о информационој безбедности у складу са правилима и стандардима струке и одредбама овог Уговора.

Члан 3.

Уговорена цена износи _____ динара, без ПДВ-а, односно _____ динара, са ПДВ-ом **(попуњава понуђач).**

Уговорена цена је фиксна и не може се мењати до коначног испуњења Уговора.

Уговорена цена обухвата све зависне трошкове које Добављач има.

Члан 4.

Добављач ће услуге из члана 2. овог Уговора извршити у року од _____ дана **(попуњава понуђач)** од дана од испостављања захтева за услугом.

Члан 5.

Наручилац се обавезује да пружене услуге плати у року од _____ дана од дана пријема потписане и оверене фактуре од стране Добављача.

Уз рачун Добављач ће доставити и документ о пријему.

Добављач је дужан да достављену фактуру пре испостављања Наручиоцу, региструје у регистру фактура који води Управа за трезор Министарства финансија.

Плаћање ће се извршити на текући рачун Добављача број _____ код банке _____ **(попуњава понуђач).**

Наручилац има право да у случају немогућности плаћања на начин који је прописан у ставу 1. овога члана, а из разлога који не зависе од његове воље (као што је привремена обустава плаћања иницирана од Управе за трезор због проблема са ликвидношћу буџета и сл.), плаћање изврши након престанка насталих објективних околности, и то у најкраћем року.

Обавезе које доспевају у наредној буџетској години биће реализоване највише до износа средстава која ће за ту намену бити одобрена у тој буџетској години.

Члан 6.

Добављач гарантује Наручиоцу да је квалитет услуга изнад стандардног тј. у складу са спецификацијом.

Члан 7.

Свака од уговорних страна може једнострано раскинути уговор у случају када друга страна не испуњава или неблаговремено испуњава своје уговором преузете обавезе, без отказног рока.

О намери да раскине уговор из других разлога, уговорна страна је дужна писаним путем обавестити другу страну.

У случају из става 2. овог члана, уговор ће се сматрати раскинутим од дана пријема писаног обавештења.

Члан 8.

За све што није предвиђено овим Уговором, примењиваће се одредбе Закона о облигационим односима.

Члан 9.

Све евентуалне спорове уговорне стране ће решавати споразумно. У немогућности споразумног решавања спора, спор ће се решити пред Привредним судом у Београду.

Члан 10.

Уговор производи правна дејства даном потписивања обе уговорне стране.

Члан 11.

Овај уговор сачињен је у четири примерка, од којих свака уговорна страна задржава по два примерка.

Добављач

_____

Наручилац

_____

Вања Удовичић