РЕПУБЛИКА СРПСКА
КАЗНЕНО-ПОПРАВНИ ЗАВОД ДОБОЈ

ПЛАН БЕЗБЈЕДНОСТИ ЛИЧНИХ ПОДАТАКА У КАЗНЕНО ПОПРАВНОМ ЗАВОДУ ДОБОЈ

Добој, октобар 2020. године.

На основу члана 11. став 4. Закона о заштити личних података („Службени гласник БиХ“ број: 49/06, 76/11 и 89/11), члана 6. Правилника о начину чувања и посебним мјерама техничке заштите личних података (Службени гласник БиХ“ број 176/09) и члана 19. Правилника о провођењу закона о заштити личних података у Казнено – поправном заводу Добој бр. 01-170-2992/20, директор Казнено-поправног завода Добој, д о н о с и,

ПЛАН БЕЗБЈЕДНОСТИ ЛИЧНИХ ПОДАТАКА
КАЗНЕНО - ПОПРАВНОГ ЗАВОДА ДОБОЈ

I - ОПШТЕ ОДРЕДБЕ

Члан 1.
(Предмет плана)

Планом безбједности личних података прописују се неопходне ефективне безбједносне мјере у поступку обраде, преноса и чувања личних података, те се ближе уређују посебни организациони и технички видови заштите личних података у Казнено – поправном заводу Добој (у даљем тексту КПЗ Добој).
Планом безбједности личних података одређују се мјере, средства и услови чувања, обезбјеђења, заштите и преноса посебних категорија личних података и збирки таквих података, мјере одржавања и провјере исправности рада рачунарске, телекомуникационе и програмске опреме система за вођење збирки посебних категорија личних података, обезбјеђење радних просторија у којима је смјештена та опрема, лица овлаштена за провођење предвиђених мјера, те лица одговорна за надзор над провођењем тих мјера.

Члан 2.
(**Циљ плана)**

Циљ мјера Плана безбједности (у даљем тексту: План) је заштита личних података који се обрађују, преносе, те података сачуваних у збиркама личних података КПЗ Добој од случајног или бесправног уништавања, или случајног губитка, неовлаштеног приступа, измјена података и сл., као и откривање, те истрагу таквих случајева.

Члан 3.
(**Садржај плана безбједности)**

1) План садржи категорије личних података које се обрађују и попис инструмената заштите односно организационе и техничке мјере заштите којима се обезбјеђује:

а) **повјерљивост** - да само лица овлаштена за то могу имати приступ личним подацима,
б) **интегритет** - да за вријеме обраде, лични подаци остану непромијењени, потпуни и ажурни,
ц) **расположивост** - да су подаци стално доступни, да су на располагању и да се могу исправно обрађивати,
д) **аутентичност** - да се у свако доба може утврдити поријекло личних података,

е) **могућност ревизије** - да се може утврдити ко, када, које је личне податке и на који начин обрађивао,
ф) **транспарентност -** да је поступак при обради личних података потпун, ажуран и на одговарајући начин евидентиран,

2) План је сачињен у писменој форми, редовно се ажурира и стално је доступан Агенцији за заштиту личних података Босне и Херцеговине.

Члан 4.
(Повјерљивост)

1) Запослени у КПЗ Добој могу имати приступ личним подацима који се обрађују, само уколико у опису радног мјеста на које су распоређени произилази потреба приступа личним подацима, односно збиркама личних података који се обрађују у КПЗ Добој, односно ако се ради о електронској обради посједују корисничко име и приступну шифру додјељену на начин и по поступку који је прописан овим Планом.

2) Изузетно, запослени у КПЗ Добој могу приступати личним подацима уколико им то не произилази из описа радног мјеста на које су распоређени, уколико се таква потреба појави у вези са извршавањем редовних послова.

3) Запослени КПЗ Добој из става (2) овог члана, морају имати посебно одобрење директора, одобрење мора садржавати јасну назнаку који подаци односно збирке личних података се могу обрађивати, у случају приступа електронским подацима додијелит ће им се приступно корисничко име и шифра који ће важити само за одређени период назначен одобрењем из става (3) овог члана.

Члан 5.
(Интегритет)

1) Запослени у КПЗ Добој који обрађују личне податке дужни су правовремено ажурирати податке, на основу релевантне документације.

2) Обавеза запослених КПЗ Добој је да ажурирају податке у евиденцијама које се воде у оквиру КПЗ Добој у складу са Законом о заштити личних података („Службени гласник БиХ“ број: 49/06) и Правилником о провођењу закона о заштити личних података у Казнено-поправном заводу Добој.

Члан 6.
(Расположивост)

Запослени КПЗ Добој дужни су податке из збирке личних података коју обрађују, чинити доступним и на располагању, како за друге службенике, тако и за друге организационе јединице КПЗ Донбој и остале кориснике изван КПЗ Добој, а у складу с чланом 17. Закона о заштити личних података и Законом о извршењу кривичних и прекршајних санкција РС (у даљем тексту, ЗИКПС).

