NAZARBAYEV UNIVERSITY

«Назарбаев Университеті» дербес білім беру ұйымында және оның ұйымдарында антивирустық қорғауды қолдану қағидалары

Санаты: Қағидалар

Бекітілген күні: 03.06.2025

Күшіне енген күні: 03.06.2025

Қолжетімділік деңгейі: Ашық қолжетімділік

Сыныптауыш бойынша нөмірі: 7. IT

Бекітуші орган: Басқарушы кеңес

Тіркеу нөмірі: 03.06.25

Иесі: «Nazarbayev University IT Support» жеке мекемесі

Қайта қарау күні: 05.06.2028

Қолданылуы: НУ және оның ұйымдары

Күші жойылған құжаттар:

Атауы: «Назарбаев Университеті» дербес білім беру ұйымында вирусқа қарсы қорғанысты ұйымдастыру қағидасы

Күні: 25.04.2013

Тіркеу нөмірі: 4.4.1

Бекітуші орган: Атқарушы кеңес

1-бөлім. Мақсаты және қолданылуы

1.1. Осы «Назарбаев Университеті» дербес білім беру ұйымында және оның ұйымдарында антивирустық қорғауды қолдану қағидалары (бұдан әрі – Қағидалар) «Назарбаев Университеті» дербес білім беру ұйымының (бұдан әрі – Университет) виртуалды және физикалық серверлері мен корпоративтік құрылғыларын зиянды бағдарламалық жасақтамадан қорғауды ұйымдастыруға қойылатын талаптарды регламенттейді.

1.2 Осы Қағидалардың мақсаты Университеттің виртуалды және физикалық серверлері мен корпоративтік құрылғыларын зиянды бағдарламалық жасақтамадан тиісті қорғауды қамтамасыз ету болып табылады.

1.3. Осы Қағидалардың әрекеті мен талаптары Университеттің барлық виртуалды және физикалық серверлеріне және корпоративтік құрылғыларына, сондай-ақ Университет пен оның ұйымдарының корпоративтік желісіне қосылған жеке тұлғалардың жеке құрылғыларына қолданылады.

2-бөлім. Терминдер / Анықтамалар

2.1. Осы Қағидаларда мынадай терминдер, анықтамалар мен қысқартулар қолданылады:

1) **Сервер әкімшісі** – Университеттің немесе оның ұйымдарының құрылымдық бөлімшесінің физикалық немесе виртуалды серверді баптауды және қолдауды қамтамасыз ететін, сондай-ақ Университеттің корпоративтік құрылғыларының қауіпсіздігін қамтамасыз ететін жұмыскері;

2) **Антивирустық БЖ** – компьютерлерден және басқа корпоративтік құрылғылардан зиянды бағдарламалық жасақтаманы (вирустарды, трояндарды, шпиондық бағдарламаларды және зиянды бағдарламалық жасақтаманың басқа түрлерін) анықтауға, таратуға және жоюға арналған бағдарламалық жасақтама немесе бағдарламалық жасақтама жиынтығы;

3) **Зиянды БЖ** – бұл компьютерлерге, серверлерге, мобильді құрылғыларға немесе желілерге зиян келтіру, рұқсатсыз қол жеткізу, жүйелердің жұмысын бұзу, деректерді ұрлау немесе басқа да зиянды әрекеттер жасау мақсатында жасалған кез келген бағдарламалық жасақтама;

4) **Корпоративтік құрылғы** – Университеттің серверлерінде орналастырылған виртуалды машиналарды қоса алғанда, Университеттің деректері орналасқан компьютер немесе өзге де құрылғы;

5) **Корпоративтік желі** – деректердің қауіпсіз алмасуын, бірлескен жұмысты және бизнес-процестерді басқаруды қамтамасыз ету мақсатында Университеттің ақпараттық ресурстарын, пайдаланушыларын, құрылғылары мен жүйелерін біріктіретін жеке есептеу желісі;

6) **Қорғау объектілері** – зиянды БЖ-дан қорғалуға жататын виртуалды және физикалық серверлер, сондай-ақ корпоративтік құрылғылар;

7) **Пайдаланушы** – Университет балансына тіркелген корпоративтік құрылғыны иеленетін тұлға, сондай-ақ өзінің жеке құрылғысын Университеттің Корпоративтік желісіне қосқан тұлға;

8) **Мекеме** – Университет пен оның ұйымдарының ақпараттық жүйелері мен пайдаланушыларына техникалық қолдау мен сүйемелдеуді жүзеге асыратын «Nazarbayev University IT Support» жеке мекемесі.

2.2. Осы Қағидаларда қолданылған, бірақ айқындалмаған терминдер Қазақстан Республикасының заңнамасында және Университеттің ішкі нормативтік құжаттарында қолданылатын мағынада пайдаланылады.

