22-431/16
26.05.2016

Република Српска
УНИВЕРЗИТЕТ У БАЊОЈ ЛУЦИ
Управни одбор

Број: 03/04-3.1409-13/16
Дана, 19.05.2016. године

На основу члана 26. став (1) тачка 2) Статута Универзитета у Бањој Луци, а након разматрања Приједлога Политике безбједности информационог система Универзитета у Бањој Луци, Управни одбор Универзитета, на 43. сједници одржаној дана 19.05.2016. године, д о н о с и

О Д Л У К У
о усвајању Политике безбједности информационог система Универзитета у Бањој Луци

I

Усваја се Политика безбједности информационог система Универзитета у Бањој Луци.

II

Саставни дио ове Одлуке је Политика безбједности информационог система Универзитета у Бањој Луци.

III

Ова Одлука ступа на снагу даном доношења.

О б р а з л о ж е њ е

Управни одбор Универзитета је, након разматрања достављеног приједлога Политике безбједности информационог система Универзитета у Бањој Луци, а имајући у виду да је иста заснована на стратегији развоја Универзитета у Бањој Луци, стратегији развоја Републике Српске, те пословној политици и пословним циљевима Универзитета у Бањој Луци, одлучио као у диспозитиву ове Одлуке.

ПОУКА О ПРАВНОМ ЛИЈЕКУ: Против ове Одлуке може се уложити Приговор Управном одбору Универзитета у року од 15 дана од дана пријема исте.

Достављено:
1. Свим факултетима/Академији/Институту,
2. Ректору и проректорима Универзитета,
3. Генералном секретару,
4. Финансијском директору,
5. а/а.

ПРЕДСЈЕДНИК
УПРАВНОГ ОДБОРА

Проф. др Миле Дмичић

УНИВЕРЗИТЕТ У БАЊОЈ ЛУЦИ

ПОЛИТИКА БЕЗБЈЕДНОСТИ ИНФОРМАЦИОНОГ СИСТЕМА

Бања Лука, март 2016.

САДРЖАЈ

А. Увод

Овај документ описује безбједносне политике и стандарде Универзитета у Бањој Луци (у даљем тексту Универзитет).

Циљ „Политике безбједности информационог система" (у даљем тексту: Политика) је да обезбиједи заштиту информација Универзитета кроз безбједан и функционалан информациони систем (у даљем тексту: ИС). Тако успостављен ИС треба да обезбједи расположивост, повјерљивост, вјеродостојност, непорецивост и доказивост информације.

Политика се заснива на стратегији развоја Универзитета, стратегији развоја Републике Српске, пословној политици и пословним циљевима Универзитета, као и на важећим регулаторним захтјевима и представља највиши акт о безбједности информационог система Универзитета. Она представља темељни акт за све остале акте из области безбједности ИС-а.

А.1. Основни подаци о ИС Универзитета

Да би се добила почетна представа о величини и комплексности информационог система Универзитета у Бањој Луци (ИСУБЛ) дати су, у сљедећој табели, општи подаци о Универзитету.

Универзитет је смјештен на више локација у Бањој Луци и једној локацији у Приједору. У Приједору се налази Рударски факултет, а сви остали су у Бањој Луци и већина их је груписана у два кампуса, оба на обалама ријеке Врбас, недалеко од центра града. Кампус 1 или стари кампус смјештен је у улици Војводе Степе Степановића, а Кампус 2 или нови кампус смјештен је у бившој касарни у улици Булевар Војводе Петра Бојовића. Три факултета: Електротехнички, Природно-математички и неки дијелови Медицинског факултета смјештени су изван ових кампуса, на различитим локацијама у граду.

Б. Улоге и одговорности

Б.1. Руковођење процесима информационе безбједности

Одговорност за руковођење процесима физичке безбједности сноси финансијски директор Универзитета, кроз координацију Службе безбједности (у даљем тексту СБ). За процесе информационог система и процесе безбједности информационог система

(према важећем Правилнику о унутрашњој организацији и систематизацији радних мјеста на УНИБЛ) одговоран је генерални секретар, који координира рад Универзитетског рачунарског центра (у даљем тексту УРЦ) и администратор за безбједност информационог система.

Важну улогу има и Колегијум (ректор, проректори, финансијски директор, генерални секретар и предсједник студентског парламента). Колегијум проширен руководиоцем УРЦ-а и администратором за безбједност информационог система, обавља и функције одбора за ИТ и безбједност (за потребе стратегијског управљања), те обезбјеђује добре праксе руковођења, те укључивање и координацију свих заинтересованих страна у процесима информационог система и информационе безбједности.