Члан 7.
(Аутентичност)

1) Запослени КПЗ Добој који обрађују податке дужни су водити рачуна о поријеклу личних података, информације о поријеклу могу бити:

а) непосредно од носиоца података,

б) преузимањем из других збирки личних података који се воде,

ц) добијањем података од трећег лица коју треба навести именом, презименом и другим подацима на основу којих се лице може идентификовати,

д) властитим опажањем или истраживањем и

е) из неких других извора које треба поближе навести.

Члан 8.
(Могућност ревизије)

1) Ревизијом се обезбјеђује поступак провјере законитости обраде личних података, у којем је накнадно могуће утврдити који је запослени КПЗ Добој обрађивао личне податке, датум обраде, који лични подаци су обрађени и на који су начин обрађени.

2) Обрада личних података у смислу става 1) овог члана подразумијева да запослени КПЗ Добој који обрађују податке у евиденцију уписују своје личне податке на основу којих се могу идентификовати, датум обраде, податке односно збирке личних података које су обрађивали, на који начин су их обрадили, те правни основ као и број и датум акта на основу којег су вршили обраду личних података.

3) Уколико се врши обрада података електронским путем, систем ће омогућити похрану података о службенику који је обрађивао личне подаке на начин како је то прописано у ставу (1) овог члана.

Члан 9.
(Значење израза)

Изрази који се користе у овом Плану имају исто значење као у Закону.

Члан 10.
(Принципи заштите личних података)

1) Заштита личних података у КПЗ Добој, заснована је на принципима познатим као ААА, који подразумијева три елемента заштите.

а) Прво А је **овјера** (authentication) - поступак утврђивања идентитета лица које жели да приступи личним подацима, односно провјери тог идентитета. Услов за утврђивање аутентичности јесте посједовање неког легитимационог знака, предмета или уређаја. Аутентичност се утврђује коришћењем информације која је позната само кориснику и лицу или елементу система које врши провјере

аутентичности. То су: комбинација корисничког имена и лозинке или кодови који се користе приликом пријаве.

б) Друго А је **ауторизација** (aуthorizacion), што подразумијева дефинисање корисника или групе корисника који имају право приступа одређеном скупу личних података (ако се они воде ручно) или информационо-комуникационом систему, односно његовим дијеловима, утврђујући до којих личних података могу приступити конкретни овлаштени корисници и шта са тим подацима могу да раде (преглед, измјена, додавање и брисање).

в) Треће А је **праћење** (accountebility) и представља најважнији елемент. Он подразумијева заштиту личних података тако уређену и организовану да је у сваком тренутку, накнадно могуће утврдити када су поједини подаци обрађивани и ко је то урадио. Постоје три нивоа праћења. Први ниво омогућава накнадно утврђивање чињеница о томе ко је уносио, прегледао, промијенио, односно избрисао неки податак и када. Други ниво подразумијева праћење приступа подацима, нпр. ко и када је одређеном податку само приступио (увид, упознавање), али при томе није вршио никакве измјене. Трећи ниво обухвата потпуно праћење у коме се евидентира све: ко и када је приступио подацима или је мијењао податке, какав је податак био и у шта је промијењен.

Члан 11.
(Врсте мјера заштите)

1) КПЗ Добој у циљу заштите личних података које обрађује предузима:

а) организационе мјере,

б) техничке мјере;

2) Организационе и техничке мјере заштите личних података се предузимају у свакој организационој јединици у којој се обрађују лични подаци у оквиру повјерених надлежности.

II - ОРГАНИЗАЦИОНЕ МЈЕРЕ ЗАШТИТЕ ЛИЧНИХ ПОДАТАКА

Члан 12.
(Облик збирки личних података)

1) Начин вођења збирки личних подака прописан је Правилником о провођењу закона о заштити личних података у Казнено-поправном заводу Добој.

2) КПЗ Добој води следеће збирке личних података:

а) Евиденција о запосленим у КПЗ Добој на основу Закона о раду („Службени гласник Републике Српске“ бр. 01/16 и 66/18) и Закона о извршењу кривичних и прекршајних санкција Републике Српске („Службени гласник Републике Српске“ бр. 63/18), (у даљем тексту ЗИКПС-а)

б) Евиденција о обрачуну и исплатама плата запослених у КПЗ Добој на основу Закона о платама запослених у институцијама правосуђа Републике Српске („Службени гласник Републике Српске“ бр 66/18, 54/19 и 105/19), (у даљем тексту Закон о платама),
в) Евиденција о притвореним лицима на основу Закона о извршењу кривичних и прекршајних санкција Републике Српске („Службени гласник Републике Српске“ бр. 63/18), Правилника о кућном реду за извршење мјере притвора („Сл. галасник РС“ бр. 58/20), Кривичним закоником Републике Српске („Сл. галасник РС“ бр. 64/17), и Законом о кривичном поступку Републике Српске („Сл. галасник РС“ бр. 53/12, 91/17, и 66/18) и Правилника о кућном реду за извршење мјере притвора („Сл. галасник РС“ бр. 58/20),

