«М.Х. Дулати атындағы Тараз
өңірлік университеті» КЕ АҚ
Директорлар кеңесінің шешімімен
(20.08.2021 жылғы № 6 хаттама)
БЕКІТІЛДІ

«М.Х. Дулати атындағы Тараз өңірлік университеті» коммерциялық емес акционерлік қоғамының ақпараттық қауіпсіздігі туралы ЕРЕЖЕ

Тараз 2021 жыл.

1. Жалпы ережелер

Ақпараттық қауіпсіздік туралы осы ереже (бұдан әрі - ереже) - «М.Х. Дулати атындағы Тараз өңірлік университеті» коммерциялық емес акционерлік қоғамында (бұдан әрі – Дулати Университеті) ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі жалпы ережелер мен саясатты белгілейді. Ережеде көрсетілген талаптар Дулати Университеттің барлық қызметкерлерінің орындауы үшін міндетті болып табылады, бұл ретте орындалатын жұмыстардың жеделдігі мен маңыздылығы осы Ережені бұзу үшін негіз болып табылмауы тиіс.

АҚ қамтамасыз етуге жалпы басшылықты Дулати Университетінің ректоры жүзеге асырады. Дулати Университетінің құрылымдық бөлімшелерінің басшылары өз құрылымдық бөлімшелерінде АҚ жөніндегі талаптарды ұйымдастырады және олардың орындалуын қамтамасыз етеді. Қызметкерлер құпия құжаттармен, негізгі ақпаратты жеткізушілермен жұмыс істеу тәртібін сақтауға, осы Ереженің және АҚ бойынша басқа да құжаттардың талаптарын сақтауға міндетті.

Ереже талаптарының орындалуын бақылауды Дулати университетінің бірінші проректоры және ЦИКЛ директоры жүзеге асырады.

Ереженің негізгі мақсаты - Ақпаратты қорғау және Дулати Университетінің Жарғысында көрсетілген қызметті жүзеге асыру кезінде Дулати Университетінің барлық ақпараттық-есептеу кешенінің тиімді жұмысын қамтамасыз ету.

Ереже Ақпараттық активтерді қаскүнемдердің құқыққа қарсы әрекеттерінен туындайтын қатерлерден қорғауға, аварияларда, қызметкерлердің абайсыз (қате) әрекеттерінен, техникалық іркілістерден, ақпаратты сақтау, беру және өңдеу процесінде дұрыс емес ұйымдастырушылық және технологиялық шешімдерден тәуекелдерді азайтуға және ықтимал зиянды азайтуға бағытталған.

2. Терминдер, анықтамалар, белгілер және қысқартулар.

Осы Ережеде келесі анықтамалар пайдаланылды:

Корпоративтік ақпараттық жүйе - Дулати Университетінің ақпараттық қажеттіліктерін қанағаттандыру мақсатында деректерді автоматтандырылған өңдеуді орындау үшін ұйымдық-құрылымдық, тақырыптық, технологиялық немесе басқа белгілері бойынша біріктірілген деректерді өңдеу мен берудің техникалық құралдары, бағдарламалық қамтамасыз ету, деректер қоры, персонал мен пайдаланушылар жиынтығы болып табылатын ұйымдық-техникалық жүйе.

Жеке есептік жазба (есептік жазба) - бұл компьютерлік жүйеде сақталатын, Дулати университетінің қызметкері немесе білім алушысы

туралы мәліметтер жиынтығы, оны аутентификациялауға және оның жеке деректері мен параметрлеріне қол жеткізуге мүмкіндік береді.

Пайдаланушы - есептік жазба алған Дулати Университетінің қызметкері немесе білім алушысы.

Ақпараттық қауіпсіздік саясаты - ақпараттық қауіпсіздікке көзқарастар жүйесі, ақпаратты қорғау тәсілдері мен құралдарын әзірлеуге және/немесе іс жүзінде қолдануға бағытталған іс-қимылдар жиынтығы.

