ATYRAU UNIVERSITY

КеАҚ «Х.Досмұхамедов атындағы Атырау университеті»

ЕРЕЖЕ

БЕКІТЕМІН
КеАҚ Х.Досмұхамедов атындағы
Атырау университетінің
Басқарма төрағасы - ректор
_____С.Н.Идрисов
«12» 09 2024 ж.

АВТОМАТТАНДЫРЫЛҒАН АҚПАРАТТЫҚ ЖҮЙЕМЕН (ААЖ) ЖҰМЫС ЖАСАУ БАРЫСЫНДА АҚПАРАТТЫҚ ҚАУІПСІЗДІК ТУРАЛЫ ЕРЕЖЕ

№ 223

Атырау 2024ж.

	Лауазымы	Т.А.Ә.	Қолы	Күні
Жасақтаған	АКТ әзірлеу және дамыту орталығының жетекшісі	Мендигалиев.Ж.Ж.		25.08.2024
Келісілді	Академиялық мәселелер жөніндегі проректор	Чукуров А.Е.		2.09.2024
Келісілді	Вице- проректор (цифрлік офицер)	Сүлейменова Ж.У		26.08.24
Келісілді	Сапа мониторинг кеңсесінің жетекшісі	Кайшыгулова Ж.Т.		27.08.24
Келісілді	Заңгер	Куанов К.С.		28.08.2024.

Мазмұны

1. ЖАЛПЫ ЕРЕЖЕЛЕР

1.1 Осы Ереже (АВТОМАТТАНДЫРЫЛҒАН АҚПАРАТТЫҚ ЖҮЙЕМЕН (ААЖ) ЖҰМЫС ЖАСАУ БАРЫСЫНДА АҚПАРАТТЫҚ ҚАУІПСІЗДІК ТУРАЛЫ ЕРЕЖЕ)Халел Досмұхамедов атындағы Атырау университетінде (бұдан әрі – Атырау университеті) «Platonus» автоматтандырылған ақпараттық жүйесінде (бұдан әрі – ААЖ) парольдерді жасау, өзгерту және тоқтату (пайдаланушы тіркелгілерін жою) процестерін ұйымдастырушылық-техникалық қамтамасыз етуді, парольдерді пайдалану бойынша қауіпсіздік шаралары, сондай-ақ логиндермен және парольдермен жұмыс істеу кезінде пайдаланушылар мен жүйеге техникалық қызмет көрсету қызметкерлерінің әрекеттерін бақылау.

1.2. Осы Ереженің талаптары Атырау университетінің қауіпсіздік шаралары мен ақпаратты қорғау кешенінің құрамдас бөлігі болып табылады.

1.3. Ақпараттық қауіпсіздікті қамтамасыз ету ақпараттың құпиялылығын, тұтастығын және қолжетімділігін сақтауды білдіреді. Ақпараттың құпиялылығы ақпаратқа тек уәкілетті тұлғалардың қол жеткізуін қамтамасыз ету арқылы, тұтастық – деректерге тек рұқсат етілген өзгертулер енгізу арқылы, қолжетімділігі – уәкілетті тұлғалардың қызметтік міндеттерін орындауы үшін деректерге қолжетімділікті қамтамасыз ету арқылы қамтамасыз етіледі.

1.4. Ереже мыналар үшін әдістемелік негіз болып табылады:

1)ақпаратты қорғауға бағытталған келісілген нормативтік, құқықтық, технологиялық және ұйымдастырушылық шаралар кешенін әзірлеу және жетілдіру;

2)ақпараттық қауіпсіздікті қамтамасыз ету;

3)ақпараттық қауіпсіздік талаптарын сақтау бойынша жұмыстарды жүргізу кезінде университеттің құрылымдық бөлімшелерінің қызметін үйлестіру.

1.5. Осы Ереженің талаптары мен шарттары университеттің барлық ақпараттық жүйелеріне қолданылады.1.7. Осы Ереже ЖОО-ның ақпараттық-коммуникациялық инфрақұрылымының (бұдан әрі – БҚИ) ағымдағы жай-күйі мен дамуының жақын перспективаларын ескере отырып әзірленген. Регламентте жұмыстың мақсаттары, міндеттері және құқықтық негіздері, жұмыс режимдері, сондай-ақ қауіпсіздік қатерлерінің талдауы сипатталған.

