На основу члана 10. Закона о јавним предузећима ("Службени гласник Републике Српске", број: 75/04 и 78/11), члана 11. став 4. Закона о заштити личних података ***("Службени. гласник БиХ", бр. 49/2006, 76/2011 и 89/2011 - испр.)***, члана 51. Статута Јавног предузећа шумарства "Шуме Републике Српске" а.д. Соколац и члана 16. Правилника о провођењу Закона о заштити личних података у ЈПШ "Шуме Републике Српске" а.д. Соколац, Управа Јавног предузећа, на сједници одржаној дана 24.09.2020. године, **донијела је**

# ПЛАН СИГУРНОСТИ ЛИЧНИХ ПОДАТАКА У ЈПШ „ШУМЕ РЕПУБЛИКЕ СРПСКЕ“ а.д. Соколац

I - ОПШТЕ ОДРЕДБЕ

## Члан 1.
## (Предмет Плана)

Планом сигурности личних података прописују се неопходне ефективне сигурносне мјере у поступку обраде, преноса и похрањивања личних података, те се ближе уређују посебни организациони и технички видови заштите личних података у ЈПШ „Шуме Републике Српске“ а.д. Соколац (у даљем тексту Јавно предузеће).
Планом сигурности личних података одређују се мјере, средства и услови похрањивања, 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 овлашћена за провођење предвиђених мјера, те лица одговорна за надзор над провођењем тих мјера.

## Члан 2.
## (Циљ Плана)

Циљ мјера Плана сигурности је заштита личних података који се обрађују, преносе, те података похрањених у збиркама личних података у Јавном предузећу од случајног или бесправног уништавања, или случајног губитка, неовлашћеног приступа, измјена и сл., као и откривање, те истрагу таквих случајева.

## Члан 3.
## (Садржај Плана сигурности)

План сигурности личних података (у даљем тексту: План) садржи категорије личних података које се обрађују и попис инструмената заштите односно организационе и техничке мјере заштите којима се обезбјеђује:

а) да само лица овлашћена за то могу имати приступ личним подацима – **повјерљивост,**
б) да за вријеме обраде, лични подаци остану непромијењени, потпуни и ажурни – **интегритет,**
в) да су подаци стално доступни, да су на располагању и да се могу исправно обрађивати – **расположивост,**
г) да се у свако доба може утврдити поријекло личних података – **аутентичност,**
д) да се може утврдити ко, када, које је личне податке и на који начин обрађивао - **могућност ревизије;**
ђ) да је поступак при обради личних података потпун, ажуран и на одговарајући начин евидентиран - **транспарентност.**

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

**Члан 4.**
**(Повјерљивост)**

Службеницима Јавног предузећа који у обављању редовних послова имају потребу приступа личним подацима, односно збиркама личних података који се обрађују у информационом систему у Јавног предузећу, издаје се посебно рјешење којим се овлашћују за приступ тим подацима. Службеницима којима се изда ово рјешење додјељује се корисничко име и приступна шифра на начин и по поступку који је прописан овим Планом.
Рјешење о овлашћењу за приступ наведеним подацима доноси директор организационог дијела Јавног предузећа.
Остали службеници могу приступати личним подацима уколико се таква потреба појави у вези са извршавањем редовних послова, за што им се од стране директора издаје посебно одобрење.
Овим службеницима додјељује се приступно корисничко име и шифра који важе само за одређени период који је наведен у одобрењу.
Одобрење мора да садржи јасну назнаку, који подаци, односно збирке личних података се могу обрађивати и период важења одобрења.

**Члан 5.**
**(Интегритет)**

Службеници Јавног предузећа који обрађују личне податке дужни су правовремено ажурирати податке, на основу релевантне документације.
Службеници Јавног предузећа дужни су ажурирати податке у евиденцијама које се воде у оквиру Јавног предузећа у складу са Законом о заштити личних података (у даљем тексту Закон) и Правилником о провођењу закона о заштити личних података у Јавном предузећу.

**Члан 6.**
**( Расположивост)**

Службеници Јавног предузећа дужни су податке из збирке личних података коју обрађују, чинити доступним и на располагању, како за друге службенике, тако и за друге организационе јединице Јавно предузеће и остале кориснике ван Јавног предузећа, а у складу с чланом 17. Закона.