Жеке саясат - АҚ-ның бір немесе бірнеше салаларына қолданылатын және қандай да бір белгі бойынша біріктірілген ақпараттық қауіпсіздік мәселелері мен салаларына көзқарастар жүйесі.

Электрондық қолтаңба - электрондық нысандағы басқа ақпаратқа қосылған немесе ақпаратқа қол қоятын белгілі бір тұлға үшін пайдаланылатын осындай ақпаратпен өзгеше түрде байланысты электрондық түрдегі ақпарат.

Қарапайым электрондық қолтаңба - кодтарды, логинді және парольдерді немесе өзге де құралдарды пайдалану арқылы электрондық хабарламаның немесе іс-қимылдың белгілі бір тұлға жүргізгенін растайтын электрондық қолтаңба.

АЖО	- автоматтандырылған жұмыс орны-дербес немесе басқа жүйелердің құрамында жұмыс істеуге қабілетті деректерді өңдеу жүйелерінің бағдарламалық және техникалық элементтерінің жиынтығы;
АЖ	- автоматтандырылған жүйе - персонал мен автоматтандыру құралдары кешенінің көмегімен белгіленген функцияларды орындаудың ақпараттық технологиясын іске асыратын жүйе;
АҚ	- Ақпараттық қауіпсіздік-ол үшінші тұлғалар тарапынан араласуға және залал келтіруге неғұрлым аз сезімтал болатын ақпараттық жүйенің жай-күйі;
АЖ	- ақпараттық жүйе;
АРҚЖ	- ақпаратқа рұқсатсыз қол жеткізу-есептеу техникасы құралдарымен немесе автоматтандырылған жүйелермен ұсынылатын штаттық құралдарды пайдалана отырып қол жеткізуді шектеу қағидаларын бұзатын ақпаратқа қол жеткізу;
Білім алушы	- студент, магистрант, докторант
Дербес деректер ДД	- дербес деректері-айқындалған немесе айқындалатын жеке тұлғаға (дербес деректер субъектісіне) тікелей немесе жанама қатысты кез келген ақпарат;
ВҚҚҚ	- вирусқа қарсы қорғау құралдары;
АҚҚ	-ақпаратты қорғау құралдары-ақпаратты қорғауға арналған техникалық, криптографиялық және басқа да құралдар;
АҚ жүйесі	- ақпараттық қауіпсіздік жүйесі-қорғалатын ақпараттың таралып кетуін немесе оған рұқсатсыз әсер етуді болдырмау

	жөніндегі ұйымдастырушылық және техникалық іс-шаралар кешені;

3. Ереженің міндеттері

Дулати Университетінің АҚ басқару жүйесін ұйымдастыру сипаттамасы.

АҚ саясатын анықтау:

1) вирусқа қарсы қорғауды іске асыру саясаты;
2) есептік жазбалар саясаты;
3) ақпараттық ресурсқа қол жеткізуді ұсыну саясаты;
4) пароль саясаты;
5) АЖО қорғау саясаты;
6) құпия іс жүргізу саясаты;

Дулати Университетінің АЖ сүйемелдеу тәртібін анықтау.

4. АҚ қамтамасыз етудің негізгі қағидаттары

Дулати Университетінде АҚ қамтамасыз етудің негізгі қағидаттары:

1) ақпараттық ресурстардың осалдығын анықтау мақсатында Дулати Университетінің ақпараттық кеңістігін тұрақты және жан-жақты зерделеу;

2) Дулати Университетінің АҚ-на әсер етуі ықтимал проблемаларды уақтылы анықтау;

3) қолданыстағы қорғау шараларын түзету немесе оларды іске асыруға арналған шығындарды ескере отырып, жаңа қорғау шараларын әзірлеу және енгізу (бұл ретте АҚ-ны қамтамасыз ету үшін қабылданатын шаралар университеттің негізгі мақсаттарына қол жеткізуді қиындатпауға, сондай-ақ ақпаратты өңдеудің технологиялық процестерінің еңбек сыйымдылығын едәуір арттыруға тиіс);

4) қабылданатын шаралардың тиімділігін бақылау;

5) университет қызметкерлері арасындағы рөлдер мен жауапкершіліктердің барабар бөлінуі.