Б.2. Одговорност администратора за безбједност информационог система

Одговорност Службе безбједности и администартора за безбједност информационог система укључује непосредну оперативну одговорност за физичку безбједност, безбједоносне аспекте свих ИТ процеса, као и њихову усклађеност, што је детаљније описано у „Закону о информационој безбједности Републике Српске"[1] и „Правилнику о минималним стандардима информационе безбједности"[2] који дефинише професионалне стандарде од интереса за институције од значаја за Републику Српску.

Б.3. Одговорност запослених на Универзитету

Запослени у свим чланицама и организационим дијеловима Универзитета су дужни да поступају у складу са одредбама ове Политике.

Б.4. Хијерархија структуре управљања безбједношћу

Управљање процесима безбједности информационог система се обавља путем администартора за безбједност информационог система који је надлежан за цијелу организациону структуру Универзитета.

[1] Службени гласник Републике Српске 70/11

[2] http://www.aidrs.org/sr/legislativa-i-standardizacija/podzakonski-akti/pravilnik-standardima-informacione-bezbjednosti/

Ц. Управљање ризицима безбједности информационог система

Захтјеви који се постављају пред модерне информационе системе односе се на заштиту информационих ресурса и смањење ризика. Увећавањем рачунарске снаге персоналних рачунара, трендовима увећавања количина података, виртуелизације сервера и рјешења у „облаку" значајно се измијенио и концепт безбједности, управљања и контроле информационих ресурса. Неадекватна контрола рачунарских система може имати озбиљне посљедице укључујући:

- Немогућност извршавања мисије и усвојених стратегија,
- Губитак средстава,
- Губитак кредибилитета и повјерења.

Избјегавање ових посљедица може се постићи постављањем адекватног система заштите информационих ресурса.

Служба за безбједност (у процесима физичке безбједности) и администартор за безбједност информационог система, у сарадњи са руководиоцем Универзитетског рачунарског центра (УРЦ), одговорна је за редовно спровођење анализе ризика информационе имовине, те са њима повезаних пријетњи и рањивости. Управљање ризицима треба се укључити и у сљедећим пословним процесима:

- Одржавање безбједносне свијести запослених (АПО7[1])
- Управљање системом безбједности информационог система – ИСМС (АПО13)
- Управљање инцидентима (ДСС2)
- Управљање континуитетом и опоравком пословања (ДСС4)
- Управљање безбједносним сервисима (ДСС6)

Ове анализе ризика се спроводе у складу са важећом „Методологијом управљања ИТ ризицима".

Д. Минимални стандарди безбједности информационог система

Политику безбједности ИС-а чини скуп стандарда којима је уређено његово функционисање. У наставку ћемо појаснити сваки од важећих стандарда безбједности информационог система појединачно.

[1] Ознаке процеса су преузете из оквира за управљање COBIT верзија 5.0

Д.1. Обука запослених

Заштита података и информационог система је више људско него техничко питање јер је човјек витална карика у заштити информационог система. Саме информације потичу од људи, уносе се у систем од стране људи и користе људима. Стога је потребно кориснике ИС-а редовно обавјештавати о насталим промјенама и обучавати их како да користе ИС, а да не угрозе његову безбједност.

Обука запослених ће се дефинисати на свим нивоима унутар Универзитета (извршне функције и функције које креирају политику, руководиоце чланица и заједничких организационих дијелова, посебно лица одговорних за заштиту информационих ресурса, лица са улогама у Информационом систему Универзитета, лица одговорна за развој, операције и пружање подршке за крајње кориснике). Најважнији циљ обуке је да корисницима јасно укаже на њихова права и одговорности коју имају за безбједност ИС-а, те повећање укупне безбједносне спремности запослених.

Д.2. Софтвер

Д.2.1 Инсталација новог софтвера (Software Security Policy)

На компјутерима и мрежама у Универзитету који су повезани са Информационим системом Универзитета, као и у мрежама које су повезане са повјерљивим подацима, дозвољено је инсталирати само оне софтверске пакете који су усклађени са важећим уговорима о лиценцирању. Инсталирање бесплатних програма са Интернета или било којих меморијских медија у поменутим мрежама није дозвољено. Дозвољено је коришћење искључиво тестираног и одобреног софтвера. Инсталацију софтвера информационог система Универзитета раде искључиво овлашћена лица из УРЦ. Препоручује се да рачунари који приступају информационом систему Универзитета буду дио посебног домена са централизованим наметањем политика која одржава УРЦ.

Д.2.1 Тестирање новог софтвера (New Software Security Policy)

Универзитет не дозвољава незакониту израду копија софтвера. Запослени који направе, прибаве или употребе недозвољене копије софтвера дисциплински

одговарају. У рачунарској мрежи информационог система Универзитета, и мрежама које су повезане са повјерљивим подацима дозвољено је коришћење софтвера, литературе или других ауторских дијела за које су плаћене лиценце или накнаде.