**Члан 7.**
**(Аутентичност)**

Службеници Јавног предузећа 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;
в) добијањем података од трећег лица које треба навести именом, презименом и другим подацима на основу којих се лице може идентификовати;
г) властитим опажањем или истраживањем и

д) из неких других извора које треба поближе навести.

**Члан 8.**
**(Могућност ревизије)**

Ревизијом се обезбјеђује поступак провјере законитости обраде личних података, у којем је накнадно могуће утврдити који је службеник Јавног предузећа обрађивао личне податке, датум обраде, који лични подаци су обрађени и на који су начин обрађени. Обрада личних података у смислу овог члана подразумијева да службеници Јавног предузећа 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.

Уколико се врши обрада података електронским путем, систем ће омогућити похрану података о службенику који је обрађивао личне податке 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)**

Заштита личних података у Јавном предузећа, заснована је на принципима познатим као ААА, који подразумијева три елемента заштите.

Прво А јесте аутентичност (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.

Друго А је ауторизација (authorization), 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 конкретно овлашћени корисници и шта са тим подацима могу да раде (преглед, измјена, додавање и брисање).

Треће А је праћење (accountability) 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)**

Јавно предузеће у циљу заштите личних података које обрађује предузима:

1) организационе мјере,
2) техничке мјере.

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)**

Начин вођења збирки личних података прописан је Правилником о провођењу закона о заштити личних података у Јавном предузећу.

**Члан. 13.**
**(Вођење збирки личних података)**

Директор одређује извршиоце обраде збирке личних података које се воде у Јавном предузећу. Извршилац из става 1) овог члана је одговоран за чување збирки личних података, спрјечавање неовлашћеног приступа и коришћења, те увида у податке из збирке као и тачност и аутентичност података унесених у збирке.

**Члан 14.**
**(Чување података)**

Подаци у збиркама личних података чувају се у складу са Законом о заштити личних података.

**Члан 15.**
**(Информисање и обука запослених)**

Јавно предузеће ће провести план обука запослених лица у Јавном предузећу 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 сигурности код свих запослених.
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.
Прије непосредног отпочињања обављања послова везаних за обраду личних података, запослени се додатно упознају са конкретним обавезама по питању заштите личних података.

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

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),
в) лица која обрађују информације и
г) како ће се архивирати информације.

Мјере физичке заштите су тако осмишљене да:

а) спријече недозвољен или насилан упад од стране неовлашћеног лица,
б) одврате, спријече и открију радње неовлашћеног лица,
в) омогуће селекцију лица у погледу приступа личним подацима и
г) омогуће откривање и поступање у свим случајевима угрожавања сигурности што је прије могуће.

**Члан 17.**
**(Физички надзор улаза и излаза)**

Систем улазног надзирања треба да буде осмишљен тако да обезбјеђује потпуни надзор над улазом односно излазом лица у просторије сједишта Јавног предузећа, дозвољава улаз само лицима која имају одговарајуће одобрење за приступ просторијама или која су запослена у Јавном предузећу, односно имају посебне дозволе за улазак у службене просторије.

Службеници обезбјеђења обезбјеђују службени улаз у просторије сједишта Јавног предузећа 24 часа дневно, 7 дана у седмици.

Прије уласка незапослених лица у просторије Јавног предузећа, службеник обезбјеђења који надзире улазак у службене просторије Јавног предузећа, мора провјерити њихов идентитет и разлог уласка, као и испуњавање других услова за улазак у просторије Јавног предузећа.

Незапосленим лицима којима се дозвољава улазак у просторије Јавног предузећа издаје се сигурносна пропусница којом се дозвољава кретање просторијама Јавног предузећа и даје им се до знања да је њихово кретање надзирано и евидентирано.

Сва лица која нису запослена у Јавном предузећу, а која приступају просторијама Јавног предузећа морају имати на видљивом мјесту закачену сигурносну пропусницу за улазак и кретање кроз просторије Јавног предузећа, а службеници обезбјеђења ће водити евиденцију о издатим сигурносним пропусницама.

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 другим лицима у пратњи службеног лица.

**Члан 18.**
**(Просторије, ормари и сефови)**

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

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

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.

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

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.**
**(Спрјечавање неовлашћеног умножавања, копирања и преписивања личних података)**

Личне податке могу умножавати, копирати или преписивати само лица која су задужена за обраду личних података у складу са потребама обављања редовних радних задатака.
Опрема за умножавање поставља се на мјестима чија је употреба под надзором лица овлашћених за обраду личних података или на мјестима покривеним видео надзором.

