Акт о безбедности информационо-комуникационог система Врховног суда

Напомена

Овај документ је власништво организације и његов садржај не сме се саопштавати неовлашћеним особама, или особама ван организације без писане сагласности менаџера безбедности. Документ је обавезан за примену. Дужност сваког запосленог на кога се документ односи је да се са истим упозна и поступа на прописан начин. Обавезна је примена свих упутстава и записа који су дефинисани овим документом.

Историјат измена

Верзија	Датум	Израдио документ	Власник документа
в1.0	15.03.2024	Слободан Шолајић	Врховни суд

Преиспитивање документа

Датум следећег заказаног преиспитивања
15.03.2025. године

Дистрибуција

Назив	Наслов
Судска управа	Председник суда
Секретаријат суда	Секретар суда
Писарнице	Управитељ писарнице
Рачуноводство	Руководилац службе
Служба за ИКТ	Руководилац службе, свим запосленима у служби
Остали	Свим судијама и запосленима

Одобрио

Име	Позиција	Потпис	Датум
Јасмина Васовић	Председник суда		15.03.2024

Садржај

1 Увод

На основу члана 8. став 1. Закона о информационој безбедности („Службени гласник РС”, број 6/16, 94/17 и 77/19), чл. 2. и 3. Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја („Службени гласник РС”, број 94/16), Врховни суд доноси **Акт о безбедности информационо-комуникационог система (АБИКТ)**, заједно са свим документованим информацијама (документима и записима) који су организовани **у пакетима фолдера од Z5 до Z10 и од A6 до A17**, све у складу са најбољом праксом српског и међународног стандарда SRPS ISO/IEC 27001.

Као модеран, окренут ка будућем пословању, Врховни суд, је препознао потребу да се пословне операције обављају безбедно и без прекида, од чега имају корист грађани, корисници услуга, руководство, али и све друге заинтересоване стране.

Актом о безбедности информационо-комуникационог система, у складу са Законом о информационој безбедности, ближе се уређују мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима информационо-комуникационог система.

Како би обезбедио такав ниво безбедности информација, Врховни суд је имплементирало Акт о безбедности ИКТ система од посебног значаја (у даљем тексту АБИКТ) у складу са Законом о информационој безбедности и према међународном и домаћем стандарду за информациону безбедност SRPS ISO/IEC 27001.

Пословање у складу са АБИКТ има бројне користи за пословање, међу којима су:

- Заштита пословања Врховног суда у целини
- Безбедна достава услуга корисницима и државним органима
- Одржавање и јачање значаја Врховног суда
- Усаглашеност са захтевима закона и прописа

Важно је разумети које области пословања су обухваћене у оквиру АБИКТ, а које су из њега искључене. Намена овог документа је да дефинише општу политику везану за безбедност информација, која одговара потребама и која укључује:

- Оквир за постављање циљева безбедности информација
- Посвећеност испуњавању захтева
- Посвећеност континуираном побољшавању АБИКТ

АБИКТ је доступан и у папирној и у електронској форми и биће прослеђен запосленима у оквиру организације, као и свим заинтересованим трећим странама.

2 Постављање циљева безбедности информација

Главни циљеви безбедности информација у организацији од кључног су значаја за пословање и њих не треба често мењати.

Главни приоритети којима мора да се бави АБИКТ, нарочито у сагледавању потенцијалних последица, дати су у оквиру следећих циљева:

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

Успешност АБИКТ оцењиваће се на основу успешности испуњавања ових циљева.

Ови општи циљеви биће смернице за креирање циљева нижег нивоа, краткорочних циљева креираних током годишњег планирања безбедности информација чији се временски оквир поклапа са планирањем буџета организације. На овај начин ће се обезбедити одговарајућа средства за идентификоване активности за побољшање, и ови краткорочни циљеви ће се креирати на основу јасног разумевања општих циљева и захтева пословања, и пратиће се начин на који они могу да се мењају током године.

Циљеви безбедности информација документоваће се у оквиру финансијског плана за дату фискалну годину, заједно са детаљима плана њиховог постизања. Једном одобрен, овај план ће се преиспитивати годишње у оквиру процеса преиспитивања од стране руководства, током ког ће се преиспитивати и циљеви, како би се обезбедила њихова валидност. Уколико су неопходне измене, њима ће се управљати преко процеса управљања променама у организацији.

3 Посвећеност испуњењу примењивих захтева

Посвећеност испуњењу безбедности информација обухвата највише нивое организације, а демонстрира се кроз овај АБИКТ и обезбеђивање адекватних ресурса за постављање и развој АБИКТ.

Судска управа ће се побринути да се редовно спроводи систематско преиспитивање мера у оквиру АБИКТ, како би се потврдило испуњење циљева безбедности информација и како би се преко аудита и процеса управљања идентификовала питања везана за безбедност. У оквиру АБИКТ, постоји неколико главних улога које треба доделити, како би се обезбедио успех и заштитило пословање од ризика информационе безбедности.

Менаџер за информациону безбедност је главни одговорни и овлашћени за имплементацију и управљање АБИКТ, нарочито за:

- Идентификацију, документовање и испуњење примењивих захтева прописа из области информационе безбедности
- Додељивање овлашћења и одговорности за имплементацију, управљање и побољшавање АБИКТ
- Интеграцију пословних процеса са АБИКТ
- Усаглашеност са законским, регулаторним и уговорним захтевима везаним за безбедно управљање коришћеним ИКТ средствима
- Обавештавање највишег менаџмента о перформансама и побољшањима АБИКТ

Одговорност **Менаџера за информациону безбедност** је да се побрине да запослени разумеју улоге које треба да испуне и да имају одговарајуће вештине и компетентности за њихово извршавање.