Тестирање нелиценцираног софтвера у ограниченом временском трајању је дозвољено само овлаштеним и обученим радницима који имају најмање двије године релевантног радног искуства.

Д.3. Набавка, развој и тестирање инфраструктуре и апликација

Свака набавка, инсталација и имплементација информационе, комуникационе и друге пратеће опреме, система и апликација треба да је у складу са одлуком надлежног органа Универзитета. Архитектура самих апликација треба да је усклађена са дефинисаном архитектуром ИС-а. Развој и провјера свих апликација треба да се врши на тестном окружењу. Све апликације треба да се детаљно тестирају у тестном окружењу прије пуштања у продукциони рад.

Ради сепарације права програмера и администратора, лица и тимови који раде развој и одржавање апликација немају права приступа продукционом окружењу (осим евентуално корисничка ако су они заиста и корисници апликације), док су њихова права приступа на тестном окружењу лимитирана на разумну мјеру.

Д.4. Односи са добављачима

Односи са добављачима се граде на принципима којима се штити безбједност ИС-а и података Универзитета, те у складу са Законом о јавним набавкама. Универзитет не ставља ни једног добављача услуга или опреме у повољнији положај у односу на друге, на начин који би могао угрозити безбједност ИС-а. Сви добављачи услуга којима је потребан приступ ИС-у, обавезни су да потпишу одговарајући уговор о пословној сарадњи којим се дефинишу њихова права и обавезе, као и уговор о чувању повјерљивих информација.

Д.4.1. Екстернализација административних зона

Екстернализације административних зона није предмет екстренализације. Дио администартивних зона управљан је од стране „техничких" факултета, а остале зоне од стране УРЦ.

Д.5. Контрола приступа

Физички и електронски приступ информацијама, документима, радним станицама, серверима, комуникационим уређајима и мрежама, оперативним системима и апликацијама је контролисан. У циљу постизања адекватне заштите контролисање се спроводи на сљедећи начин:

- ауторизација - права приступа се одобравају на бази принципа "потребно да зна" и "потребно да уради" и то искључиво на захтјев надлежног руководиоца. У зависности од система коме се приступа, ауторизација може бити одобрена на бази конкретног корисника, на бази његове улоге/радног мјеста, као и на бази контекста (нпр. са ког рачунара или *IP* адресе се приступа) или комбинацијом ова три принципа.
- идентификација (аутентификација) - приступ подацима и апликацијама се омогућава искључиво на бази јединствене корисничке идентификације (корисничког налога) на основу које је познато о ком запосленом, клијенту или партнеру се ради. Да би приступио подацима корисник користи лозинку као метод идентификације.
- управљање лозинкама – све корисничке лозинке треба да буду криптоване и познате само кориснику којем припадају. Корисници који приступају информационом систему одговорни су за све активности које се изврше у ИС-у под њиховим корисничким налогом. С тога, корисник треба да обезбједи тајност своје лозинке како друга лица не би могла да је открију и злоупотријебе. Са друге стране, лозинке је потребно креирати на начин да прате најбољу праксу у одређивању најмање дужине лозинке, обавезне структуре лозинке, могућности понављања саме лозинке у систему и сл.
- удаљени приступ - приступ мрежи Универзитета споља може се омогућити само када је то неопходно и то искључиво на бази појединачних корисника и апликација и само кроз одговарајуће уређаје и системе уз примјену правила аутентификације. Удаљени приступ треба да буде криптован.
- привилеговани приступ - привилеговани приступ ресурсима ИС-а којим се заобилазе системске и апликативне контроле омогућава се уз строго поштовањем сљедећих принципа:
    - привилеговани приступ се користи искључиво за радње које се не могу обавити помоћу стандардног приступа,
    - врши се идентификација свих лица, процеса и система са привилегованим приступом,

- привилеговани приступ се ограничава на одређен временски период и/или одређену активност.

- Физички приступ - физички приступ информацијама као и областима у којима се одвија процесирање информација треба бити контролисан и ограничен искључиво на ауторизована лица. У циљу обезбјеђења физичке заштите информација и ИС-а примјењују се сљедећи принципи:
  - сви сервери и комуникациона опрема требају бити инсталирани у просторијама са контролисаним приступом уз евиденцију приступа,
  - преносне радне станице, меморијски медији са подацима и документи у папирном облику требају бити заштићени од неовлашћеног коришћења.