**Члан 20.**
**(Уништавање докумената)**

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.
На исти начин уништава се помоћни и радни материјал (нпр. матрице, израчуна и графикони, скице, тестних односно неуспјешне штампе итд.) који се односи на личне податке који се уништавају. Забрањено је одбацивање отпадних носача података са личним подацима у смеће.

Директор Јавног предузећа ће одредити Комисију за уништавање докумената који садрже личне податке, те је иста дужна сачинити записник о уништавању. Комисију чине три члана, службеника Јавног предузећа. Комисија ће, након што сачини записник, исти доставити директору на верификацију.

III - ТЕХНИЧКЕ МЈЕРЕ

**Члан 21.**
**(Мјере техничке заштите)**

Јавно предузеће обезбјеђује одговарајуће мјере техничке заштите просторија и опреме у којима се врши обрада личних података.

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)**

Службени улаз и ходници сједишта Јавног предузећа су покривени надзором видео система. Систем видео надзора повезан је на мониторинг станицу смјештену у надзорном центру на улазу у просторије Јавног предузећа. Службеници обезбјеђења обезбјеђују мониторинг станицу 24 сата, 7 дана у седмици. Систем видео надзора има могућност архивирања података, како би се подаци могли ишчитати у случају да се за тим укаже потреба.
Контролни центар Јавног предузећа је покривен системом видео надзора. Службеници обезбјеђења обезбјеђују мониторинг станицу цјелодневно, 7 дана у седмици. Систем видео надзора има могућност архивирања података, како би се подаци могли исчитати у случају да се за тим укаже потреба.

Администратор личних података је задужен за редовно похрањивање видео записа на преносиве медије, те њихово архивирање, заштиту од неовлашћеног брисања, те изузимање одређених дијелова снимака, уколико се за тим укаже потреба, уз сагласност и по налогу директора.

**Члан 23.**
**(Кључеви и шифре)**

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

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

Кључеви канцеларија у којима се обрађују лични подаци може имати само извршилац, а резервни ће се чувати у просторијама надзорног центра, а могућност њиховог коришћења је ограничена за потребе администрирања личних података, за потребе лица која врше послове хигијенског одржавања просторија, односно у случају ванредних ситуација и крајње нужде.

На просторијама, гдје постоје електронски контролори приступа, приступне шифре ће познавати само лица која у оквиру својих радних задатака имају потребу приступа тим

просторијама, а радни задаци у органу ће се распоредити тако да је број лица упознатих са појединим комбинацијама буде што мањи.
Приступне шифре на металним сефовима ће познавати само лица задужена за похрањивање докумената и медија у сеф.
Постављене комбинације електронских и механичких брава се мијењају:

а) одмах након постављања;
б) у случају откривања или сумње у откривање;
в) након шест мјесеци од задњег постављања службеника;
г) након тога када лице из прошлог става престаје обављати задатке у органу због којих је била упозната са постављеним комбинацијама и
д) када тако одлучи директор Јавног предузећа.

Приступне шифре ће бити депоноване у запечаћеној коверти и исте се похрањују на сигурно мјесто у складу са правилима заштите тајних података.

**Члан 24.**
**(Посебне мјере заштите)**

У близини рачунарске и телекомуникационе опреме не смије бити извора јаког електричног или магнетног поља и извора јонизирајућег зрачења.
У близини опреме осјетљиве на електростатички електрицитет не смије бити извора таквог електрицитета.
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 °C.
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.
У просторијама у којима су смјештени рачунари не смију се налазити уређаји који у ваздух испуштају честице прашине. Уређаји осјетљиви на прашину морају бити прописно заштићени. Посебно осјетљиви уређаји који се хладе ваздухом, морају имати филтере за ваздух.
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)**

Јавно предузеће при аутоматској обради личних података обезбјеђује техничке мјере заштите личних података 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 утврђеном временском периоду који не може бити дужи од три мјесеца,
в) корисничко име и лозинка ће дозвољавати приступ само до дијелова система потребних извршиоцу за извршење његових радних задатака,
г) 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,

д) аутоматску забрану приступа систему након три неуспјешна покушаја пријављивања на систем и аутоматско упозорење извршиоцу да потражи инструкцију од администратора збирке личних података,
ђ) ефикасну и сигурну антивирусну заштиту система, које ће се стално ажурирати ради превентиве од непознате или непланиране опасности од нових вируса;
е) компјутерска, програмска и остала неопходна опрема на електроенергетску мрежу се прикључује путем уређаја за непрекидно напајање.