5. Дулати Университетінің қорғалатын ақпараттық ресурстары

Университетте қорғауға жататын ақпараттық ресурстардың келесі санаттары бар:

1. Құпия ақпарат-ҚР Ақпаратқа қол жеткізу туралы Заңында, ҚР Ақпараттандыру туралы Заңында, сондай-ақ ҚР Азаматтық кодексінің 126-бабында айқындалған ақпарат (Жалпы бөлім).

2. Ашық ақпарат-таратуға және өңдеуге тыйым салу ресми түрде алынған жеке немесе заңды тұлғалардан алынған ақпарат; Университет қызметі нәтижесінде қалыптастырылған және құпия ақпаратқа жатпайтын ақпарат; көпшілікке қолжетімді және университет қызметінде пайдаланылатын ақпарат.

3. Қол жеткізу шектелген ақпарат-қол жетімділігі адамдардың белгілі бір санаттарына шектелген басқа санаттарға кірмейтін ақпарат.

Дербес деректерді қоса алғанда, құпия ақпараттың қауіпсіздігіне қатер ретінде оның ішіндегісін осы ақпаратпен жұмыс істеуге белгіленген тәртіппен жол берілмеген үшінші тұлғаларға ашу жолымен құпиялылықты бұзу қаралады.

Университетте ақпаратты қорғау мәліметтермен, сондай-ақ университет процестерінің жұмыс істеуін қамтамасыз ету үшін маңызды болып табылатын ақпараттық ресурстармен заңсыз немесе абайсыз әрекеттерді жою арқылы жүзеге асырылады.

Ол үшін университетте келесі іс-шаралар орындалады:

1) оқу құралы құжатпен және басқа ақпарат көздерімен жұмыс істеу тәртібін анықтайды;

2) адамдардың шеңбері мен ақпаратқа қол жеткізу тәртібі белгіленеді;

3) құпия деректері бар құжаттармен жұмыс істеуді бақылау бойынша шаралар әзірленеді;

4) А қосымшасына сәйкес қызметкерлермен құпия ақпаратты жарияламау туралы келісімдер жасалады.

Үшінші тарапқа тиесілі құпия ақпаратты қорғау университеттің осы тұлғалармен және ұйымдармен жасасқан шарттары негізінде жүзеге асырылады.

6. Университеттің ақпараттық қауіпсіздігін басқару жүйесін ұйымдастыру

Университеттің ақпараттық қауіпсіздігін басқару жүйесі университеттің АҚ құру, іске асыру, пайдалану, мониторинг, қолдау және арттыру үшін арналған.

Университеттің АҚ жүйесінің табысты жұмыс істеуі үшін мынадай процестер іске асырылуы тиіс:

- АҚ жүйесінің әрекет ету саласын анықтау және нақтылау және АҚ тәуекелдерін бағалау тәсілін таңдау (университеттің негізгі қызметімен байланысты тәуекелдер, сондай-ақ университет қызметінің құқықтық тәуекелдері);

- АҚ тәуекелдерін талдау және бағалау, аса сындарлы ақпараттық активтер үшін АҚ тәуекелдерін өңдеу нұсқалары;

- АҚ тәуекелдерін барынша азайту үшін қорғау шараларын таңдау және нақтылау;

- АҚ басқару жүйесін іске асыру.

