На основу члана 73. Статута Универзитета у Београду, Факултета ветеринарске медицине, Наставно-научно веће Универзитета у Београду, Факултета ветеринарске медицине на 236-седници од 23.11.-2022. године доноси

ПРАВИЛНИК О ЧУВАЊУ, ЗАШТИТИ И СИГУРНОСТИ ПОДАТАКА У ОКВИРУ ИНФОРМАЦИОНОГ СИСТЕМА ФАКУЛТЕТА ВЕТЕРИНАРСКЕ МЕДИЦИНЕ

I ОСНОВНЕ ОДРЕДБЕ

Члан 1.

Правилником о чувању, заштити и сигурности података у оквиру информационог система (у даљем тексту: Правилник) уређује се чување, заштита и сигурност података у оквиру информационог система који чине мрежна инфраструктура, серверска опрема, кориснички рачунари, програмска подршка и мрежни сервиси Универзитета у Београду - Факултета ветеринарске медицине (у даљем тексту: Факултет).

II ЦИЉЕВИ ЗАШТИТЕ ИНФОРМАЦИОНОГ СИСТЕМА

Члан 2.

Циљеви заштите информационог система су:

1) очување поверљивости података, чиме се онемогућава неауторизован приступ и коришћење података из информационог система;

2) заштита интегритета података, чиме се онемогућава измена података и гарантује аутентичност података;

3) очување расположивости података, чиме се омогућава реконструкција података у случају њиховог намерног или ненамерног оштећења.

Заштита из става 1. овог члана обезбеђује се кроз заштиту приступа рачунарској мрежи, опреми и просторијама у којима је смештена опрема, као и кроз заштиту приступа подацима.

Мерама заштите обезбеђује се заштита података и информација од случајних или намерних грешака, неовлашћеног коришћења и измена, уништења, оштећења, крађе, квара система, фалсификовања и злоупотребе података и информација у свим деловима информационог система.

III ЧУВАЊЕ, ЗАШТИТА И СИГУРНОСТ ПОДАТАКА

Члан 3.

Факултет је одговоран за чување, заштиту и сигурност података у оквиру информационог система, што подразумева:

1) заштиту од неовлашћеног приступа ресурсима који су предмет заштите, њихово неовлашћено коришћење или манипулације базом података информационог система од стране корисника;

2) заштиту интегритета података, њихову расположивост и неовлашћени увид у поверљиве податке;

3) заштиту базе података од вируса и осталих облика малициозних кодова;

4) осигурање преноса података из базе интерним корисницима;

5) чување података и управљање сигурносним копијама базе података у оквиру информационог система;

6) повраћај сачуваних података у случају губитка, оштећења или уништења рачунарске опреме информационог система;

7) инсталирање софтверске надоградње ради уклањања сигурносних проблема који се установе на бази података у оквиру информационог система или на повезаном софтверу;

8) праћење сигурносних инцидената у бази података информационог система ради предузимања корективних мера;

9) управљање сигурносним инцидентима, едукација и обука свих овлашћених особа ради стицања потребних знања о чувању и сигурности података;

10) физички приступ и заштита базе података у оквиру информационог система и рачунарске опреме;

11) одржавање рачунарске опреме информационог система.

IV МЕРЕ ЗАШТИТЕ ПРИСТУПА ИНФОРМАЦИОНОМ СИСТЕМУ

Члан 4.

Мере заштите информационог система су:

1) обезбеђење просторија у којима се примају, смештају и чувају подаци, прописаним мерама физичке заштите (портири и ноћни чувари, решетке на вратима и прозорима) и противпожарне заштите;

2) обезбеђење серверске опреме уређајима за непрекидно напајање електричном енергијом;

3) заштита од вируса и осталих облика малициозних кодова;

4) израда резервних копија података;

5) заштита приступа подацима.

Мере заштите приступа информационом систему су:

1) аутентификација - која представља процес утврђивања идентитета особе која жели да приступи информационом систему (кориснички налози за приступ рачунару или мрежном сервису);

2) ауторизација - представља право приступа рачунару или мрежном сервису и дозвољеним операцијама аутентификованим лицима;

3) немогућност порицања одговорности - што подразумева обезбеђење доказа да је неко извршио одређену радњу, односно трансакцију;

4) рестрикција приступа корисничких уређаја информационој мрежи Факултета.

V ПРИСТУП ИНФОРМАЦИОНОМ СИСТЕМУ

Члан 5.

Факултет управља корисничким налозима, правима приступа и корисничким лозинкама за интерне кориснике базе података.

Факултет је дужан да обезбеди приступ подацима у оквиру информационог система само од стране овлашћених лица.

Сваки приступ информационом систему мора бити аутоматски забележен јединственим идентификатором лица у бази података јединственог система, са тачним временом приступа.

О сазнањима у вези са покушајима неовлашћеног приступа информационом систему, администратори базе података дужни су да обавесте руководиоца Информационо-комуникационог центра.

VI ОДРЖАВАЊЕ, ПОПРАВКА И ПОВЛАЧЕЊЕ ИЗ УПОТРЕБЕ ОПРЕМЕ ЗА ИНФОРМАЦИОНИ СИСТЕМ

Члан 6.

Факултет обезбеђује одржавање рачунарске опреме за информациони систем, а у случају поправки, претходно спрема безбедносне копије података, како би се спречио њихов губитак.

Одржавање и поправка сервисне и мрежне опреме, врши се искључиво под надзором руководиоца Информационо-комуникационог центра на Факултету и/или трећих лица овлашћених за то од стране Факултета.

У случају повлачења рачунарске опреме из информационог система, због застарелости, неупотребљивости или квара, сви подаци претходно морају бити трајно и сигурно избрисани.

VII ЗАВРШНЕ ОДРЕДБЕ

Члан 7.

Овај Правилник ступа на снагу осмог дана од дана објављивања интернет страници Факултета.

Председник Наставно-научног већа
Декан
Факултета ветеринарске медицине
Проф. др Милорад Мириловић