г) Евиденција о затвореницима у КПЗ Добој на основу Закона о извршењу кривичних и прекршајних санкција Републике Српске („Службени гласник Републике Српске“ бр. 63/18), Кривичног законика Републике Српске („Сл. галасник РС“ бр. 64/17), и Законом о кривичном поступку Републике Српске („Сл. галасник РС“ бр. 53/12, 91/17, и 66/18) и Правилника о кућном реду за издржавање казне затвора („Сл. галасник РС“ бр. 58/20),

Члан. 13.
(Вођење збирки личних података)

1) Директор одређује извршиоце обраде збирке личних података које се воде у организационим јединицама у КПЗ Добој.

2) Извршилац из става 1) овог члана је одговоран за чување збирки личних података, спречавање неовлаштеног приступа и коришћења, те увида у податке из збирке као и тачност и аутентичност података унесених у збирке.

Члан 14.
(Чување личних података)

Подаци у збиркама личних података које се воде у КПЗ Добој, чувају се у складу са Законом о заштити личних података („Сл. гласник БиХ“ бр. 63/18), Правилником о заштити личних података КПЗ Добој бр. 01-170-2992/20, Листом категорија регистарског материјала са роковима чувања у Казнено-поправном заводу Добој бр. 01-621-4037/16 од 26.12.2016. године, Законом о извршењу кривичних и прекршајних санкција („Сл. гласник РС“ бр. 63/18) Закону о слободи приступа информацијама („Сл. гласник РС“ бр. 20/01) и Правилником о начину чувања службене тајне („Сл. гласник РС“ бр.12/20).

Члан 15.
(Информисање и обука запослених)

1) КПЗ Добој ће провести план обуке запослених лица, којом ће се запослени упознати са правилима и процедурама у вези са заштитом личних података у поступку обраде, похрањивања и архивирања личних података како би се осигурало да је у сваком тренутку задовољен досљедно висок стандард безбједности код свих запослених.

2) Након пријема у радни однос, а прије отпочињања обављања радних дужности, свако лице које ће у оквиру послова и задатака обрађивати личне податке упознаје се са мјерама заштите личних података.

3) Прије непосредног отпочињања обављања послова везаних за обраду личних података, запослени се додатно упознају са конкретним обавезама по питању заштите личних податка.

Члан 16.
(Физичке мјере заштите просторија и опреме у којима се врши обрада личних података)

1) Све канцеларије у којима се обрађују и архивирају лични подаци, требају бити заштићене одговарајућим мјерама физичке заштите. Код одлучивања о степену потребне физичке сигурносне заштите, у обзир ће се узети релевантни фактори као што су:

а) категорија личних података;

б) количина и облик (штампане на папиру/ на медијима за компјутерско похрањивање);

ц) особље које обрађује информације;

д) како ће се архивирати информације.

2) Мјере физичке заштите су тако осмишљене да:

а) спријече недозвољен или насилан упад од стране неовлаштеног лица;

б) одврате, спријече и открију радње неовлаштеног лица;

ц) омогуће селекцију особља у погледу приступа личним подацима и

д) омогуће откривање и поступање у свим случајевима угрожавања безбједности што је прије могуће.

Члан 17.

(Физички надзор улаза и излаза лица)

1) Систем улазног надзирања осмишљен је тако да обезбјеђује потпуни надзор над улазом односно излазом лица у просторије сједишта КПЗ Добој, дозвољава улаз само лицима, које имају одговарајуће одобрење за приступ просторијама или које су запослене у КПЗ Добој, односно имају посебне дозволе за улазак у Установу путем система (centaur- контрола улаза и излаза).

2) Полицајци службе обезбјеђења у КПУ обезбјеђују службени улаз у просторије КПЗ Добој 24 часа дневно, 7 дана у седмици.

3) Прилаз КПЗ Добој и улаз у Установу покривен је системом видео надзора.

4) Прије уласка незапослених лица у просторије КПЗ Добој, полицајац службе обезбјеђења који надзире улазак у службене просторије КПЗ Добој, мора провјерити њихов идентитет и разлог уласка, као и испуњавање других услова за улазак у просторије КПЗ Добој.

5) Незапосленим лицима којима се дозвољава улазак у просторије КПЗ Добој, крећу се под надзором полиције до одређених просторија и даје им се до знања да је њихово кретање надзирано и евидентирано. Поступак надзирања и евиденције лица која долазе у установу прописано је на основу Закона о извршењу кривичних и прекршајних санкција Републике Српске.

6) Приступ просторијама гдје се чувају и обрађују лични подаци могућ је само у току редовног радног времена. Изван радног времена приступ службеним просторијама је могућ само запосленим лицима приликом обављања ванредних службених дужности, односно лицима у пратњи службене особе.

