

На основу члана 53. Закона о високом образовању („Службени гласни РС“, бр. 76/2005, 100/2007 аутентично тумачење, 97/2008, 44/2010, 93/2012 и 89/2013), члана 15. Статута Факултета спорта и физичког васпитања у Нишу, Предлога Правилника Наставно-научног већа Факултета бр. 04-311/13 од 26.02.2014.године, Савет Факултета спорта и физичког васпитања у Нишу на својој седници одржаној 19.03.2014. године донео је следећу

ОДЛУКУ

ДОНОСИ СЕ Одлука о усвајању ПРАВИЛНИКА О ИТ БЕЗБЕДНОСТИ ФАКУЛТЕТА СПОРТА И ФИЗИЧКОГ ВАСПИТАЊА У НИШУ.

Текст Правилника саставни је део ове Одлуке.

Одлуку доставити: Одељењу за рачунарско-информационе послове, општој служби и писарници Факултета.

САВЕТ ФАКУЛТЕТА СПОРТА И ФИЗИЧКОГ ВАСПИТАЊА У НИШУ

Бр. 04- 532/3

У Нишу, 19.03.2014. године

ПРЕДСЕДНИК САВЕТА
Проф. др Саша Миленковић



На основу члана 53. Закона о високом образовању („Сл. гласник РС“ 76/2005, 100/2007 – аутентично тумачење, 97/2008, 44/2010, 93/2012, 89/2013) члана 15. Статута Факултета спорта и физичког васпитања у Нишу, Предлога Правилника Наставно-научног већа Факултета бр.04-311/13 од 26.02.2014. године, Савет Факултета спорта и физичког васпитања у Нишу на својој седници одржаној дана 19.03.2014. године донео је

ПРАВИЛНИК

О ИТ безбедности Факултета спорта и физичког васпитања у Нишу

Уводне одредбе

Члан 1.

Овим Правилником уређује се сигурност информационих система на Факултету спорта и физичког васпитања у Нишу (даље: Факултет).

Правилник се односи на:

- рачунарске системе,
- рачунарску опрему која се користи у просторијама Факултета,
- рачунарску опрему која је на задужењу ван просторија Факултета,
- администраторе рачунарских система,
- кориснике, међу које спадају: запослени, спољни сарадници, студенти.

Организација управљања сигурношћу

Члан 2.

Особе које се користе рачунарским системима на Факултету деле се на даваоце информационих услуга и кориснике информационих услуга.

Даваоци информационих услуга су запослени у Одељењу за информационе послове Факултета а корисници информационих услуга су особе које се у свом раду или образовању служе рачунарским ресурсима и системима Факултета.

Безбедност рачунарских система

Члан 3.

Свака апликацију или рачунарски систем које Факултет користи за обраду података, а која је од важности за Факултет, мора имати одговорно лице (администратора) које се брине о правилном коришћењу апликације или рачунарског система.

Одговорно лице одређује декан на темељу специфичности поједине апликације или рачунарског система.

Одговорно лице је дужно да обезбеди несметан рад корисницима који користе апликацију или рачунарски систем, као и да се брине о безбедности података и правовременом прављењу резервних копија података. Одговорно лице даље регулише права приступа додељеним апликацијама и рачунарским системима.

Члан 4.

Корисници који користе рачунарске системе Факултета, дужни су да приликом обављања својих послова или едукације, ни у једном тренутку свесно не доведу систем у неоперативно стање.

Најстроже је забрањено инсталирање вируса и малаверних апликација у циљу угрожавања стабилности рачунарских система Факултета или било ког корисника ван рачунарске мреже Факултета.

Забрањено је инсталирање апликација (keylogger-а, spyware-а) у циљу прибављања личних и службених података о корисницима као што су: корисничка имена, лозинке и сл.

Забрањено је инсталирање поменутих програма из Члана 4. у едукативне сврхе.

Члан 5.

Неопходно је обезбедити да се на сваком рачунарском систему Факултета налази инсталиран лиценцирани антивирусни програм који своју базу вируса надограђује самостално на дневном нивоу без интервенције администратора система.

Члан 6.

Корисници су дужни да приликом уношења података у рачунарске системе Факултета (путем USB меморијских уређаја, CD-DVD медија, електронске поште, cloud система и сл.) користе антивирус у циљу утврђивања безбедног коришћења унетих података.

У случају инфекције рачунарског система, корисници су дужни да обавесте надлежног администратора.

По добијању информација од стране корисника о инфекцији рачунарског система, администратор је дужан да у што краћем року отклони настали проблем. Администратор је дужан да води дневник о оваквим појавама у циљу анализе и спречавања поновних инфекција или штетног деловања корисника.

Члан 7.

Забрањено је без знања и сагласности администратора мењати мрежне параметре на рачунарским уређајима и системима.

Члан 8.

Администратори рачунарских система свакодневно прате рад истих, проверавају лог записе и рад сервиса.

Члан 9.