1.6. Ереженің негізгі мақсаттары:

1)өңделген ақпараттың болуы;

2)университеттің ИКИ тұрақты жұмыс істеуі;

3)компьютерлік техникамен сақталатын, өңделетін және байланыс арналары арқылы берілетін ақпараттың құпиялылығын қамтамасыз ету;

3)университеттің ақпараттық жүйелерінде сақталатын және өңделетін және байланыс арналары арқылы берілетін ақпараттың тұтастығы мен шынайылығы.

1.7. Қойылған мақсаттарға жету үшін келесі міндеттер қойылады:

1) университетте ақпараттық қауіпсіздік саласында бірыңғай саясатты қалыптастыру және іске асыру;

2) университеттің үздіксіз жұмысын қамтамасыз ету және ақпараттық қауіпсіздікке төнетін қатерлерді жүзеге асырудан, оларды ескерту және алдын алу арқылы экономикалық залалды барынша азайту;

3) ақпараттық қауіпсіздікке қатерлердің әртүрлі түрлерін іске асыру салдарын анықтауға, көрсетуге және жоюға бағытталған рәсімдерді айқындау;

4) ақпараттық қауіпсіздікті қамтамасыз ету мәселелерін шешу қажеттілігін ескере отырып, университет ішінде ақпараттандыруды басқару рәсімдерінің мазмұнына қойылатын талаптарды анықтау;
5) ақпараттық қауіпсіздік стандарттарының талаптарын сақтай отырып, ХКИ-де жұмыстарды жүргізу кезінде университет қызметін үйлестіру;
6) университеттің компьютерлік ақпараттық технологияларының қауіпсіздік деңгейін арттыру;
1.8. Осы Ереже ақпарат өңделетін университеттің құрылымдық бөлімшелеріне, оның ішінде әкімшілік деректері бар автоматтандырылған ақпаратты, таратылуы шектелген ақпаратты (ресми ақпарат) немесе дербес деректерді, сондай-ақ ақпаратты әзірлейтін, жүргізетін, қызмет көрсететін ұйымдарға қолданылады. университет жүйелері.
1.9. Басқа ақпараттық жүйелердің ақпараттық қауіпсіздігінің көлемін олардың иелері белгілейді. Ақпараттық жүйенің деректері ЖОО-ның компьютерлік ақпараттық жүйесіне енгізілген жағдайда, ақпараттық қауіпсіздік талаптары келісім-шарттар немесе ақпараттық жүйенің иесі мен ЖОО арасындағы өзара іс-қимылдың бірлескен ережелері шеңберінде қарастырылады.
1.10. IP пайдаланушылардың санаттарына мыналар жатады:
1) ішкі пайдаланушылар – Қазақстан Республикасының заңнамасына сәйкес ИР-ге рұқсаты бар, өз қызметін жүзеге асыратын және негізгі құқықтары мен міндеттері бар университет қызметкерлері;
2) сыртқы пайдаланушылар – университет қызметтерін тұтынушылар, оның ішінде университеттің ақпараттық технологияларын пайдаланатын тұлғалар;
3) көмекші персонал – техникалық қызмет көрсетуші, техникалық персонал және университетте өзара әрекеттесетін басқа АЖ иелері;
соның ішінде:
- телекоммуникациялық жабдыққа қызмет көрсетуге жауапты жергілікті желі әкімшілері;
- SA;
- бағдарламалық қамтамасыз етуді әзірлеушілер;
- жүйелік инженерлер, техникалық мамандар (жүйелерге техникалық қызмет көрсету) және т.б.
1.11. Осы Ереженің талаптары университетте ААЖ-ны пайдаланатын құрылымдық бөлімшелердің барлық қызметкерлеріне, профессорлық-оқытушылық құрамға және профессорлық-оқытушылық құрамға қолданылады.
1.12. Барлық ақпараттық жүйелерде парольдерді жасау, пайдалану, өзгерту және тоқтату процестерін ұйымдастырушылық қамтамасыз ету парольдермен жұмыс істеу кезінде орындаушылар мен жүйеге техникалық қызмет көрсету персоналының әрекеттерін орнату және бақылау және парольдерді құру, пайдалану, өзгерту және тоқтату процестеріне техникалық қолдау көрсету болып табылады. АКТ дамыту және дамыту орталығының мамандарына (бұдан әрі – ААЖ маманы) мекемелеріне жүктеледі.
1.13. Мекеменің компьютерлік техниканы пайдаланатын барлық қызметкерлерін құрылымдық бөлімшелердің басшылары Ереженің талаптарымен таныстырады. Ережемен танысу кезінде қызметкерлердің назары университеттің профессорлық-оқытушылық құрамы мен профессорлық-оқытушылық құрамының пароль туралы ақпаратты жариялау және жеке ақпараттың сыртқа шығуы үшін жеке жауапкершілік туралы ескертуге аударылады.