Члан 18.
(Просторије, ормари и касе)

1) Просторије у којима се обрађују лични подаци, не смију остајати без надзора и закључавају се за вријеме одсутности службених лица.

2) Збирке личних података, које се воде у писаном облику, похрањују се у канцеларијским или металним ормарима и касама.

3) Изван радног времена, ормари и писаћи столови са документима која садрже личне податке, морају бити закључани, а рачунари и друга машинска опрема искључени и физички или програмски закључани.

4) Није дозвољено остављати носаче личних података на столовима у присутности лица која немају права на приступ или увид тим подацима.

5) У просторијама, које су намијењене контактирању са странкама, документи који садрже личне податке и рачунарски монитори морају бити постављени тако, да странке не могу остварити увид у исте.

Члан 19.
(Спречавање неовлаштеног умножавања, копирања и преписивања личних података)

1) Личне податке могу умножавати, копирати или преписивати само лица која су задужена за обраду личних података у складу са потребама обављања редовних радних задатака.

2) Опрема за умножавање поставља се на мјестима чија је употреба под надзором лица овлаштених за обраду личних података или на мјестима покривеним видео надзором.

Члан 20.
(Уништавање докумената)

1) Лични подаци морају се уништавати на начин да се лични податак не може распознати и документ односно медиј који садржи лични податак не може обновити.

2) На исти начин уништава се помоћни и радни материјал (нпр. пробни односно неуспјешни исписи, прорачуни итд.) који се односи на личне податке који се уништавају.

3) Забрањено је одбацивање отпадних носача података са личним подацима у смеће.

4) Директор КПЗ ће одредити Комисију за уништавање докумената који садрже личне податке, која је дужна сачинити записник о уништавању. Комисију чине три члана, запослена у КПЗ Добој. Комисија ће, након што сачини записник, исти доставити директору на верификацију.

III - ТЕХНИЧКЕ МЈЕРЕ

Члан 21.
(Мјере техничке заштите)

1) КПЗ Добој обезбјеђује одговарајуће мјере техничке заштите просторија и опреме у којима се врши обрада личних података.

2) Техничке мјере заштите личних података, између осталог, обухватају контролу приступа просторијама и опреми за обраду личних података, заштиту од уништења и оштећења личних података и друго.

Члан 22.
(Видео надзор)

1) Службени улаз и ходници сједишта КПЗ Добој су покривени надзором видео система.

2) Систем видео надзора повезан је на „REC“ ормар са мониторима, снимачима видеозаписа смјештени су у надзорној сервер соби у једној просторији КПЗ Добој. Полицајци службе обезбјеђења обезбјеђују „REC“ ормар 24 сата, 7 дана у седмици. Систем видеонадзора има могућност архивирања података, како би се подаци могли ишчитати у случају да се за тим укаже потреба.

3) Виши стручни сарадник за информационе системе задужен је за похрањивање видео записа на преносиве медије, те њихово архивирање, заштиту од неовлаштеног брисања, те изузимање

одређених дијелова снимака, уколико се за тим укаже потреба, уз сагласност и по налогу директора.

Члан 23.
(Кључеви, касе-метални ормари и улазне картице)

1) Кључеви просторија у којима се налазе лични подаци, чувају се и употребљавају у складу са утврђеним правилима у КПЗ Добој.

2) Није дозвољено остављање кључева у брави са ванјске стране врата просторије у којој се врши обрада личних података.

3) Кључеви канцеларија у којима се обрађују лични подаци може имати само извршилац, а резервни ће се чувати у просторијама Службе обезбјеђења у металној каси, а могућност њиховог кориштења је ограничена за потребе администрирања личних података, за потребе особља које врши послове хигијенског одржавања просторија - чишћења, односно у случају вандредних ситуација и крајње нужде.

4) На просторијама, гдје постоје електронски контролори приступа, приступ имају само овлаштена лица, приступне картице имају сва запослена лица која у оквиру својих радних задатака имају потребу приступа просторијама у КПЗ Добој. Сви улази у КПЗ Добој покривени су камерама видеонадзора.

5) Приступне шифре на металним касам-ормарима и кључеве ће имати само лица задужена за похрањивање докумената у касу.

6) Картице улаза за запослене додјељују се и мјењају у случају:

а) по запослењу лица;

б) у случају откривања или сумње у копију или на други начин злоупотребу;

ц) када запосленом у КПЗ престане радни однос;

д) након тога када лице из прошлог става престаје обављати задатке у органу због којих је било упознато са постављеним комбинацијама и шифрама;

е) када тако одлучи директор КПЗ Добој;

6) Приступне шифре и картице ће бити депоноване код Вишег стручног сарадника за информационе системе у запечаћеној коверти и исте се похрањују на сигурно мјесто у складу са правилима заштите тајних података.

Члан 24.
(Посебне мјере заштите)

1) Посебне мјере заштите за телекомуникациону опрему и системе који су дефинисани и Упутство о праћењу видео надзора у КПЗ Добој обавезно је и:

а) У близини рачунарске и телекомуникационе опреме не смије бити извора јаког електричног или магнетског поља и извора јонизирајућег зрачења.