Белгілі бір процестің ерекшелігіне байланысты оны жүзеге асыру келесі кезеңдерді сақтай отырып жүзеге асырылады:

1) Оқу жоспары жоспарлау кезеңінде активтерді түгендеуді, қауіптер мен осалдықтарды пысықтауды, қарсы шаралар мен ықтимал залалдың

тиімділігін бағалауды, қалдық тәуекелдердің жол берілетін деңгейін анықтауды қамтитын әдіснаманы және тәуекелдерді бағалауды айқындайды;

2) Іске асыру кезеңінде тәуекелдерді азайтуға арналған бақылау механизмдерін өңдеу және енгізу жүзеге асырылады. Университет тәуекелдер бойынша шешім қабылдауы мүмкін: елемеу, болдырмау, сыртқы жағына беру, азайту. Осыдан кейін қабылданған шешімге сәйкес белгілі бір шаралар қабылданады.

3) Тексеру кезеңінде тетіктердің жұмыс істеуі, тәуекел факторларының (активтердің, қауіптердің, осалдықтардың) өзгеруі қадағаланады;

4) Іс-қимыл кезеңінде мониторинг нәтижелері бойынша түзету іс-шаралары орындалады: тәуекел шамасын қайта бағалау, әдіснаманы түзету және тәуекелді азайту бойынша қабылданатын шаралар.

7. Ақпараттық тәуекелдерді бағалау

Университеттің ақпараттық тәуекелдерін бағалау келесі негізгі қағидаттар бойынша жүзеге асырылады:

1) университет жұмысы үшін маңызды ақпараттық ресурстарды анықтау және сандық бағалау;

2) ықтимал қауіптерді бағалау;

3) бар осалдықтарды бағалау, сондай-ақ АҚ қамтамасыз ету құралдарының тиімділігі

4) Бұл жағдайда ақпараттық тәуекелдер мыналарға байланысты:

5) ақпараттық ресурстар құндылығының көрсеткіштері;

6) ресурстар үшін қауіптерді іске асыру ықтималдығын анықтау;

7) АҚ-ны қамтамасыз етудің қолда бар немесе жоспарланатын құралдарының тиімділігін бағалау.

Тәуекелдерді бағалау нәтижесінде университеттің ақ қажетті деңгейін қамтамасыз ететін құралдарды таңдау мүмкін болады.

8. Ақпараттық ресурстарға қол жеткізуді ұсыну саясаты

Ақпараттық ресурсқа қол жеткізуді ұсыну саясаты қызметкерлерге университеттің қорғалатын ақпараттық ресурстарына қол жеткізуді ұсыну бойынша негізгі ережелерді анықтайды.

Қызметкерлер немесе мердігерлер және өзге де контрагенттер әзірлеген ақпараттық ресурстарға құқықтар, егер осы Шарт шартта бекітілген болса, университетке тиесілі болады.

Мұндай ақпараттық ресурстарды университет ректорының немесе ол уәкілеттік берген тұлғаның жазбаша келісімінсіз жалпы пайдалану желілерінде, оның ішінде Интернетте кез келген орналастыруға тыйым салынады.

Нақты ақпараттық ресурстармен жұмыс істеуге жіберілген университеттің әрбір қызметкеріне ол АЖ-да тіркелетін дербес бірегей есім (пайдаланушының есептік жазбасы) берілуге тиіс.

Қажет болған жағдайда кейбір қызметкерлерге бірнеше ерекше атаулар (есептік жазбалар) ұсынылуы мүмкін. Бірнеше қызметкердің бір пайдаланушы атын пайдалануына жол берілмейді.

Пайдаланушының жүйелер мен ресурстардың есептік жазбаларына қол жеткізу құқықтарын беру (немесе өзгерту) ресурсқа қол жеткізудің рұқсат етілген түрлерін (рөлдерін) көрсете отырып, құрылымдық бөлімше басшысының өтінімі негізінде жүзеге асырылады.

Пайдаланушының өкілеттіктерінің қолданылу мерзімі тоқтатылған кезде есептік жазба қызметкермен шарттық қатынастар аяқталған кезден бастап бұғатталады.