Извршилац који обавља кадровске послове, дужан је да извјештава администратора збирке личних података о запослењу 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. 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)**

Да би корисник приступио систему путем радне станице потребно је да има важећи кориснички налог и лозинку.
Сваки корисник добија кориснички налог и почетну лозинку, коју је дужан промијенити након првог пријављивања на систем.
Кориснички налог је јединствен, један корисник може имати само један кориснички налог, који ће садржавати прво слово имена и презиме корисника.
У случају да два или више корисника имају исто име и презиме, администратор система додјељује другачије корисничко име од прописаног у ставу (3) овог члана.

**Члан 27.**
**(Корисничка лозинка)**

Корисничка лозинка треба да садржи најмање 8 (осам) карактера, који представљају комбинацију великих и малих слова, те бројева.
Корисник је дужан мијењати лозинку сваких 90 дана и не смије је дијелити са другим службеницима.

Уколико корисник намјерава одсуствовати са посла, дужан је да све информације које би требао дијелити са другим службеницима, пребаци у дјељиве директоријуме.

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.

Службеник је дужан да памти своју лозинку и иста се не може записивати, а посебно не у близини рачунара.
У случају да корисник заборави своју лозинку потребно је Служби за информационе технологије, путем руководиоца службе поднијети захтјев за додјелу нове. Промјену лозинке врши администратор система, а тај податак се уписује у администраторски дневник.

**Члан 28.**
**(Приступ систему)**

Корисничко име и лозинка ће дозвољавати приступ само до дијелова система потребних извршиоцу за извршење његових радних задатака - привилеговани ниво.
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 радне странице, дужни су обавезно да се одјаве са система. Администратор 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)**

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 Служби за информационе технологије, путем руководиоца службе поднесе захтјев за додјелу нове. Промјену лозинке врши администратор система.

**Члан 31.**
**(Антивирусна заштита)**

Информациони систем Јавног предузећа мора имати ефикасну и сигурну антивирусну заштиту система, која се редовно ажурира ради превентиве од непознате или непланиране опасности од нових вируса.
Антивирусни програм треба да спријечи инфекцију малициозним програмима (вирусима, црвима, тројанцима), односно да ублажи или потпуно санира посљедице њиховог дејства својим дјеловањем. Квалитет антивирусног програма се оцјењује на основу брзине скенирања, способности да открије вирусе, конфигурисана и ажурирања листе потписа познатих вируса.

**Члан 32.**
**(Обавеза употребе уређаја за непрекидно напајање)**

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.

**Члан 33.**
**(Организационе мјере)**

Јавно предузеће при аутоматској обради личних података обезбјеђује организационе мјере заштите личних података и то:

а) потпуну тајност и сигурност 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.
в) уништавање медија који садрже личне податке по истеку рока за обраду,
г) 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,
ђ) мјере физичке заштите радних просторија и опреме гдје се обрађују лични подаци,
е) поштовање техничких упутстава при инсталирању и коришћењу опреме која служи за обраду личних података.

**Члан 34.**
**(Тајност лозинки)**

Јавно предузеће ће осигурати потпуну тајност лозинки и осталих начина приступа рачунарима и програмима на којима се врши обрада личних података.
Сваки корисник ће потписати изјаву да је упознат са мјерама сигурности при аутоматској обради личних података, значајем корисничке шифре, правилима њеног коришћења и дужностима обавјештавања у случају сумње корисника даје његова шифра откривена или кориштена.

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

Администратор збирки личних података при аутоматској обради у Јавном предузећу је дужан омогућити безбједно преузимање и снимање докумената путем електронске поште или других извора.

**Члан 36.**
**(Изношење личних података ван радних просторија)**

Медији који садрже личне податке, ван радних просторија Јавног предузећа за послове са странцима, могу се износити само уз посебну дозволу коју издаје директор Јавног предузећа, односно лица које директор овласти.
Службеник који износи медиј који садржи личне податке дужан је обезбедити исте како не би дошло до губљења или незаконитог коришћења медија који се износи.