2.Нормативтік сілтемелер

1)«Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы» Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы No 832 қаулысы ;

2)ҚР ҚНжЕ 2.02-05-2009 «Ғимараттар мен құрылыстардың өрт қауіпсіздігі»;

3)ҚР ҚН 3.02-17-2011 «Құрылымдық кабельдік желілер. Жобалау стандарттары»;

4)ҚР СТ 34.005-2002 «Ақпараттық технологиялар. Негізгі терминдер мен анықтамалар»;

5)ҚР СТ 34.006-2002 «Ақпараттық технологиялар. Дерекқор. Негізгі терминдер мен анықтамалар»;

6)ҚР СТ 34.007-2002 «Ақпараттық технологиялар. Телекоммуникациялық желілер. Негізгі терминдер мен анықтамалар»;

7)ҚР СТ ИСО/МЭК 17799-2006 «Ақпараттық технологиялар. Қорғанысты қамтамасыз ету әдістері. Ақпараттық қауіпсіздікті басқару тәжірибесі кодексі»;

8)ҚР СТ ИСО/МЭК 27002-2009 «Ақпараттық технологиялар. Қолдау білдіреді. Ақпараттық қауіпсіздікті басқару тәжірибесі кодексі».

9)ҚР СТ ИСО/МЭК 27002-2015 «Қолдау білдіреді. Ақпараттық қауіпсіздікті басқару тәжірибесі кодексі».

3. ТЕРМИНДЕР МЕН АНЫҚТАМАЛАР

Осы Ережеде мынадай терминдер, олардың анықтамалары мен аббревиатуралары пайдаланылады:

Ақпараттық жүйе (АЖ) – мәліметтер мен ақпаратты сақтауға, беруге және өңдеуге және есептеулерді орындауға арналған бағдарламалық және техникалық құралдардың жиынтығы.

Ақпараттық қауіпсіздік (АЖ) – процестің үздіксіздігін қамтамасыз ету және тәуекелдерді барынша азайту мақсатында ақпараттың қауіпсіздігін (оның құпиялылығы, тұтастығы, қолжетімділігі) қауіптердің кең ауқымынан қамтамасыз ету.

Тіркелгі – AIS пайдаланушысы туралы ақпарат: пайдаланушы аты, пароль, жүйеде жұмыс істеу кезінде ресурстарға және артықшылықтарға қол жеткізу құқығы. Есептік жазбада қосымша ақпарат болуы мүмкін (ЖСН, телефон нөмірі және т.б.).

Ең аз артықшылық принципі – жүйенің әрбір субъектісіне жүктелген міндеттерді орындау үшін қажетті өкілеттіктердің ең аз жиынтығы (немесе ең аз рұқсат) берілетін принцип. Бұл принципті қолдану кездейсоқ, қате немесе рұқсатсыз пайдалану нәтижесінде келтірілген зиянды шектейді.

Ымыра – ақпараттың үшінші тұлғаларға қол жетімді еместігіне деген сенімнің жоғалуы.