Обзиром да је Факултет део Јединственог универзитетског наставно-научног информационог система (ЈУНИС), администратори рачунарских система Факултета су дужни да прате безбедоносне билтене и у што краћем року одговоре на добијене информације о безбедоносним пропустима и проблемима везаних за мрежу или рачунарски систем који администрирају.

Физичка сигурност

Члан 10.

Рачунарска опрема од виталног значаја за Факултет (мрежно чвориште и сервери) се налази инсталирана у просторијама Одељења за информационе послове.

Члан 11.

Рачунарско - комуникациона опрема мора да буде физички заштићена од неовлашћеног приступа.

Члан 12.

Рачунарско - комуникациона опрема мора да буде под сталним видео надзором.

Члан 13.

Рачунарска опрема у Одељењу за Информационе послове мора да буде прописно хлађена и прикључена на уређаје за непрекидно напајање, чија је аутономија деловања прописана од стране произвођача.

Члан 14.

Рачунарска учионица која је предвиђена за коришћење од стране студената мора да буде под видео надзором.

Члан 15.

Потребно је да постоји списак ИТ опреме коју Факултет поседује са описом уграђених компоненти.

Члан 16.

Запослени на Факултету могу по формацијској дужности или из другог разлога да буду задужени рачунарском опремом и да је износе ван Факултета. За такву опрему мора да постоји обострано потписан реверс са даном задужења и описом опреме заведен у правној служби Факултета.

Права приступа корисника

Члан 17.

Право приступа кориснику неке апликације или рачунарског система додељује администратор тог система путем корисничког имена и лозинке.

Лозинка која је додељена кориснику је службена тајна и тако се према њој треба односити. Забрањено је давати информације другим корисницима о корисничком идентитету и лозинки. Најстроже је забрањено преузимање туђег идентитета.

У циљу безбедног коришћења рачунарских система Факултета на које се корисник пријављује, пожељно је да корисник у двомесечном периоду промени лозинку. Забрањено је за лозинку користити име корисника, надимак, датум рођења, број телефона или једноставан сет карактера (123, spase и сл.).

Лозинка треба да садржи насумичан сет изабраних карактера који укључују бројке и (комбинација малих и великих) слова као и неки од специјалних карактера (+-*# и сл.).

У случају да кориснички налог буде злоупотребљен због примене једноставне лозинке или давања исте другом на коришћење, корисник налога сам сноси евентуалне последице настале услед губитка података а у посебним условима и кривичну одговорност.

Члан 18.

Забрањено је без знања администратора прикључивати на рачунарску мрежу приватну (гостујућу) рачунарско – комуникациону опрему (радне станице, лаптоп рачунаре, таблет рачунаре, мобилне телефоне и сл.). Администратори морају да поседују списак (гостујуће) опреме, која је прикључена на рачунарску мрежу.

Члан 19.

Студентима није дозвољено коришћење рачунарске мреже на својим приватним рачунарско – комуникационим уређајима. Такво коришћење рачунарске мреже може да се одобри само ако је студент део неког истраживачког пројекта који спроводи Факултет. Корисник такве услуге по аутоматизму постаје особа која је у обавези да чува службену тајну.

Члан 20.

Свим студентима и гостима Факултета може да се омогући коришћење “отворене” рачунарске мреже али само ако је она одвојена од инфраструктуре (LAN-а) којом Факултет располаже.

Архивирање и чување електронских података

Члан 21.

Документи у електронском облику сматрају се службеним документима на исти начин као и документи у папирном облику па је сходно томе потребно осигурати њихово чување и приступ само овлашћеним особама.

Члан 22.

Сви запослени су дужни да самостално праве и на безбедан начин чувају резервну копију података за које су задужени.

Податке који су од виталног значаја за Факултет архивира и чува администратор система, коме је додељена та обавеза.

За чување одређених података могу бити именовани различити администратори.

Електронска комуникација запослених

Члан 23.

У циљу правовременог обављања пословних задатака, давања информација и службене комуникације користи се службена електронска пошта. Службена електронска преписка је службена тајна.

Члан 24.

Сви запослени на Факултету су дужни да поседују службену е-маил адресу и да је свакодневно користе.

Члан 25.

Службена електронска пошта је сервис, који има свог администратора и који гарантује правовремену размену информација између корисника службене електронске поште.

Члан 26.

Због осетљивости службених података није препоручљиво користити комерцијалне е-маил клијенте у службене сврхе.

Спољни сервис

Члан 27.

Факултет може да користи спољне сервисе (као што је хостовање система ван рачунарске мреже Факултета или извршавање апликација од виталног значаја) и у том случају фирма/институција који обавља хостовање тог сервиса или администрирање апликације, дужна је да обезбеди правилан рад сервиса, његову безбедност као и прављење резервних копија.

Члан 28.

Правилник ступа на снагу по усвајању на седници Савета Факултета.

САВЕТ ФАКУЛТЕТА СПОРТА И ФИЗИЧКОГ ВАСПИТАЊА У НИШУ

Број: 04-532/3

У Нишу, 19.03.2014. године

Председник Савета

Проф. др Саша Милековић