Парольдің үшінші тұлғаларға берілгені анықталған жағдайда немесе Пайдаланушының университетке тікелей немесе жанама залал келтіруі мүмкін іс-әрекеттері анықталған кезде есептік жазбаның қолданылуы тоқтатыла тұрады.

9. Есептік жазба саясаты

Есеп саясаты Университеттің ақпараттық жүйелерін пайдаланушыларға есеп жазбаларын берудің негізгі ережелерін анықтайды.

Есептік жазбалардың түрлері:

1) университеттің ақпараттық ресурстарын пайдаланушыларды сәйкестендіруге және аутентификациялауға арналған пайдаланушы нұсқаулықтары;

2) операциялық жүйелердің қажеттіліктері үшін қолданылатын жүйелік;

3) жеке процестердің немесе қосымшалардың жұмыс істеуін қамтамасыз етуге арналған қызметтік.

Есептік жазбаны жасағаннан кейін пайдаланушыға жеке кабинет, университет қызметкерінің лауазымдық міндеттері, университетте білім алушылардың құқықтары мен міндеттері шеңберіндегі АЖ функционалы қолжетімді.

10. Құпиясөз саясаты

Құпиясөз саясаты университеттің қорғалатын ақпараттық жүйелеріне қол жеткізу үшін қолданылатын құпиясөздерді пайдаланудың негізгі ережелерін анықтайды.

Парольде минималды ұзындық болуы керек - 6 (алты) таңба және мезгіл-мезгіл өзгеруі керек. Пайдаланушы тіркелгілерінің құпия сөздері келесі қауіпсіздік талаптарына сәйкес келуі керек:

1) парольдің жоғарғы және төменгі регистрлерде цифрлық символдар мен латын әріптерінің таңбалары болуы тиіс;

2) пароль өзгерген кезде жаңа мән алдыңғы мәннен кемінде екі позицияда ерекшеленуі керек;

3) пароль пайдаланушының атымен сәйкес келмеуі керек, сонымен қатар таңбалардың есептелген тіркесімдерін, жалпы қабылданған қысқартуларды (ЭЕМ, LAN, USER және т.б.) қамтуы керек, тегі, аты-жөні, телефон нөмірі және т. б. болмауы керек.

Жүйеге пароль енгізудің 5 (бес) әрекеті сәтсіз аяқталғаннан кейін пайдаланушының есептік жазбасы бұғатталуы мүмкін. Бұғаттауды тиісті АЖ әкімшісі алып тастай алады.

11. Вирусқа қарсы қорғауды іске асыру саясаты

Бұл Саясат университетте антивирустық қорғауды жүзеге асырудың негізгі ережелерін анықтайды.

АЖО компьютерлік вирустардың әсерінен ақпаратты қорғаудың негізгі тәсілі вирусқа қарсы қорғау құралдарын (бұдан әрі-ВҚҚҚ) қолдану болып табылады.

АЖО-да ВҚҚҚ ретінде университет орталықтандырып сатып алған бағдарламалық өнім пайдаланылады. АЖО-да ақпаратты қорғау жөніндегі іс-шараларды тікелей орындау үшін уәкілетті адам немесе цикл адамдар тобы жауап береді.

ВҚҚҚ үшін вирустық қолтаңбалар базаларын жаңарту жаңартулардың түсуіне қарай, бірақ айына кемінде бір рет жүзеге асырылады.

АЖО-ға зиянды бағдарламалардың енуін болдырмау мақсатында АЖО-ның техникалық құралдарына қосылған кезде барлық сыртқы машиналық ақпарат тасығыштар вирусқа қарсы кіріс бақылауына тартылуы тиіс.

12. Ақпараттық жүйелерді сүйемелдеу саясаты

АҚ АЖ жұмыс істеуінің (өмірлік циклінің) барлық сатыларында қамтамасыз етілуі тиіс:

- әзірлеу;
- пилоттық (тестілік) пайдалану;
- өнеркәсіптік пайдалану;
- мұрағаттық көшірме.