Д.6. Безбједност административних зона

Д.6.1. Размјештај и степен безбједности

Административне зоне се према степену безбједности дијсле на зоне:

- Високог ризика – зоне са ограниченим приступом (сервер сала УРЦ, сервер сале факултета и института)
- Средњег и ниског ризика (јавне зоне)

За административне зоне високог ризика потребно је обезбиједити посебне услове:

- Приступ – евиденција улазака и излазака из зоне
- Форме идентификације запослених и гостију
- Давање и провјера права приступа

Препоручује се додатно:

- Коришћење двофакторске аутентикације
- Видео надзор
- Усклађеност са Законом о заштити од пожара
- Имплементација сензора за влагу или заштите од поплава

Д.6.2. Означавање адмнистративних зона

Административне зоне високог ризика требају се ненаметљиво означавати, тако да обични посјетиоци не могу препознати сврху осјетљивих објеката и опреме.

Размјештај и степен безбједности адмнн. зона координира се организационим дијеловима Универзитета.

Д.7. Безбједно коришћење информационог система

Д.7.1. Коришћење интернета

Приступ и коришћење интернета је доступан свим запосленим у Универзитету, с тим да је приступ интернету регулисан. Регулисање интернета је урађено на начин да одговара пословним потребама запослених у складу са њиховим радним позицијама. Запослени у своме раду треба да воде рачуна да интернет користе на начин да не угрозе безбједност ИС-а и података у Универзитету. То значи да запослени требају употребу интернета да ограниче на потребе посла и то на начин да воде рачуна да странице којима приступају нису странице које су ризичне или могу бити ризичне за безбједност ИС-а и података Универзитета.

Универзитет задржава право да у сврху обезбјеђења безбједности ИС-а надгледа и администрира приступ интернету.

Д.7.2. Коришћење електронске поште

Сваком запосленом се отвара адреса за електронску пошту и она је јединствена за сваког запосленог. Запослени су дужни да коришћењем електронске поште не компромитују Универзитет и не угрозе безбједност информационог система. То значи да су обавезни електронску пошту користити на начин да воде рачуна о ономе што шаљу и коме шаљу, какву пошту су добили и од кога су је добили, као и да адресу електронске поште не користе за регистровања на садржајима који нису повезани са пословањем Универзитета.

Универзитет задржава право да у случају потребе и на захтјев надлежног државног органа, односно овлашћених лица у Универзитету, приступи свакој електронској пошти, посебно када постоји основана сумња да је угрожена безбједност, учињено кривично дјело или је извршена повреда радне обавезе.

Д.7.3. Коришћење факс уређаја, штампача, копир апарата и скенера

Коришћењем факс уређаја, штампача, копир апарата и скенера, корисници могу угрозити повјерљивост података, а на тај начин и безбједност ИС-а. Да би се то избјегло, корисници треба да се придржавају сљедећег:

- повјерљиве документе послане или примљене путем факса потребно је одмах склонити са факс уређаја

- повјерљиве документе одштампане на заједничким штампачима обавезно је одмах преузети са штампача
- повјерљиве копије докумената, као и њихове оригинале, потребно је одмах склонити са копир апарата
- повјерљива документа која се скенирају на заједничком скенеру, треба одмах да се пруzму и обришу из система скенера како им друга лица не би имала приступ,
- радни папири и документи који се бацају, а садрже било какве информације или податке, морају се на одговарајући начин уништити (уништити физичким путем или помоћу уређаја).

Д.8. Заштита од малициозног кода

Софтвер за заштиту оперативног система од малициозног кода (антивирусна заштита) поставља се на свим нивоима (радне станице, сервери, системи електронске поште) како би била обезбијеђена адекватна заштита. Он треба да буде лиценциран и у складу са потребама Универзитета. Његову инсталацију врше искључиво овлашћена лица из УРЦ-а или администратори у организационим јединицама.

Д.9. Електронски канали за комуникацију са корисницима ИС

Приликом размјене информација и обављања електронских сервиса, као и током вршења трансакција путем јавне мреже, Универзитет ће обезбједити заштиту која је прописана подзаконским актима Републике Српске. Процедуре аутентикације и ауторизације ће се спроводити за све финансијске и нефинансијске трансакције, информацијске и трансакцијске сервисе. Све јавно доступне информације ће се заштитити од неовлашћених измјена, а веб стране Универзитета ће се идентификовати квалификованим сертификатима.

Д.10. Управљање системским записима ИС

Универзитет ће успоставити одговарајући процес управљања системским записима (лог фајловима), те дефинисати критерије за идентификовање критичних догађаја који се провјеравају, као и њихово документовање и чување. Лог фајлови требају садржавати само информације захтијеване за идентификацију забиљеженог догађаја и морају бити ограничене на оно што је нужно за идентификацију догађаја.