б) У близини опреме осјетљиве на електростатички електрицитет не смије бити извора таквог електрицитета.

в) У просторијама у којима је смјештена рачунарска и телекомуникациона опрема мора се одржавати релативна влажност ваздуха између 20 и 80% и температура између 5 и 30°Ц.

г) У просторијама и у близини просторија у којима је смјештена опрема система, не смију се налазити нагризајуће текућине, експлозивна средства и сличне опасне или штетне материје.

д) У просторијама у којима су смјештени рачунари не смију се налазити уређаји који у зрак испуштају честице прашине. Уређаји осјетљиви на прашину морају бити прописно заштићени.

ђ) Посебно осјетљиви уређаји који се хладе зраком, морају имати филтере за зрак.

е) Уређаји за које је то допуштено техничким упутствима, морају се покривати заштитним покривачима за вријеме када нису у употреби.

IV - ЗАШТИТА ЛИЧНИХ ПОДАТАКА У АУТОМАТСКОЈ ОБРАДИ

Члан 25.
(Техничке мјере)

1) КПЗ Добој при аутоматској обради личних података обезбјеђује техничке мјере заштите личних податка и то:

а) јединствено корисничко име и лозинку за пријаву на електронске евиденције састављену од обавезне комбинације минимум осам карактера, бројева или слова,

б) измјену лозинке по потреби,

ц) корисничко име и лозинка ће дозвољавати приступ до дијелова система потребних извршиоцу за извршење његових радних задатака,

д) аутоматско одјављивање са система по истеку одређеног периода неактивности, не дуже од 5 минута, а за поновно активирање система потребно је наново уписати корисничко име и лозинку;

е) аутоматску забрану приступа систему након три неуспјешна покушаја пријављивања на систем и аутоматско упозорење извршиоцу да потражи инструкцију од вишег стручног сарадника за информационе системе збирке личних података,

ф) ефикасну и сигурну антивирусну заштиту система, које ће се стално ажурирати ради превентиве од непознате или непланиране опасности од нових вируса;

г) компјутерска, програмска и остала неопходна опрема на електоренергетску мрежу се прикључује путем уређаја за непрекидно напајање (УПС и агрегат).

2) Запослени који обавља кадровске послове, дужан је да извјештава вишег стручног сарадника за информационе системе збирке личних података (о запосленим, платама запослених, притворених лица и затвореника) или ангажовању сваког извршиоца с правом приступа информационом систему, како би се додијелили корисничко име и лозинка, као и по престанку запослења или ангажовања, да би се корисничко име и лозинка избрисали односно забранио даљњи приступ.

3) Извјештавање из става 2. овог члана врши се и приликом било које друге промјене радног статуса извршиоца, која утиче на ниво или обим приступу збирке личних података.

Члан 26
(Корисничко име и лозинка)

1) Да би корисник приступио систему потребно је да има важећи кориснички налог и лозинку.

2) Кориснички налог је јединствен и један корисник може имати само један кориснички налог.

Члан 27.

1) Корисничка лозинка треба да садржи најмање 8 (осам) карактера, који представљају комбинацију великих и малих слова, те бројева. Корисник је дужан мијењати лозинку сваких 12 мјесеци и не смије је дијелити са другим службеницима.

2) Уколико корисник намјерава одсуствовати са посла, дужан је да све информације које би требао дијелити са другим службеницима омогући приступ само једном запосленом који ће га мјењати на тим пословима у његовом одсуству, а у случају потребе.

3) Лозинка не може садржавати име или презиме корисника, брачног друга, дјеце или било који други податак који се на очигледан начин могу довести у везу са корисником.

4) Службеник је дужан да памти своју лозинку и иста се не може записивати, а посебно не у близини рачунара.

5) У случају да корисник заборави своју лозинку потребно је да путем руководиоца организационе јединице поднесе захтјев за додјелу нове. Промјену лозинке врши виши стручни сарадник за информационе системе, који тај податак уписује у евиденцију-шифрарник.

Члан 28.
(Приступ систему)

1) Корисничко име и лозинка ће дозвољавати приступ само до дијелова система потребних извршиоцу за извршење његових радних задатака**-** привилеговани ниво**.**

2) Сваки улаз у систем ће бити аутоматски забиљежен корисничким именом, датумом и временом пријаве и одјаве**.**

Члан 29.
(Аутоматско одјављивање са система по истеку одређеног периода неактивности)

Када се корисници удаљавају од рачунара, дужни су обавезно да се одјаве са система.
виши стручни сарадник за информационе системе ће обезбједити аутоматско одјављивање са система по истеку одређеног периода неактивности, не дуже од 5 минута. За поновно активирање система потребно је наново уписати корисничко име и лозинку.