Техникалық тапсырмаларды әзірлеу, АЖ қорғау құралдары мен жүйелерін жобалау, құру, тестілеу, қабылдау цикл қызметкерлерінің қатысуымен жүргізіледі. АЖ енгізу тәртібі регламенттелуі және бақылануы тиіс.

АҚ мәселелері бөлігінде АЖ-ны іске қосу, пайдалану, пайдаланудан шығару цикл қызметкерлерінің қатысуымен жүзеге асырылуы тиіс.

Дайын АЖ-ны және олардың компоненттерін сатып алу кезінде әзірлеуші пайдалану үшін қажетті, оның ішінде қорғау шараларының сипаттамасы бар құжаттаманы ұсынуы тиіс. Сондай-ақ, әзірлеуші жеткізілетін компоненттерге (модульдерге) қажетті құжаттаманы ұсынады.

АЖ және олардың құрауыштарын сатып алу туралы шартқа (келісімшартқа) жеткізілетін бұйымдарды алып жүру жөніндегі ережелерді енгізу ұсынылады.

Шартқа (келісімшартқа) әзірлеушіге көрсетілген талаптарды енгізу мүмкін болмаған жағдайда, әзірлеушінің қатысуынсыз АЖ және олардың компоненттерін алып жүру мүмкіндігін қамтамасыз ететін бұйымға арналған жұмыс конструкторлық құжаттамасының толық жиынтығын сатып алу мүмкіндігін қарау қажет.

Егер аталған екі нұсқа да қолайсыз болса, мысалы, жоғары құны салдарынан, университет басшылығы АЖ және оның компоненттерін алып жүру мүмкін еместігі қаупінің жұмыстың үздіксіздігін қамтамасыз етуге әсерін талдауды қамтамасыз етуге тиіс.

Пайдалану сатысында мынадай қауіп-қатерлерден қорғау қамтамасыз етілуге тиіс:

1) ақпаратты қасақана рұқсатсыз ашу, өзгерту немесе жою;
2) ақпаратты абайсызда өзгерту немесе жою;
3) ақпараттың жеткізілмеуі немесе қате жеткізілуі;
4) қызмет көрсетуден бас тарту немесе қызмет көрсетудің нашарлауы.
5) Сүйемелдеу сатысында қатерлерден қорғау қамтамасыз етілуі тиіс:
6) АЖ-ға оның функционалдығының бұзылуына немесе құжатсыз мүмкіндіктердің пайда болуына әкелетін өзгерістер енгізу;
7) әзірлеушінің/өнім берушінің АЖ-ның дұрыс жұмыс істеуі мен жай-күйін қолдау үшін қажетті өзгерістерді енгізбеуі.

Пайдаланудан шығару сатысында санкцияланбаған пайдаланылуы университетке зиян келтіруі мүмкін ақпаратты және АҚ қамтамасыз ету құралдары пайдаланатын ақпаратты АЖ тұрақты жадынан немесе сыртқы тасығыштардан алып тастау қамтамасыз етілуге тиіс.

13. Ережені бұзудың алдын алу

Ережені бұзудың алдын алу деп Ақпаратты қорғау бойынша регламенттік жұмыстарды жүргізу, университетте болуы мүмкін АҚ бұзушылықтардың алдын алу және пайдаланушылар арасында Ақ бойынша түсіндіру жұмыстарын жүргізу түсініледі.

Университеттің АЖ-да ақпаратты қорғау бойынша регламенттік жұмыстарды жүргізу АҚҚ функцияларын бақылау тестілеуі рәсімдерін орындауды болжайды, бұл оның жұмысқа қабілеттілігін тестілеу кезеңіне дейінгі дәлдікпен көрсетеді.

АҚҚ функцияларын бақылау тестілеуі ішінара немесе толық болуы мүмкін және белгіленген кезеңділікпен жүргізілуі керек.