Информације које пружају лог фајлови су информације повјерљивог садржаја и као такве ће се заштитити од неовлашћеног приступа и промјена. Те информације ће се чувати на временски период који дозволе техничке могућности. Приступ лог фајловима треба да има администратор за безбједност информационог система и интерна ревизија за потребе својих активности када лог фајлови могу помоћи у конкретној ревизији.

Континуиране или неселективне контроле лог фајлова су забрањене, изузев у случају вршења истражних активности. У случају захтјева од стране овлаштених државних институција за приступ лог фајловима потребно је евидентирати примопредају ових података у складу са важећим актима Универзитета.

Д.11. Пријављивање инцидената везаних за ИС

Инциденти су неизбјежна посљедица употребе информационог система. Битно је да се инциденти на вријеме идентификују и да се на вријеме укаже на њих надлежним лицима. Пријављивање инцидената ће се ријешавати системски кроз апликацију која је дио информационог система Универзитета. Сви запослени су дужни да у случају сазнања о појави инцидента одмах пријаве тај инцидент.

Д.12. План за дјеловање у ванредним ситуацијама ИС

Универзитет ће прописати и редовно ажурирати одговарајуће планове који гарантују да се Универзитет може опоравити од било које штете на документима или опреми у разумном временском периоду, а посебно у ванредним околностима (нпр. пад система, дјеловање хакера и преваре, нестанак електричне енергије, природне катастрофе, вандализам и сл.). Ово укључује, али се не ограничава, на сљедеће планове:

- План континуитета пословања,
- План опоравка пословања.

Д.13. Мрежна безбједност

Да би се смањиле сигурносне пријетње у рачунарској мрежи, потребно је да се користе различити уређаји, технологије и технике за филтрирање саобраћаја. Свака организациона јединица која жели да побољша ефикасност филтрирања и ниво безбједности своје мреже, треба да примјени сљедеће препоруке:

1. Да дефинише правила о филтрирању саобраћаја (*packet filtering/firewall policy*), којима ће бити одређено како се регулише проток долазног и одлазног саобраћаја на мрежи.
2. Да се у складу са захтјевима и потребама опредијели за технологију филтрирања саобраћаја која ће се имплементирати.
3. Да на изабраној технологији, изврши имплементацију дефинисаних правила и усклади их са перформансама уређаја.
4. Да одржава све компоненте рјешења, што укључује не само уређаје, већ и релевантне документе и процедуре.

Посебна пажња треба се посветити директном повезивању (оптичком влакнима) издвојених локација Електротехничког факултета, Природно-математичког факултета, Медицинског факултета и Рударског факултета са основном мрежом како би се правила мрежне безбједности конзистентно пропагирала у интерној рачунарској мрежи Универзитета.

Д.13.1 Политика удаљеног приступа (RemoteAccess Policy)

Осигурање удаљеног приступа обавезно се контролише са енкрипцијом, односно виртуелним приватним мрежама (Virtual Private Networks - VPN) и јаким приступним лозинкама.
Приликом повезивања рачунара из мреже Универзитета или мреже информационог система универзитета корисници требају обезбиједити да удаљени хост није истовремено повезан и са другим мрежама у исто вријеме (мреже које нису под контролом двије повезане стране).
Коришћење екстерних ресурса треба надзирати администратор за безбједност информационог система/администратор безбједности
Повезивање приватних уређаја у мрежу мора бити усклађено са правилима која важе за трећа лица и партнере.

Д.13.2 Безбједносна политика мрежних уређаја (Network Devices Security Policy)

Добављачи и корисници не могу повезивати уређаје који нису претходно верификовани и одобрени. Руководилац УРЦ одобрава све мрежне и бежичне уређаје који се повезују у мрежу Универзитета у Кампусу 1 и Кампусу 2.

Д.13.3 Безбједносна политика опреме у ДМЗ (DMZ Security Policy)

Продукциони системи не смију зависити од ресурса у DMZ дијелу мреже. DMZ дио мреже не смије се повезивати са интерним мрежама Универзитета, било директно или преко бежичне везе. Препоручује се да DMZ дио мреже буде смјештен у физички одвојеном простору од интерног дијела мреже. Ако то није могуће потребно је обезбиједити рек ормаре са ограниченим приступом, те водити дневник приступа опреми.

Једино firewall уређај може бити приступна тачка између DMZ дијела мреже и осталих мрежа Универзитета и/или интернета. Свака форма повезивања која заобилази firewall уређај је стриктно забрањена. Све измјене конфигурација треба надзирати администратор за безбједност информационог система.