Кілттік тасымалдаушы – негізгі ақпарат (сертификаттар және т.б.) орналасқан электрондық тасымалдағыш (флэш-диск, қатты диск және т.б.).

Аутентификация – жүйеде іске асырылған ұсынылған рұқсат тіркелгі деректерінің сәйкестігін анықтау арқылы қол жеткізу субъектісінің немесе объектісінің түпнұсқалығын растау;

Мәліметтер қоры (МҚ) – концептуалды құрылымға сәйкес ұйымдастырылған мәліметтер жиынтығы, ол осы деректердің сипаттамаларын, сондай-ақ олардың объектілері арасындағы байланыстарды,

Ақпараттық жүйені ақпараттық қауіпсіздік деңгейлері бойынша градациялау – ақпараттық жүйені ақпараттық қауіпсіздікті қамтамасыз ету талаптарының деңгейіне сәйкес сыныптарға бөлу;

Ақпараттық ресурстар (IR) мәліметтер жиынтығы: мәтін; графика өнері; аудио; ақпараттық жүйелерде сақталған бейне және т.б.

Ақпараттық жүйе (АЖ) – аппараттық-бағдарламалық кешеннің көмегімен ақпаратты сақтауға, өңдеуге, іздеуге, таратуға, беруге және беруге арналған жүйе;

Ақпараттық қауіпсіздік (АЖ) – ақпараттың немесе оны өңдеу құралдарының құпиялылығын, тұтастығын, қолжетімділігін, сәтсіздікке жол бермейтіндігін, есептілігін, түпнұсқалығын және сенімділігін анықтауға, қол жеткізуге және қолдауға қатысты барлық аспектілер;

Электрондық ақпараттық ресурстар (EIR) – АЖ-де қамтылған, тиісті бағдарламалық қамтамасыз етумен біріктірілген және ақпаратты пайдаланушыларды қызықтыратын ақпараттың электрондық жүйеленген массивтері (ақпараттық деректер базасы);

Ақпараттық-коммуникациялық инфрақұрылым (ICI) – компьютерлік құралдардың, телекоммуникациялық жабдықтардың, деректерді беру арналары мен ақпараттық жүйелердің, коммутация және ақпарат ағынын басқару құралдарының жиынтығы;

Жергілікті желі (LAN) – шағын аумақта орналасқан абоненттерді біріктіретін желі;

Ақпаратқа рұқсатсыз қол жеткізу (UAI) – компьютерлік технологиялар немесе автоматтандырылған жүйелер қамтамасыз ететін стандартты құралдарды пайдалана отырып, қолжетімділікті басқару ережелерін бұзатын ақпаратқа қол жеткізу;

Нормативтік құқықтық актілер (НҚА) – құқықтық нормаларды белгілейтін, олардың қолданылуын өзгертетін, тоқтататын немесе тоқтата тұратын лауазымды тұлға(лар) қабылдаған, белгіленген нысандағы жазбаша ресми құжат, сондай-ақ жазбаша нысандағы электрондық цифрлық нысандағы құжат. электрондық цифрлық қолтаңба арқылы куәландырылған ресми құжат;

АЖ пайдаланушысы – өзіне қажетті электрондық IR алу үшін АЖ-ға жүгінетін және оларды пайдаланатын субъект;

Бағдарламалық қамтамасыз ету (БҚ) – ақпаратты өңдеу жүйесінің компьютерлік бағдарламаларының және осы бағдарламалардың жұмыс істеуі үшін қажетті бағдарламалық құжаттардың жиынтығы;

Қолданбалы бағдарламалық қамтамасыз ету (ASW) – қолданбалы мәселені шешуге арналған бағдарламалық құрал (немесе бағдарлама);

Серверлік бөлме – серверлік, белсенді және пассивті желілік жабдықты (телекоммуникация) және құрылымдық кабельдік жүйелердің жабдықтарын орналастыруға арналған бөлме;

Мәліметтер қорын басқару жүйесі (ДҚБЖ) – мәліметтер базасын басқаруды қамтамасыз ететін бағдарламалық және тілдік құралдар жиынтығы;