**Члан 37.**
**(Приступ просторијама мрежног чворишта)**

Мрежно чвориште је смјештено у сједишту Јавно предузеће, климатизовано је, са уграђеним антистатичким подом и адекватним уземљењем, те је под сталним видео надзором.
У просторији из става 1. налазе се сервери који су физички одвојени од осталих просторија.
Просторија у којој је смјештено мрежно чвориште мора имати један од приступних сигурносно- заштитних механизама на улазним вратима.
Физички приступ мрежном чворишту дозвољен је само службеницима Службе за информационе технологије.
Изузетно , улаз у мрежно чвориште дозвољен је у ванредним 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)**

Рачунари за вођење збирки личних података, централни рачунар збирки и рачунарску мрежу смјешта, поставља и уграђује стручнолице, у складу с важећим нормама, стандардима и техничким упутствима, према пројекту.
Један примјерак пројектне документације из става 1. овог члана чува се на безбједном мјесту, у радним просторијама администратора збирке личних података .

**Члан 39.**
**(Поштовање техничких упутстава при инсталирању и коришћењу опреме за обраду личнихподатака )**

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

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

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

Одржавање и поправљање машинске, информатичке и друге опреме дозвољено је само са знањем овлашћеног лица, а могу их изводити само овлашћена стручна лица или овлашћени сервиси, односно њихова лица, у складу са уговором о одржавању који је потписан између Јавног предузећа и овлашћеног сервисера.

**Члан 40.**
**(Брисање података при аутоматској обради)**

По истеку рока чувања, лични подаци се бришу, уништавају, блокирају или анонимизирају, осим уколико није другачије одређено.
Рокови, чувања појединих категорија личних података, прописани су Правилником о провођењу закона о заштити личних података у Јавном предузећу.
За брисање података из компјутерских медија употребљава се таква метода брисања, да онемогућује рестаурацију свих или дијела обрисаних података.

Код преноса носача личних података на мјесто уништења, потребно је осигурати примјерено обезбјеђење.
Пренос носача података на мјесто уништења, те уништавање носача личних података надзире посебна комисија, која саставља одговарајући записник о уништењу.

**Члан 41.**
**(Мрежна баријера)**

Јавно предузеће 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)**

Приступ подацима похрањеним у збиркама личних података дозвољен је службеницима и запосленицима који имају овлашћење за приступ личним подацима, овлашћеним лицима задуженим за одржавање и развој система за вођење збирки личних података.
Директор Јавног предузећа, односно лице које он овласти, одређује лица која имају овлашћење за приступ личним подацима похрањеним у збиркама личних података.
Захтјев за приступ или обраду, те захтјев за престанак овлашћења за приступ збиркама личних података или обраду личних података подноси се директору Јавног предузећа или лицу које он овласти за давање или укидање дозвола за приступ збиркама.
Приступ у информациони систем за вођење збирки личних података или обраду података из збирки дозвољен је уз употребу одговарајућих корисничких имена и лозинки. Није дозвољено да се укинуто корисничко име додијели другом лицу. Корисничко име и лозинка не смију се одати или дати другом лицу.

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

Сваки приступ информационом систему за вођење збирки личних података мора бити аутоматски забиљежен корисничким именом, датумом и временом пријаве и одјаве.
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.
Сваки покушај неовлашћеног приступа систему мора бити аутоматски забиљежен корисничким именом, датумом и временом, ако је то могуће и мјестом с којег је такав приступ покушан.
Администратор збирке личних података и извршилац дужни су обавијестити одговорно лице у Јавном предузећу о сваком покушају неовлашћеног приступа систему.