Д.13.4 VPN политика (VPN Policy)

Администрацију VPN политика на Универзитету обавља УРЦ. Факултети су одговорни да у координацији са УРЦ имплементирају VPN везе, набавке интернет сервиса (Internet Service Provider - ISP), координацију имплементације и инсталације софтвера и плаћање припадајућих трошкова. Даљи детаљи су појашњени у Политици удаљеног приступа (Remote Access Policy).

Д.13.5 Политика бежичне комуникације (Wireless Policy)

Бежичне мреже неће се користити за потребе информационог система Универзитета или друге пословно критичне процесе.

Д.13.6 Политика ИП телефоније (IP Telephony Policy)

Потребно је одржавати тајност свих података одговарајућим контролама приступа. Ниједан екстерни приступ интернету или другим екстерном сервису не треба дозволити према / из центра IP телефоније.
Рестрикције позива треба имплементирати глобално на свим кластерима.
Само овлаштена лица могу приступити IP опреми у сервер салама, као и конфигурацијама и подацима IP телефоније.
Према могућностима потребно је користити енкрипцију.

Д.13.7 Политика енкрипције (Acceptable Encryption Policy)

Приликом енкрипције потребно је обезбиједити минималне или више услове из "AES-компатибилних" или "дјелимично AES-компатибилних" каталога енкрипције које објављује IETF/IRTF.
Размјена кључева мора да користи један од слиједећих протокола: DiffieHellman, IKE или „Elliptic curve Diffie-Hellman" (ECDH). Потребно је извршити аутентикацију прије размјене/дервиације session кључева. Сервери који се користе за аутентикацију (RADIUS или TACACS) треба да имају валидне сертификате. Сви сервери и апликације које користе SSL или TLS треба да користе квалификоване сертификате.

Д.13.8 Екстранет политика (Extranet Policy)

Повезивање трећих страна које захтијева повезивање интерних ресурса Универзитета, без обзира да ли су у питању мреже провајдера или ВПН везе (осим провајдера интернета или телефоније), одређено је овом политиком. Све ванске (extranet) везе морају проћи безбједносну анализу од стране Службе безбједности/Администратора за безбједност информационог система. Безбједносна анализа треба да усклади захтјева за повезивањем са минималним пословним потребама, односно да на најбољи начин примијени принцип минималног могућег приступа.

Д.13.9 Политика приступа интернету (Internet Access Policy)

Бежични приступ интернету је одвојен од локалне мреже Универзитета. Приступ интернету за сегмент изван рачунарске мреже Универзитета (бежични приступ и приступ за госте) је слободан, али и редовно надзиран и контролисан из безбједносних разлога.

Д.13.10 Политика приватних уређаја (BYOD)

Запосленима није дозвољена употреба властитих мобилних уређаја/таблет/преносних рачунара у заштићеној приватној мрежи Универзитета (мрежа информационог система универзитета или други домени са дефинисаним високим стандардима безбједности).

Д.14. Резервне копије података

Системи морају да обезбиједи механизме заштите (backup) свих програма и података (табела и фајлова, како активних тако и архивских) те враћања истих у претходно оперативно стање (restore). Периодично треба да се изводи аутоматски 'backup' података, без прекида у раду система,

За потребе припреме резервних копија података организациони дијелови универзитета треба да припреме каталог сервиса на годишњем нивоу са распоредом процедура копирања и ресторације података.