3-бөлім. Негізгі ережелер

3.1. Антивирустық БЖ орнату

3.1.1. Университетте қолдануға тек қана Мекеменің Ақпараттық қауіпсіздік қызметі мақұлдаған лицензияланған Антивирустық БЖ рұқсат етіледі.

3.1.2. Қорғау Объектілері үшін Мекеменің Ақпараттық қауіпсіздік қызметі сатып алатын қорғау құралдары қолданылады.

3.1.3. Антивирустық БЖ-ны Мекеменің жұмыскерлері немесе сервер әкімшілері барлық қорғау Объектілеріне міндетті түрде орнатады.

3.1.4. Антивирустық БЖ-ны орнату қиын болған жағдайда әкімшілер өтінімді техникалық қолдау қызметіне – Университеттің IT Helpdesk порталына (https://helpdesk.nu.edu.kz/support/home) жібере алады.

3.1.5. Егер Пайдаланушы жеке құрылғысын Корпоративтік желіге қосса, онда сол құрылғыда қазіргі нұсқада жұмыс істейтін Антивирустық БЖ орнатылуы тиіс.

3.1.6. Егер Корпоративтік желіге қосылған жеке құрылғыда Антивирустық БЖ орнатылмаған болса, Мекеменің Ақпараттық қауіпсіздік қызметі мұндай құрылғыны Корпоративтік желіден ажыратуға құқылы.

Бұл ретте осындай құрылғының иесіне корпоративтік электрондық пошта арқылы тиісті хабарлама жіберілетін болады.

3.1.7. Техникалық немесе өзге де объективті себептерге байланысты Антивирустық БЖ-ны орнату мүмкін болмаған жағдайда Пайдаланушы бұл құрылғы үшін «ерекше жағдайды» Мекеменің Ақпараттық қауіпсіздік қызметімен келісіп, жазбаша негіздеме ұсынуға және балама қорғаныс шараларын қамтамасыз етуге міндетті.

3.2. Пайдаланушылардың шектеулері, құқықтары мен міндеттері

3.2.1. Пайдаланушыларға қойылатын шектеулер:

1) қорғау Объектілерінде орнатылған Антивирустық БЖ-ны өзгертуге немесе жоюға тыйым салынады;

2) Корпоративтік құрылғыларды Антивирустық БЖ-сыз пайдалануға тыйым салынады;

3) алдын ала Антивирустық БЖ арқылы тексерусіз алмалы ақпарат тасымалдағыштарды пайдалану ұсынылмайды;

4) белгісіз немесе сенімсіз дереккөздерден/веб-сайттардан немесе жіберушілерден алынған файлдарды (оның ішінде БЖ-ның пираттық көшірмелерін) ашуға тыйым салынады.

5) Корпоративтік құрылғыда зиянды БЖ-ны анықтау үшін сканерлеу жүргізіп жатқан Антивирустық БЖ-ның жұмысына кедергі келтіруге тыйым салынады.

3.2.2. Пайдаланушы зиянды БЖ-ның болуына күдік туындаған кезде (бағдарламалардың типтік емес жұмысы, деректердің бұрмалануы, файлдардың жоғалуы, жүйелік қателер туралы хабарламалардың жиі пайда болуы және инфекцияның басқа белгілері) қорғау Объектілерінде Антивирустық БЖ-ны жоспардан тыс тексеруді өз бетінше іске қосуы қажет.

3.2.3. Антивирустық БЖ арқылы жойылмайтын зиянды БЖ анықталған жағдайда Пайдаланушы бұл туралы тиісті өтінімді дереу Мекеменің Ақпараттық қауіпсіздік қызметіне жолдауы тиіс.

3.3. Бұзушылықтар үшін жауапкершілік

3.3.1. Пайдаланушылар осы Қағидалардың талаптарын сақтауы керек. Осы Қағидалардың талаптары бұзылған жағдайда Пайдаланушылар жауапкершілікке тартылуы мүмкін.

3.3.2. Бұзушылықтың сипаты мен ауырлығына байланысты мынадай шаралар қолданылуы мүмкін:

1) ескерту – алғаш рет бұзушылық болған жағдайда, егер ол елеулі салдарға әкеп соқпаса;

2) қолжетімділікті шектеу – бұзушылықты жойғанға дейін Корпоративтік құрылғыны уақытша бұғаттау.

3.3.3. Осы Қағидалардың талаптарының орындалуын бақылауды Мекеменің Ақпараттық қауіпсіздік қызметі жүзеге асырады.

4-бөлім. Босату

4.1. Қолданылмайды.

5-бөлім. Уақытша ережелер

5.1. Қолданылмайды.

6-бөлім. Қайта қарау

6.1. Осы Қағидалар бекітілгеннен кейін жыл сайын үш жыл бойы тексерілуге және қажет болған жағдайда қайта қаралуға тиіс.

7-бөлім. Өзара байланысты құжаттар

7.1. Қолданылмайды.