**Члан 44.**
**(Сигурносна копија)**

Јавно предузеће врши редовно 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.
Лице овлашћено од стране директора Јавног предузећа провјерава употребљивост сигурносних копија збирки уз провјеру поступка повратак збирки похрањених на преносивом информатичком медију тако да враћени подаци након извршене провјере буду у цијелости расположиви за употребу, без губитка информација.
Администратор збирке је дужан вршити редовно снимање сигурносних копија личних података система на преносиве информатичке медије употребом метода које гарантују сигурност и тајност тако похрањених личних података.
Збирке посебних категорија личних података похрањују се на преносне информатичке медије мјесечно и/или годишње, у складу са одговарајућом процјеном администратора, 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.
Мјесечно похрањивање података система проводи се посљедњи радни дан у мјесецу, за сваки мјесец посебно, у 12 примјерака годишње.
Годишње похрањивање података система проводи се посљедњи радни дан у години. Сваки примјерак годишње похрањених података чува се у периоду одређеном роковима чувања појединих категорија личних података.
Сваки примјерак похрањених података на преносном информатичком медију мора бити означен бројем, врстом (мјесечно, годишње), датумом похрањивања, те именом лица које је похрањивање спровело.
Администратор збирке води евиденцију свих примјерака преносних информатичких медија на којима су похрањене збирке посебних категорија личних података.
Подаци система мјесечно и/или годишње похрањени на преносне информатичке медије, спремају се на безбједно мјесто одређено од стране администратора збирке личних података.
Употребљивост годишње сигурносне копије збирке посебних категорија личних података провјерава се најмање једном годишње уз провјеру поступка повратка збирки похрањених на преносном информатичком медију тако да враћени подаци након извршене провјере буду у потпуности расположиви за употребу, без губитка информација.
Употребљивост мјесечне сигурносне копије збирке посебних категорија личних података провјерава се најмање сваких шест мјесеци.

**Члан 45.**
**(Лице одговорно за заштиту личних података)**

Директор Јавног предузећа именује лице одговорно за уредно провођење мјера обезбјеђења, похрањивања и заштите личних података, те администратора збирки личних података.

**Члан 46.**
**(Лице овлашћено за додјељивање корисничких имена)**

Администратор збирки личних података је лице овлашћено за додјељивање и уклањање корисничких имена лицима овлашћеним за рад у систему, а којима је дозвољен приступ збиркама личних података.

**Члан 47.**
**(Заштита посебне категорије личних података)**

Приликом обраде посебне категорије личних података у свим фазама обраде, Јавно предузеће означава да се ради о обради наведене категорије података.
Јавно предузеће предузима допунске техничке и организационе мјере при обради посебних категорија личних података.
Путем допунских техничких и организационих мјера при обради посебне категорије личних података обезбјеђује се:

а) могућност за препознавање сваког појединачног овлашћеног приступа информационом систему. Апликативни систем за обраду посебних категорија личних података треба да обезбједи евидентирање активности свих корисника односно оператера у систему, датум и вријеме, те локацију са које је извршена активност. 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 радног времена Јавног предузећа. Изузетно се посебни подаци могу обрађивати и ван радног времена о чему мора бити обавијештен руководилац организационе јединице гдје се врши обрада личних података.
в) 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)**

За уредно провођење мјера обезбјеђења, похрањивања и заштите личних података које се обрађују и воде у електронском облику одговара администратор збирки личних података.

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.

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.

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.

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, Плана сигурности личних података Јавног предузећа, а изјава мора садржавати и поуку о посљедицама прекршаја.

**Члан 49.**
**(Провјера система)**

Администратор збирке личних података седмично, мјесечно и годишње провјерава рад свих дјелова система по принципу случајног узорка о чему сачињава записник.

**Члан 50.**
**(Злоупотреба личних података)**

Са сваким неовлашћеним приступом личним подацима, њиховим уништењем, крађом или другим догађајем који указује на злоупотребу личних података, треба одмах упознати руководиоца органа 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)**

Сви службеници и запосленици Јавног предузећа су дисциплински одговорни за кршење одредби овог Плана.

Поступање службеника Јавног предузећа које је супротно од утврђених правила у поступку обраде личних података, подлијеже дисциплинској одговорности, у складу с прописима који се односе на дисциплинску одговорност службеника.

**Члан 52.**
**(Ступање на снагу)**

Овај План ступа на снагу осмог дана од дана објављивања на огласним таблама Дирекције Јавног преузећа.
План сигурности личних података у ЈПШ "Шуме Републике Српске" а.д. Соколац објавиће се и на интернет страници Јавног предузећа.

**В.Д. ДИРЕКТОРА ЈАВНОГ ПРЕДУЗЕЋА**
Славен Бојковић дипл. инж. шумарства

План сигурности личних података у ЈПШ "Шуме Републике Српске" а.д. Соколац објављен је на огласним таблама Дирекције Јавног предузећа дана 01.10. 2020. године.

Јавно предузеће шумарства "Шуме Републике Српске" а.д. Соколац Дирекција
Примљено: 01.10.20 20
Број: 0116 Број протокола: 3634/20

**ДИРЕКТОР СЕКТОРА**
**за имовинско-правне, кадровске и опште послове**
Драгана Гудурић дипл. правник