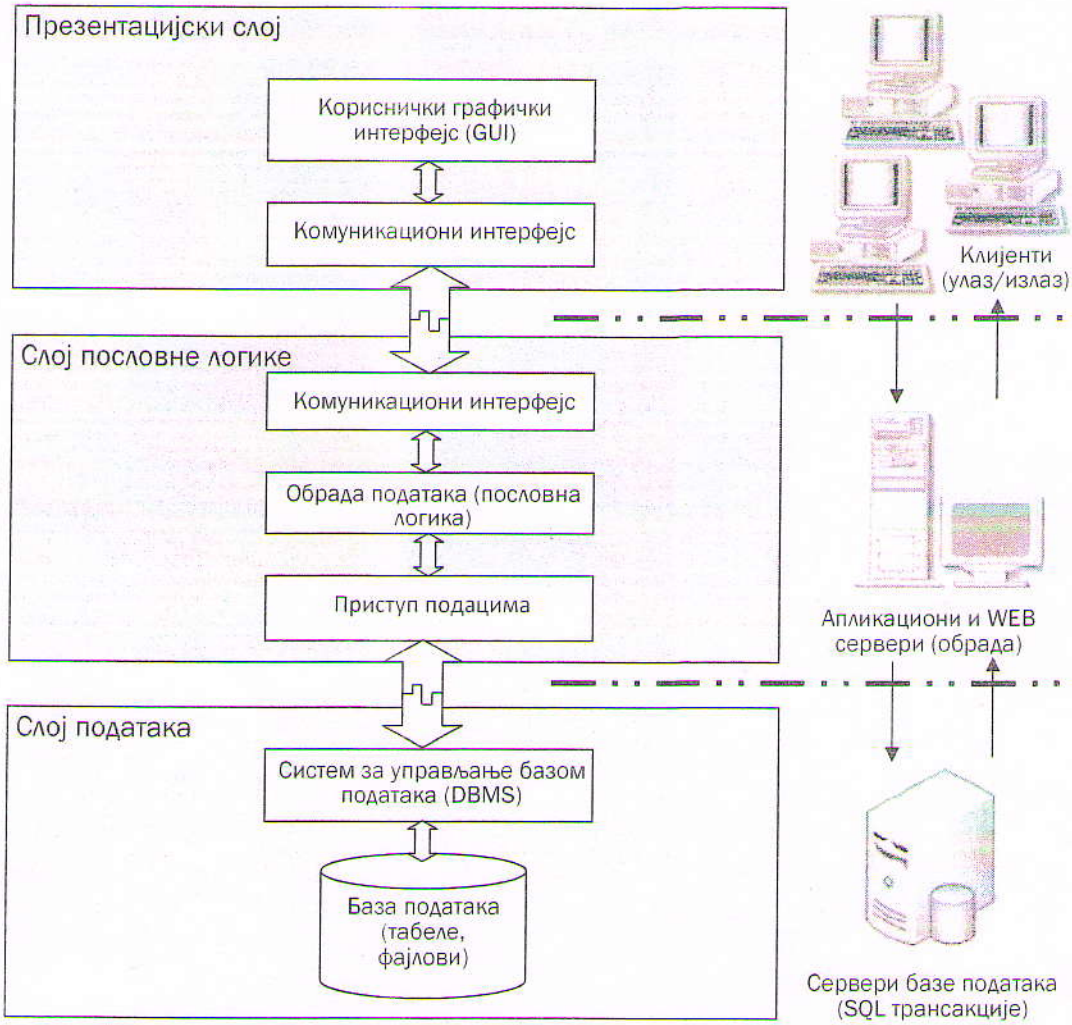
Д.15. Нормализација података

Сви подсистеми ИСУБЛ требају бити интегрисани на принципу 'један податак на једном мјесту'. Неки подаци могу се уносити са различитих мјеста, али једном инесен податак смјешта у базу на јединствено мјесто и путем размјене података између модула користи на свим мјестима на којима је потребан, како унутар система тако и у комумикацији са екстерним системима. Другим ријечима, потребно је обезбиједити аутоматску размјену података између различитих подсистемима ИСУБЛ, као и са екстерним системима са којима су повезани пословни процеси ИСУБЛ. Уколико табеле базе података садрже изведена поља, тј. поља чији се садржај може добити обрадом других, постојећих поља, морају постојати трансакције за њихово ажурирање чим дође до измјене постојећих поља.

Д.16. Препоручена архитектура информационог система

Пожељна је интеракција на бази вишеслојне, сервисно орјентисане архитектуре (SOA), састављене од најмање три слоја: презентацијског слоја, слоја пословне логике и слоја података (слика 0).

У функционисању система не смије бити заобилажења слојева, што значи да се презентацијски слој не смије обраћати директно бази података.



Слика: Слојевита архитектура ИСУБЛ

Презентацијски слој треба да обезбиједи екранске форме и прозоре за унос и приказ података и да при томе обавља само минорне операције обраде података.

Главнина обраде треба да се изводи у оквиру слоја пословне логике. Ту се захтјеви са улаза комбинују са подацима из базе података, обрађују по правилима пословања и добијени резултати прослеђују презентацијском слоју за приказ и/или систему за управљање базом података за ажурирање садржаја.

Како су данас DBMS све способнији један дио пословне логике може се предати у надлежност DBMS систему. Баланс између апликацијског слоја и слоја података ствар је пројектног рјешења, али понуђач треба да образложи како је постигао оптималан баланс. Услов који се при том мора испунити је да не дође до дуплања пословних правила у апликацијском слоју и слоју података.

Апликацијски слој треба да буде независан од базе података, односно да без репрограмирања ради са различитим базама података, најмање сљедећим: *Oracle, MS SQL, DB2, MySQL, Postgress.*

Поред логичке вишеслојне структуре, систем треба да се одликује и физичком вишеслојном, најмање трослојном структуром. То подразумијева да се поједини слојеви физички раздвоје тако што се њихове компоненте (exe, dll, Activex, фајлови) распореде

на различите машине (рачунаре). Такво рјешење омогућује боље прилагођавање перформанси машине захтјевима процеса појединог слоја, увођење сигурносних мјера на нивоу хардвера итд.