Организација ће се побринути да су запослени одговорни за управљање безбедношћу информација компетентни, на основу одговарајућег образовања, обуке, вештина и искуства (нпр. интерни и водећи аудитори према светски акредитованим програмима персоналне обуке и сертификације итд.).

Вештине неопходне да би се успоставила и одржавала безбедност информација одредиће се и редовно преиспитивати заједно са проценом постојећих нивоа вештина у организацији. Потребе за обуком ће се идентификовати, а план одржавати, како би се обезбедило постојање потребних компетенција.

Секретаријат суда интерно води записе о обукама, образовању и осталим релевантним записима, како би све индивидуалне вештине биле документоване.

Детаљи о одговорностима повезаним са сваком од неопходних улога и на који начин су оне додељене у оквиру организације налазе се у посебном документу под називом **Улоге, одговорности и овлашћења**.

Организација користи различите треће стране, интерно и екстерно, за испоруку услуга својим корисницима и државним органима. Када ово подразумева обављање пословног процеса, или дела пословног процеса, који је у склопу дефинисаног подручја примене АБИКТ, тада се то контролише и прати од стране организације и **Менаџера за информациону безбедност**.

У сваком случају организација задржава управљање над релевантним процесима, које спроводе треће стране, демонстрирајући:

- Одговорност за процес
- Контролу дефиниције процеса и интерфејса са процесом
- Праћење перформанси и усаглашености
- Контролу над побољшањем процеса

Ово ће бити подржано документованим информацијама (документима и записима) преко уговора, записа са састанака и извештаја о перформансама.

4 Континуирано побољшавање АБИКТ

Активности организације које се односе на континуирано побољшавање АБИКТ упућују на:

- Континуирано побољшавање ефективности АБИКТ у свим областима
- Побољшавање постојећих процеса, како би се ускладили са добром праксом дефинисаном у SRPS ISO/IEC 27001
- Повећање степена проактивности (и пословне перцепције проактивности) уз осврт на постојећу безбедност информација
- Постизање и повећање разумевања и бољег односа између организационих јединица у којима се примењује АБИКТ
- Прикупљање идеја за побољшавање преко редовних састанака на којима се врши преиспитивање, и њихово документовање у **Процедури континуираног побољшавања - корективне мере**
- Стицање у перспективи ISO/IEC 27001 сертификата за организацију и његово редовно обнављање (ресертификација)

Идеје за побољшавање могу доћи из различитих извора, укључујући државне органе, кориснике, добављаче, запослене, процене ризика и аудите. Када се идентификују, идеје се додају у **Процедуру континуираног побољшавања - корективне мере**.

Током оцењивања предложених побољшавања користиће се следећи критеријуми:

- Трошкови
- Пословне користи
- Ризик
- Временски оквир имплементације
- Потребни ресурси

Уколико се прихвати, предлогу побољшавања биће додељен приоритет, како би се омогућило ефективно планирање. За више детаља погледати документ **Процедура за континуирано побољшавање - корективне мере**.

5 Приступ управљању ризиком

Користиће се стратегија и процес управљања ризиком који су у складу са захтевима и препорукама ISO/IEC 27005, међународним и домаћим стандардом за управљање ризицима по безбедност информација. Ово подразумева идентификовање релевантних средстава (информационе имовине) и узимање у обзир следећих аспеката:

- Претње
- Рањивости
- Утицај и вероватноћа пре третирања ризика
- Третирање ризика
- Утицај и вероватноћа након третирања ризика
- Власник ризика/власник средства
- Временски оквир и учесталост преиспитивања

Управљање ризиком обављаће се на неколико нивоа у оквиру АБИКТ, укључујући:

- Планирање безбедности информација – ризици постизања циљева
- Процена ризика по безбедност информација
- Процена ризика по континуитет пословања у контексту информационе безбедности
- Процена ризика промена као део процеса управљања пословним променама

Процена значајних ризика вршиће се једном годишње или након значајних промена у пословном окружењу. За више детаља о приступу процени ризика погледати документ **Методологија управљања ризиком**.

Од кључног значаја је спровођење редовне провере о томе колико се поштују процедуре и процеси безбедности информација. Ово ће се обављати на два нивоа:

1. Интерни аудит према стандарду SRPS ISO/IEC 27001 од стране тима за имплементацију, одржавање и побољшање АБИКТ

2. Екстерни, сертификациони аудит треће стране, према стандарду, како би се потврдила усаглашеност са SRPS ISO/IEC 27001 (у перспективи добио и сачувао сертификат ISO/IEC 27001)

Детаљи о томе како ће се спроводити интерни аудити могу се наћи у **Процедури интерне провере**.

6 Контрола документованих информација (докумената и записа)

Све документоване информације у вези са безбедношћу информација које чине део АБИКТ морају бити креиране тако да се њима управља током животног циклуса, на начин приказан у **Правилнику за израду интерних аката**.

Сви документи у АБИКТ имају јединствени број и прате се текуће (важеће) верзије – погледати документ **Списак докумената**.

Чување записа представља основни део АБИКТ континуитета пословања. Записи представљају кључни извор информација и доказ да се процеси ефикасно спроводе – погледати документ **Преглед записа**. Контроле за управљање записима дефинисане су у документу **Правилник за израду интерних аката**.

7 Примена Акта о безбедности информационо-комуникационог система Врховног суда

Акт о безбедности информационо-комуникационог система Врховног суда ступа на снагу 8 дана од дана доношења и оглашавања на огласној табли Врховног суда, а примењује се од 16. маја 2024. године.