Жүйелік программалық қамтамасыз ету – есептеу техникасының жұмысын қамтамасыз ететін компьютерлік бағдарламалар жиынтығы;

Жүйелік әкімші (ЖБ) – сервердің дұрыс жұмыс істеуіне және сервердегі бағдарламалық құрал параметрлеріне жауапты тұлға;

Мамандандырылған бағдарламалық қамтамасыз ету – көмекші және сервистік міндеттерді шешу үшін қолданылатын компьютерлік бағдарламалар;

Компьютердің аппараттық құралдары (КТ) - дербес немесе басқа жүйелердің бөлігі ретінде жұмыс істеуге қабілетті кірісті немесе шығысты қамтитын ақпаратты өңдеу жүйелерінің бағдарламалық және техникалық элементтерінің жиынтығы;
Интернет – халықаралық ресурстарға қол жеткізуді қамтамасыз ететін желілер жүйесі.

4. АҚПАРАТТЫҚ ҚАУІПСІЗДІК ОБЪЕКТІЛЕРІ

Университеттің ақпараттық қауіпсіздігін қорғаудың негізгі объектілері:
1) рұқсат етілмеген әсерлерге және олардың қауіпсіздігін бұзуға сезімтал, құпияны құрайтын қолжетімділігі шектеулі IR, оның ішінде ұсыну нысаны мен түріне қарамастан ашық (жария) ақпаратты;
2) АЖ-де ақпаратты өңдеуге арналған процестер мен адам ресурстары – ақпараттық технологиялар, ақпаратты жинау, өңдеу, сақтау және беру жөніндегі ережелер мен рәсімдер, әзірлеуші персонал, жүйенің ішкі пайдаланушылары және оған қызмет көрсететін персонал;
3)ақпарат алмасу арналарын, IR және АЖ құрамдастары орналасқан объектілер мен үй-жайларды қоса алғанда, ақпаратты өңдеу және талдау, беру және көрсету жүйелерін қамтитын ақпараттық инфрақұрылым.

5. АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЖӘНЕ ЖҮЙЕНІ БАСҚАРУ ҮШІН ЖАУАПТЫ ТҰЛҒАНЫҢ ҰЙЫМДАСТЫҚ-ҚҰҚЫҚТЫҚ МӘРТЕБЕСІ

Ақпараттық қауіпсіздікке жауапты тұлға қажетті құқықтарға ие:
1) университеттің ақпараттық инфрақұрылымының мониторингі және бақылауы;
2) университеттің АЖ, SVT және LAN орнатылған университеттің барлық үй-жайларына қолжетімділік;
3) қорғалатын ақпаратқа тікелей қауіп төнген жағдайда ақпаратты автоматтандырылған өңдеуді тоқтатуға міндетті.
Ақпараттық қауіпсіздікке жауапты тұлғамен келісім бойынша СА мыналарға құқылы:
1) университеттің АЖ, SVT және LAN орнатылған университеттің барлық үй-жайларына қол жеткізу;
2) қорғалатын ақпаратқа тікелей қауіп төнген жағдайда ақпаратты автоматтандырылған өңдеуді тоқтатуға міндетті.

6. АҚПАРАТТЫҚ ҚАУІПСІЗДІК ТАЛАПТАРЫ

6.1. Жалпы құпиялылық талаптары

6.1.1.Құпиялылықтың негізгі талаптары кез келген құпия ақпараттың ағып кетуіне (жариялануына) жол бермеу және ақпараттың тек уәкілетті тұлғаларға берілуін қамтамасыз ету болып табылады.
6.1.2. Ішкі пайдаланушылардың университеттің АЖ-мен байланысы толық және мұқият жазылуы керек, бұл ақпарат 1 жылдан аспайтын мерзімге сақталады (тіркелу).
6.1.3.Университеттің АЖ-де өңделетін және сақталатын меншікті және басқа да қорғалатын ақпарат тек жетекшілік ететін проректор-кеңес мүшесінің ресми рұқсатымен ғана көшіріліп, үшінші тарапқа берілуі тиіс.
6.1.4.Университеттің АЖ-мен жұмыс істеу кезінде ішкі пайдаланушының монитор экранында көрсетілетін ақпаратты рұқсат етілмеген тұлғалардың бақылау мүмкіндігін болдырмау керек.