Члан 30.
(Аутоматска забрана приступа систему након три неуспјешна покушаја пријављивања)

1) Уколико се за било који налог, погрешна шифра унесе 3 пута, налог ће се аутоматски блокирати. Поступак за ресетовање лозинке је такав да је корисник дужан да вишем стручном сараднику за информационе системе, путем руководиоца организационе јединице поднесе захтјев за додјелу нове.

2) Промјену лозинке врши виши стручни сарадник за информационе системе.

Члан 31.
(Антивирусна заштита)

1) Информациони систем КПЗ Добој мора имати ефикасну и сигурну антивирусну заштиту система, која се редовно ажурира ради превентиве од непознате или непланиране опасности од нових вируса.

2) Антивирусни програм треба да спријечи инфекцију малициозним програмима (вирусима, црвима, тројанцима), односно да ублажи или потпуно санира последице њиховог дејства својим дјеловањем. Квалитет антивирусног програма се оцјењује на основу брзине скенирања, способности да открије вирусе, конфигурисања и ажурирања листе потписа познатих вируса.

Члан 32.

(Обавеза употребе уређаја за непрекидно напајање)

1) Рачунари за вођење збирки личних података и мрежно чвориште се прикључују на енергетску мрежу преко уређаја за непрекидно напајање (УПС). УПС уређај, у случају прекида или нестанка електричне енергије, омогућава несметан наставак рада рачунара и друге опреме кроз одређено кратко вријеме, тако да се послови у току могу завршити без опасности за комплетност информација које се тим рачунаром и опремом обрађују, а рачунар и друга опрема у том времену могу уредно угасити.

2) Уколико дође до нестанка електричне енергије у КПЗ Добој, аутоматски се пали агрегат који напаја електричну инсталацију до доласка електричне енергије кроз енергетску мрежу, након чега се агрегат аутоматски гаси.

3) Исправност и повремено паљење агрегата овлаштени радници врши једном у мјесец дана током године.

Члан 33.
(Организационе мјере)

1) КПЗ Добој при аутоматској обради личних података обезбјеђује организационе мјере заштите личних података и то:

а) потпуну тајност и безбједност лозинки и осталих форми за идентификацију приступа личним подацима;

б) организациона правила за приступ извршиоца интернету која се односе на преузимање и снимање докумената путем електронске поште или других извора;

ц) уништавање медија који садрже личне податке по истеку рока за обраду;

д) свако изношење било којег медија који садржи личне податке ван радних просторија мора бити са посебном дозволом и контролом да не дође до губљења или незаконитог коришћења;

е) мјере физичке заштите радних просторија и опреме гдје се обрађују лични подаци;

ф) поштивање техничких упутстава при инсталирању и коришћењу опреме која служи за обраду личних података.

Члан 34.
(Тајност лозинки)

1) КПЗ Добој ће осигурати потупуну тајност лозинки и осталих начина приступа рачунарима и програмима на којима се врши обрада личних података.

2) Сваки корисник ће потписати изјаву да је упознат са мјерама безбједности при аутоматској обради личних података, значајем корисничке шифре, правилима њеног кориштења и дужностима обавјештавања у случају сумње корисника да је његова шифра откривена или кориштена.

Члан 35.
(Преузимање и снимање докумената путем електронске поште или других извора)

Лице задужено за одређену збирку личих података при аутоматској обради у КПЗ Добој је дужно омогућити безбједно преузимање и снимање докумената путем електронске поште или других извора.

Члан 36
(Изношење личних података ван радних просторија)

1) Медиј, акте и збирке који садрже личне податке, ван радних просторија КПЗ Добој, могу се износити само уз посебну дозволу коју издаје помоћник директора или руководилац организационе јединице, односно лице које директор овласти.

2) Службеник који износи медиј, акте и збирке који садржи личне податке дужан је обезбједити исте како не би дошло до губљења или незаконитог кориштења приликом изношења ван просторија КПЗ Добој.

Члан 37.
(Приступ просторијама мрежног чвориште)

1) Сервер соба је смјештена у КПЗ Добој, климатизована је, са уграђеним адекватним уземљењем, те је под сталним надзором полиције службе обезбјеђења и видео надзором.

2) У просторији из става 1. налазе се сервери који су физички одвојени од осталих просторија.

3) Сервер соба у којој је смјештено мрежно чвориште мора имати један од приступних сигурносно-заштитних механизама на улазним вратима.

4) Физички приступ мрежном чворишту у сервер соби дозвољен је само вишем стручном сараднику за информационе системе, овлаштеним припадницима службе обезбјеђења у складу са Упутством о праћењу видео надзора.

5) Изузетно, улаз у мрежно чвориште дозвољен је у вандредним ситуацијама (пожар, поплава или нека друга елементарна непогода) и то само лицима која су надлежна да поступају у таквим ситуацијама.

Члан 38.
(Смјештање, постављање и уградња рачунара и рачунарске мреже)

1) Рачунари за вођење збирки личних података, рачунарску мрежу смјешта, поставља и уграђује стручна особа, у складу с важећим нормама, стандардима и техничким упутствима, према пројекту.