Университеттің АЖ-да ақпараттық қауіпсіздікті ықтимал бұзушылықтардың алдын алу міндеті келесі оқиғалардың басталуына қарай шешіледі:

1) университеттің АЖ-де осал тұстар пайда болған жағдайда университеттің АЖ құрамына жаңа бағдарламалық және техникалық құралдарды (жұмыс станцияларын, серверлік немесе коммутациялық жабдықтарды және т. б.) қосу;

2) операциялық жүйелер және/немесе университеттің АЖ-да пайдаланылатын техникалық құралдардың бағдарламалық қамтамасыз етуінің құрамында анықталған осал жерлер туралы мәліметтер пайда болған кезде университеттің АЖ АҚҚ-да осал орындар пайда болған жағдайда АЖ бағдарламалық және техникалық құралдарының конфигурациясын өзгертуге жол берілмейді.

Әкімші (ақ саласында мамандандырылған бөгде ұйымның көмегімен болуы мүмкін) университеттің АЖ-да пайдаланылатын операциялық жүйелердің және/немесе техникалық құралдардың бағдарламалық қамтамасыз етуінің құрамында анықталған осал жерлер туралы ақпаратты жинайды және талдайды.

Мұндай ақпараттың көзі ақпаратты қорғау саласында мамандандырылған әртүрлі компаниялардың, бірлестіктердің және басқа ұйымдардың ресми басылымдары мен жарияланымдары бола алады.

АЖ қорғалуын бақылау міндеттерін шешу үшін университеттің АЖ АҚҚ құрамында іске асырылған қорғау құралдары мен функцияларын тестілеу үшін аспаптық құралдар пайдаланылады. АҚ талаптарын сақтау бойынша жоспарлы немесе жоспардан тыс түсіндіру жұмысы немесе нұсқама осы Ережені қайта қарау кезінде жүргізіледі.

14. Ережені бұзу салдарын жою

Әкімші АЖ ақпаратының қауіпсіздігін бақылаудың (мониторингтің) аспаптық құралдарын қолдану нәтижесінде алынған деректерді пайдалана отырып, ақпараттық қауіпсіздіктің бұзылуын, қорғалатын ақпараттық ресурстарға ЖТӘ жүзеге асыру фактілерін уақтылы анықтауға және оқшаулау мен жою жөнінде шаралар қабылдауға тиіс.

АҚ-ны бұзу немесе АЖ-ның қорғалатын ақпараттық ресурстарына ЖТӘ-ні жүзеге асыру фактісі анықталған жағдайда, цикл әкімшісі мен басшысына олардың нұсқауларын одан әрі орындау ұсынылады. Инцидент жойылғаннан кейін АЖ жұмыс қабілеттілігін қалпына келтіру, сондай-ақ олардың себептері мен салдарларын жою бойынша шаралар қабылданады.

15. Ережені бұзғаны үшін жауапкершілік

Өз қызметтік міндеттері шеңберінде қауіпсіздік ережесі ережелерінің орындалуына университеттің АЖ әрбір пайдаланушысы жауапты болады.

Шараларды әзірлеу және ақпаратты қорғауды қамтамасыз етуді бақылау үшін АҚ әкімшісі жауапты болады.

Ережені іске асыру үшін жауапкершілік жүктеледі:

1) сыртқы қолжетімділік және қолжетімділікті басқару, вирусқа қарсы қорғау қағидаларын әзірлеу және өзектілендіруге қатысты бөлігінде – цикл қызметкерлеріне ұсыныстар енгізеді;

2) ереже ережелерін университет қызметкерлеріне-сорпа қызметкерлеріне жеткізуге қатысты;

3) университеттің құрылымдық бөлімшелерінің қызметкерлері лауазымдық міндеттерін жүзеге асыруға байланысты оған қолжетімді ақпараттың құпиялылығы үшін дербес жауапты болады.