6.1.5.Университеттің АЖ-мен жұмыс істеу кезінде зиянды бағдарламалардан, вирустардан және желілік шабуылдардан қорғауды қамтамасыз ету үшін арнайы лицензияланған бағдарламалық жасақтаманы немесе аппараттық құралды пайдалану қажет. Университетте тіркелмеген бағдарламаларды заңсыз енгізуден және пайдаланудан қорғау үшін физикалық қорғауды қамтитын шаралардан басқа жүйелік журналдарды бақылау қажет және ішкі пайдаланушылардың жұмыс станцияларында негізгі бағдарламалық пакет орнатылуы керек. Негізгі бағдарламалық пакет SVT жұмысын қамтамасыз ету үшін қажет лицензияланған бағдарламалық құралды қамтиды.

6.1.6. Университеттің АЖ-мен жұмыс істеу кезінде ішкі пайдаланушылар мен қолдау қызметкерлерінің құпиялылық талаптарын сақтауы құпиялылық келісімімен қамтамасыз етілуі тиіс.

7. ЖҮЙЕДЕ ПАЙДАЛАНУШЫНЫҢ АУТЕНТИФИКАЦИЯСЫНА АРНАЛҒАН ТАЛАПТАР

Университеттің ақпараттық жүйесінде жұмыс істейтін барлық ішкі пайдаланушылар рұқсат етілген деректердің ағып кету және ұстап қалу мүмкіндігін болдырмау үшін қауіпсіз аутентификациядан өтуі керек.

АЖ-де ішкі пайдаланушыларды аутентификациялау үшін бірегей сәйкестендіру тіркелгілері (логин, пароль) жасалады.

Есептік жазба ақпаратының сақталуына және ашылмауына жауапкершілік ішкі АЖ пайдаланушыларының өздеріне жүктеледі.

Ішкі пайдаланушы тіркелгілері тиісті құжаттар немесе жазбалар болған жағдайда ғана жасалуы немесе жойылуы керек.

Құпия сөздермен жұмыс істеу кезінде ішкі пайдаланушылар мен АЖ қызмет көрсету қызметкерлерінің әрекеттеріне құпия сөзбен қорғауды ұйымдастыруға қойылатын талаптар жеке пароль кемінде 8 таңбадан тұруы және жалпы сөздіктегі сөздерді қамтымауы керек, бірақ кем дегенде келесі үш таңбалар жиынын қамтуы керек;

а)бас әріптер: A, B, C;

б)шағын әріптер: a, Ь, c;

в)сандар: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9;

г)символдар: '~!@#$%Л&*()_ + -= {}|[]\:

Ақпаратты байланыс желілері арқылы беру кезіндегі құпиялылық талаптары

• Университет ақпараты ұзақ қашықтыққа өзінің немесе жалға алынған талшықты-оптикалық арналар арқылы берілуі керек.

• Сервердің, телекоммуникациялық жабдықтың және құрылымдық кабельдік жүйенің техникалық реттеу талаптарына сәйкестігінің құжатталған дәлелі және ақпараттық қауіпсіздік талаптарына сәйкестік сертификаты болуы керек.

• Веб-сайттарда тіркелу кезінде және форумдарға немесе онлайн конференцияларға қатысу кезінде (бұл қызметкердің кәсіби қызметіне қатысты оқиғаларға қатысты жағдайларды қоспағанда) университеттің электрондық пошта мекенжайларын пайдалану ұсынылмайды.

• Құпия ақпаратпен жұмыс істейтін қызметкерлерге жалпыға қолжетімді Интернет пошта қызметтері мен Интернеттің жылдам байланыс жүйелері ұсынылмайды.