2) Један примјерак пројектне документације из става 1. овог члана чува се на безбједном мјесту, у КПЗ Добој.

Члан 39.
(Поштовање техничких упутстава при инсталирању и коришћењу опреме за обраду личних података)

1) На свим уређајима за обраду личних података су инсталирани софтвери у скаду са потребама радних процеса.

2) Није дозвољено инсталирање и коришћење софтвера који немају лиценцу и који нису одобрени од стране администратора.

3) Инсталацију софтвера као и све замјене на постојећој опреми за обраду личних података врши администратор система.

4) Одржавање и поправљање машинске, информатичке и друге опреме дозвољено је само са знањем овлаштене особе, а могу их изводити само овлаштена стручна лица КПЗ Добој или овлаштени сервиси, односно њихово особље, у складу са уговором о одржавању који је потписан између КПЗ Добој и овлаштеног сервисера.

Члан 40.
(Брисање података при аутоматској обради)

1) По истеку рока чувања, лични подаци се бришу, уништавају, брокирају или анонимизирају, осим уколико није другачије одређено Правилником о заштити личних података КПЗ Добој и Листом категорија регистарског материјала са роковима чувања у Казнено-поправном заводу Добој.

2) Рокови, чувања појединих категорија личних података, прописани су Правилником о провођењу закона о заштити личних података у КПЗ Добој.

3) За брисање података из компјутерских медија употребљава се таква метода брисања, да онемогућује рестаурацију свих или дијела обрисаних података.

4) Код преноса носача личних података на мјесто уништења, потребно је осигурати примјерено обезбјеђење.

5) Пренос носача података на мјесто уништења, те уништавање носача личних података надзире посебна комисија, која саставља одговарајући записник о уништењу.

Члан 41.
(Мрежна баријера)

КПЗ Добој обезбјеђује одговарајућу заштиту - мрежну баријеру између информационог система и Интернет мреже, или било које друге форме спољне мреже, као заштиту против недозвољеног покушаја улаза у систем.

Члан 42
(Право приступа систему за вођење збирки)

1) Приступ подацима похрањеним у збиркама личних података дозвољен је службеницима и запосленицима који имају овлаштење за приступ личним подацима, овлаштеним лицима задуженим за одржавање и развој система за вођење збирки личних података.

2) Директор КПЗ Добој, односно лице које он овласти, одређује лица која имају овлаштење за приступ личним подацима похрањеним у збиркама личних података.

3) Захтјев за приступ или обраду, те захтјев за престанак овлаштења за приступ збиркама личних података или обраду личних података подноси се директору КПЗ Добој или особи коју он овласти за давање или укидање дозвола за приступ збиркама.

4) Приступ у информациони систем за вођење збирки личних података или обраду података из збирки дозвољен је уз употребу одговарајућих корисничких имена и лозинки.

5) Није дозвољено да се укинуто корисничко име додијели другом лицу.

6) Корисничко име и лозинка не смију се одати или дати другом лицу.

Члан 43.
(Евиденција, праћење приступа и покушај неовлаштеног приступа систему)

1) Сваки приступ информационом систему за вођење збирки личних података мора бити аутоматски забиљежен корисничким именом, датумом и временом пријаве и одјаве.

2) Информациони систем треба да обезбједи евидентирање активности свих корисника у информационом систему: корисник који је активирао апликацију, врсту апликације која је кориштена, податке са којима је рађено са трагом промјена.

3) Сваки покушај неовлаштеног приступа систему мора бити аутоматски забиљежен корисничким именом, датумом и временом, ако је то могуће и мјестом с којег је такав приступ покушан.

4) Администратор збирке личних података и извршилац дужни су обавијестити одговорно лице у КПЗ Добој о сваком покушају неовлаштеног приступа систему.

Члан 44.
(Сигурносна копија)

1) КПЗ Добој врши снимање сигурносних копија или архивирање података у систему, да не би дошло до њиховог губљења или уништења. Сваки примјерак похрањених података на преносивом информатичком медију мора бити означен бројем, врстом, датумом похрањивања, те именом лица које је похрањивање извршило.

2) Лице овлаштено од стране директора КПЗ Добој провјерава употребљивост сигурносних копија збирки уз провјеру поступка повратa збирки похрањених на преносивом информатичком медију тако да враћени подаци након извршене провјере буду у цијелости расположиви за употребу, без губитка информација.

3) Виши сручни сарадник за информационе системе или лице које је задужено за одређену збирку личних података је дужан вршити редовно снимање сигурносних копија личних података система на преносиве информатичке медије употребом метода које гарантују безбједност и тајност тако похрањених личних података.

4) Збирке посебних категорија личних података похрањују се на преносне информатичке медије мјесечно и/или годишње, у складу са одговарајућом процјеном вишег стручног сарадника за информационе системе, по завршетку свих послова вођења збирке личних података за потребе обнове збирке у случају пожара, поплаве, потреса или неке друге несреће у разреду више силе.