База података треба да буде релационог типа, најмање MS SQL SERVER 2008 технолошког нивоа. Интегритет базе података не смије бити угрожен погрешним руковањем корисника нити системским отказима.

Систем мора бити проширив од стране особља Универзитета, што значи да се функције које недостају у базном систему могу накнадно имплементирати и једноставно интегрисати у систем. То подразумијева могућност додавања нових модула, ентитета и атрибута.

Систем треба да обезбиједи могућност паралеланог рада више стотина корисника, на свим модулима и на истим процесима обраде. Изузетно, подсистем студентске службе (поглавље **Error! Reference source not found.**) и *web* портал (поглавље **Error! Reference source not found.**) требају подржати истовремени рад и више хиљада корисника. Треба постојати и могућност проширења броја корисника. Времена одзива морају бити сведена на најмању могућу мјеру (за on-line упите о појединачним студентима, предметима, резултатима испита итд., за сваког корисника одзив мора бити < 2sec). У операцијама које захтијевају дуже вријеме (статистички прегледи, извјештаји и сл.) потребно је пружити обавјештење кориснику у облику прогрес барова, штоперица и слично.

Унос података у систем мора бити ефикасан што укључује постављање подразумијеваних вриједности гдје год је то прикладно, минимизацију броја екрана и могућност коришћења пречица са тастатуре за врло учестале команде и податке. Неопходно је да постоји механизам за исправку грешака при уносу. Кориснички интерфејс треба да буде интуитиван, једноставан и да корисницима нуди само релевантне опције. Елементи интерфејса (менији, палете, дугмад, функцијски тастери) треба да буду слични у свим подсистемима и њиховим модулима.

Е. Политика класификације информација

Ова политика дефинише основна правила и принципе за процес управљања информацијама (које су садржане у паирној и/или електронској форми) који укључује двије фазе: класификацију информација и коришћење информација. Класификација информација се користи за унапређење одговарајућих контрола за заштиту тајности информација. Потребно је чувати интегритет свих класа информација неовисно од њиховог сврставања по класама. Додељена класификација и њене припадајуће контроле се примењују у зависности од осетљивости информација које садрже. Информација се класификује према најосјетљивијем детаљу који садржи. Може се чувати у више формата (изворни доцумент, електронски документ, извештај) и очувати исту класификацију независно од формата. Слиједећи нивои се користе за класификацију информација:

Е.1. Информација крајњег корисника

Представља информацију, усмену или писану или у било којој форми ли медијуму која:

- Креирана од стране крајњег корисника (организациони дијелови Универзитета, запослени, студенти, гости)
- Односи се на прошли, садашњи или будући садржај услуга крајњег корисника
- Укључује демографске податке или друге податке који се могу користити за идентификацију података крајњег корисника

Неауторизована или неодговарајућа измјена, објављивање или деструкција ових информација може довести до кршења закона, кривичног гоњења и донијети озбиљну штету Универзитету.

Е.1. Тајна информација

Тајна информација је веома значајна и веома осетљива информација која није класификована као информација крајњег корисника. Та информације је привате или веоме осетљиве природе и мора бити ограничена на оне који имају пословну потребу да јој приступе. Примјери тајних информација су: информације о запосленима у организационим дијеловима, лозинке за приступ систему, кључеви за енкрипцију.
Неауторизовано давање ових информација без пословне потребе може довести до прекршаја закона или регулативе, изазвати озбиљне проблеме за Универзитет и његове кориснике или његове пословне партнере. Одлука о давању приступа овим информацијама мора се разјаснити са власником информације.

Е.3. Интерна информација

Интерна информација може се без ограничења користити унутар организационих дијелова Универзитета и у неким случајевима са повезаним организцијама као што су повезана правна лица (Универзитет у Источном Сарајеву) и пословни партнери.

Овај тип информација је већ широко присутан унутар Универзитета и може се даље дистрибуирати унутар организационих дијелова без претходне сагласности власника информација.

Свака информација која није дефинисана као информација крајњег корисника, тајна или јавна, по дефиције се класификује као интерна информација.

Неаутроизовано давање интерних информација ван организације може довести до правних или уговорних казни.

Е.4. Јавна информација

Јавна информација је посебно одобрена за јавну употребу од стране одговорног ауторитета из органа управљања Универзитета. Примјери Јавне информације могу бити маркетиншке брошуре и материјали објављени на веб странама Универзитета и његових чланица.

Напомена:

Релевантна документа, правилници и литература може се преузети са универзитетске web странице: www.unibl.org