8. ЕРЕЖЕНІ ҚАЙТА ҚАРАУ

8.1. Ережені әзірлеуді, қайта қарауды және бағалауды ақпараттық қауіпсіздік тәуекелдерін жыл сайынғы талдау және бағалау негізінде ақпараттық қауіпсіздікке жауапты тұлға жүзеге асырады.
8.2.Ережені қайта қарау келесі мақсаттарда жүзеге асырылады:
• ақпараттық қауіпсіздікті бақылаудың мақсаттары мен шараларын жетілдіру;
• университеттің ақпараттық қауіпсіздігін және бизнес-процестерін басқару тәсілдерін жетілдіру;
• ресурстарды және/немесе жауапкершіліктерді бөлуді жақсарту.
8.3. Ақпараттық қауіпсіздікті бұзудың елеулі оқиғаларын, жаңа осалдықтардың пайда болуын немесе ұйымдық/технологиялық инфрақұрылымдағы өзгерістерді, университет бизнесінің негізгі сипаттамаларын өзгертуді анықтау арқылы тәуекелді бастапқы бағалау негізіне әсер ететін өзгерістерге сәйкес регламент қайта қаралуы тиіс. процестер.
8.4.Ақпараттың құпиялылығын, тұтастығын, қолжетімділігін, сондай-ақ қолданылатын ақпараттық қауіпсіздік шараларының барабарлығы мен тиімділігін қамтамасыз ету мақсатында ақпараттық қауіпсіздікті қамтамасыз ететін технологияларда елеулі өзгерістер болған жағдайда.
8.5.Қағидалардың ережелеріне өзгерістер енгізуге қатысты ішкі және сыртқы пайдаланушылардан қосымша ескертулер мен ұсыныстар болған жағдайда, бұл ұсыныстарды ақпараттық қауіпсіздікке жауапты тұлға талдайды және қажет болған жағдайда бекітуге жібереді.
8.6. Университет басшылығы Ережені тәуелсіз қарауды бастауға құқылы. Мұндай шолуды тексерілетін қауіпсіздік саласына тікелей қатысы жоқ тұлға жүргізеді, мысалы, ішкі аудит функциясын тәуелсіз басқарушы немесе осындай шолуларға маманданған үшінші тарап ұйымы орындайды. Тәуелсіз сараптаманың нәтижелері есеп түрінде ресімделеді және университет кеңесі төрағасының назарына ұсынылады.
8.7. Регламент ЖОО үшін ақпараттық қауіпсіздік тәуекелдерін талдау мен бағалаудан кейін қайта қаралуы тиіс, оның нәтижелері бойынша анықталған кемшіліктерді түзетуді ескере отырып, оны жаңарту қажет.
8.8. АЖ Ережесін қайта қарау Қазақстан Республикасының СТ ҚР ИСО/МЭК 17799-2006 «Ақпараттық технологиялар. Қорғанысты қамтамасыз ету әдістері. Ақпараттық қауіпсіздікті басқару тәжірибесі кодексі».

9. ЖАУАПКЕРШІЛІК

9.1. Ақпараттық қауіпсіздікке жауапты тұлға университет кеңесінің жетекшілік ететін проректор-мүшесімен бірлесіп:
1) ұйымдастырушылық талаптарға сәйкес ақпараттық қауіпсіздік мақсаттарын анықтау және университеттің бизнес-процестеріне интеграциялау;
2) осы АЖ Қағидасының барлық тармақтарының орындалуын бақылау;
3) университеттің ақпараттық қауіпсіздігін қолдау саласындағы бастамаларды нақты басқару және көзге көрінетін қолдау;
4) ақпараттық қауіпсіздікті қамтамасыз ету үшін ресурстармен қамтамасыз ету;
5) бекітілген құжаттардың жариялануын және университеттің компьютерлік ақпараттық жүйесін пайдаланушыларға жеткізілуін бақылау.
9.2. Университеттің жетекшілік ететін проректоры ақпараттық қауіпсіздікке жауапты тұлғаның ұсынуы бойынша:

1) университеттің ақпараттық қауіпсіздігін қамтамасыз ету мәселелері бойынша әзірленетін және пысықталатын нормативтік-құқықтық құжаттарды келіседі;
2) АЖ Регламентінің іске асырылу тиімділігін бақылауды жүзеге асырады;
3) ақпараттық қауіпсіздікті қамтамасыз ету бойынша нақты рөлдер мен жауапкершіліктерді бөлуді бекітеді;
4) ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі жоспарлар мен бағдарламаларды іске асыруға;
9.3. Университеттің құрылымдық бөлімшелерінің басшылары Ереженің талаптарын орындауға, сондай-ақ қарамағындағы қызметкерлерді, оның ішінде жаңадан қабылданған қызметкерлерді осы Ережемен таныстыруға жауапты.
9.4.Университетке моральдық және материалдық залал келтірген Ереже талаптарын бұзған жағдайда, тартылған қызметкерлер Қазақстан Республикасының заңнамасына сәйкес жауапкершілікке тартылады.
9.5.Осы Қағидалардың талаптарын бұзу еңбек міндеттерін орындамау немесе тиісінше орындамаудан тұратын тәртіптік теріс қылық ретінде сараланады. Ақпараттық қауіпсіздік ережелерінің талаптарын бұзған қызметкер Қазақстан Республикасының Еңбек кодексіне және ҚР СТ ИСО/МЭК 27002- Мемлекеттік стандартының 8.2.3 және 13.2.3 тармақтарының талаптарына сәйкес тәртіптік жауапкершілікке тартылады. 2009 «Ақпараттық технологиялар. Қолдау білдіреді. Ақпараттық қауіпсіздікті басқару тәжірибесі кодексі».
9.6.Парольді қорғау талаптарын сақтамағаны үшін Мекеменің ақпараттық жүйесін пайдаланушылар дербес жауапты болады.
9.7. AIS әкімшісі артықшылықты тіркелгілерді бұзуға және дұрыс пайдаланбауға жауапты.
9.8. Жауапкершілік нысаны мен мөлшері тиісті пайдаланушының әрекетімен немесе әрекетсіздігімен Мекеменің АЖ ресурстарына келтірілген залалдың түрі мен көлеміне байланысты анықталады.

10. ҚОРЫТЫНДЫ ЕРЕЖЕЛЕР

Ережеге өзгерістер мен толықтырулар академиялық мәселелер жөніндегі проректордың рұқсатымен ғана жүзеге асырылады және оның қолымен рәсімделеді. Түпнұсқаға және есептік жұмыс көшірмелеріне өзгерістер мен толықтырулар нормативтік құқықтық актілерді әзірлеу тәртібі туралы Ереженің талаптарына сәйкес енгізіледі.
Түпнұсқаға және есептік жұмыс даналарына өзгерістер мен толықтырулар енгізуге ҚББ жауапты болады
Ереже қажеттілігіне қарай қайта қаралады.
Ережеге **өзгерістер мен толықтырулар енгізу үшін негіз бола алады:**
-заңдық күші бар нормативті-құқықтық актілерге енгізілген жаңартулар мен өзгерістердің болуы;
- басқарма төрағасы ректорының бұйрықтары;
құрылымдық бөлімдер арасындағы міндеттердің қайта бөлінуі;
-мекеменің және құрылымдық бөлімдердің атаулары өзгерген жағдайда Ереже ауыстырылады. Ереже ауыстырылған жағдайда өз күшін жойған Ереженің университеттегі барлық даналары алынады және жаңасымен ауыстырылады.

Қазақстан Республикасының нормативтік-құқықтық актілері талаптарына сәйкес Ережені келісуді Сапа мониторингі кеңсесі жүзеге асырады.
Күші жойылған Ережені ауыстыру және жою үшін ҚББ жауапты болады.
Есепке алынған Ереженің жұмыс данасын бөлімшеде сақтау үшін ҚББ жүктеледі.

ӨЗГЕРТУЛЕР МЕН ҚОСЫМШАЛАРДЫ ТІРКЕУ ПАРАҒЫ

№ р/н	Бөлім №, бөлімше,тармақ, СМЖ тармақшасының құжаты	Өзгерту енгізілген күн	Негізі (№,бұйрық күні)	Өзгерту енгізілген күн	Өзгеріс енгізген тұлғаның қолы