5) Годишње и мјесечно похрањивање података чува се у периоду одређеном роковима чувања појединих категорија личних података.

6) Сваки примјерак похрањених података на преносном информатичком медију мора бити означен бројем, врстом (мјесечно, годишње), датумом похрањивања, те именом особе која је похрањивање спровела.

7) Виши стручни сарадник за информационе системе или лице задужено за одређену збирку личних података води евиденцију свих примјерака преносних информатичких медија на којима су похрањене збирке посебних категорија личних података.

8) Подаци система мјесечно и/или годишње похрањени на преносне информатичке медије, спремају се на безбједно мјесто одређено од стране одговорног лица из става 3. за збирку личних података.

9) Употребљивост мјесечне и годишње сигурносне копије збирке посебних категорија личних података провјерава се једном годишње.

Члан 45.
(Лице одговорно за заштиту личних података)

Директор КПЗ именује лице одговорно за уредно провођење мјера обезбјеђења, похрањивања и заштите личних података.

Члан 46.
(Лице овлаштено за додјељивање корисничких имена)

Виши стручни сарадник за информационе системе збирки личних података је лице овлаштено за додјељивање и уклањање корисничких имена лицима овлаштеним за рад у систему, а којима је дозвољен приступ збиркама личних података.

Члан 47.
(Заштита посебне категорије личних података)

1) Приликом обраде посебне категорије личних података у свим фазама обраде, КПЗ Добој означава да се ради о обради наведене категорије података.

2) КПЗ Добој предузима допунске техничке и организационе мјере при обради посебних категорија личних података.

3) Путем допунских техничких и организационих мјера при обради посебне категорије личних података обезбјеђује се:

а) могућност за препознавање сваког појединачног овлаштеног приступа информационом систему. Апликативни систем за обраду посебних категорија личних података треба да обезбједи евидентирање активности свих корисника односно у систему, датум и вријеме. Систем треба да има могућност да на основу ових података изврши рестаурацију стања до жељеног временског периода.

б) рад са подацима посебне категорије личних података врши се искључиво током редовног радног времена у КПЗ Добој. Изузетно се посебни подаци могу обрађивати и ван радног времена о чему мора бити обавијештен руководилац организационе јединице гдје се врши обрада личних података.

ц) криптозаштита података при преносу преко телекомуникационих система са одговарајућим софтверским и техничким мјерама.

V – ЗАВРШНЕ ОДРЕДБЕ

Члан 48.
(Одговорност за провођење мјера обезбјеђења личних података)

1) За уредно провођење мјера обезбјеђења, похрањивања и заштите личних података које се обрађују и воде у електронском облику одговара лице задужено за вођење одређене збирке личних података.

2) За извођење поступака и мјера за чување личних података одговорни су руководиоци организационих јединица у којима се врши обрада и лица која врше обраду личних података.

3) Свако, ко обрађује личне податке, дужан је спроводити прописане поступке и мјере за обезбјеђење и чување података, за које је сазнао односно био упознат са њима приликом извршавања својих обавеза. Обавеза чувања података не престаје са престанком радног односа.

4) Прије почетка рада на радном мјесту, гдје се обрађују лични подаци, запосленик мора потписати посебну изјаву, која га обавезује на заштиту личних података у складу са прописима о заштити личних података.

5) Из потписане изјаве мора бити видљиво, да је потписник упознат са одредбама Закона о заштити личних података, одредбама Правилника о провођењу закона о заштити личних података КПЗ Добој, Плану безбједност и личних података КПЗ Добој, а изјава мора садржавати и поуку о последицама прекршаја.

Члан 49.
(Провјера система)

Виши стручни сарадник за информационе системе седмично, мјесечно и годишње провјерава рад свих дјелова система по принципу случајног узорка о чему сачињава записник.

Члан 50.
(Злоупотреба личних података)

Са сваким неовлаштеним приступом личним подацима, њиховим уништењем, крађом или другим догађајем који указује на злоупотребу личних података, треба одмах упознати директора КПЗ Добој односно лице које је он овластио и обезбједити све мјере за онемогућавање даље злоупотребе личног податка, те провести истрагу о околностима злоупотребе.

Члан 51.
(Дисциплинска одговорност)

1) Сви запослени у КПЗ Добој су дисциплински одговорни за кршење одредби овог Плана.

2) Поступање запослених КПЗ Добој које је супротно од утврђених правила у поступку обраде личних података, и ЗИКПС-а подлијеже дисциплинској одговорности, у складу с прописима који се односе на дисциплинску одговорност запослених и Правилника о дисциплинској одговорности запослених у установама за извршење кривичних санкција.

Члан 52.
(Ступање на снагу)

Овај План ступа на снагу даном доношења.

Број: 01-170-3075/20
Датум: 22.10. 2020. године.

ДИРЕКТОР
Мр Бранко Милетић