А Қосымшасы

Келісім

Құпия сипаттағы мәліметтерді жария етпеу туралы
(оның ішінде дербес деректер)

«М.Х. Дулати атындағы Тараз өңірлік университеті» КЕ АҚ атынан _____, негізінде әрекет ететін_____, бұдан әрі Университет/жұмыс беруші деп аталатын, бір жағынан, және бұдан әрі қызметкер деп аталатын _____ _____, екінші жағынан, төмендегілер туралы құпия сипаттағы мәліметтерді қамтитын ақпаратты жарияламау туралы осы Келісімді (бұдан әрі – келісім) жасасты:

1. қызметкер еңбек міндеттерін орындау кезінде құпия сипаттағы мәліметтерді қамтитын ақпаратқа қол жеткізе алады және университетпен еңбек қатынастарының бүкіл мерзімі ішінде міндеттенеді:

1) Университеттің ақпараттық қауіпсіздік туралы ережесінде және өзге де нормативтік актілерінде белгіленген Ақпараттық қауіпсіздік талаптарын сақтауға;

2) университеттің құпия сипатындағы мәліметтері бар ақпаратты, сондай-ақ өзге де кәсіпорындар мен ұйымдардың қызметкерге еңбек міндеттерін атқару кезінде берілген коммерциялық құпиясын жария етпеуге;

3) университеттің құпия сипатындағы мәліметтері бар ақпаратты ауызша немесе жазбаша хабарламауға, мұндай ақпаратты бұған құқығы бар тұлғалардың тиісті рұқсатынсыз жария етпеуге және жария етпеуге;

4) бөтен тұлғалар университеттің құпия сипатындағы мәліметтері бар ақпаратты алуға әрекет жасаған жағдайда, бұл туралы өзінің тікелей басшысына хабарлауға;

5) университетпен еңбек қатынастары тоқтатылған жағдайда лауазымдық міндеттерін орындауға байланысты қызметкердің пайдалануында болған барлық материалдық ақпарат тасығыштарды (қағаз құжаттар, қағаз құжаттардың бекітілмеген жобалары және т. б.) университет өкілдеріне (тікелей басшысына) беру;

6) университеттің құпия сипатындағы мәліметтері бар ақпараттың материалдық жеткізгіштерінің, куәліктердің, сейфтердің кілттерінің, мөрлердің жоғалуы немесе жетіспеуі туралы және университеттің құпия сипатындағы ақпаратты жария етуге әкеп соғуы мүмкін басқа да фактілер туралы, сондай-ақ осы ақпараттың жария етілуі мүмкін себептері мен шарттары туралы тікелей басшысына және дербес деректердің өңделуін қамтамасыз етуге жауапты адамға дереу хабарлауға;

7) Университет берген және жұмыс орнында орнатылған ақпараттық өңдеу мен берудің техникалық құралдарын тек өзінің еңбек міндеттерін орындау үшін пайдалануға жол берілмейді.

2. Университет қызметкерге рұқсат етілген университеттің құпия сипатындағы мәліметтерді қамтитын ақпараттың құпиялылығын қорғау

жөніндегі талаптарды орындау үшін қажетті жағдайларды, оның ішінде құжаттарға арналған қойманы, АЖО-ға, ақпараттық жүйелерге және т.б. қол жеткізуге арналған, қызметкер орындайтын міндеттермен айқындалатын құралдарды ұсынады.

3. қызметкер университетке университет бөлген ақпаратты өңдеу мен берудің техникалық құралдарын пайдалануға бақылау жасауға рұқсат береді.

4. қызметкерге еңбек қатынастарының қолданылу кезеңінде оған белгілі болған университеттің құпия сипатындағы мәліметтерді қамтитын ақпаратты жария ету Қазақстан Республикасының қолданыстағы заңнамасында көзделген тәртіптік, материалдық, әкімшілік, азаматтық-құқықтық, қылмыстық жауапкершілікке әкеп соқтыруы мүмкін екендігі белгілі.

5. қызметкер еңбек шартының бүкіл мерзімі ішінде Еңбек міндеттерін орындауға байланысты қол жеткізілген университеттің құпия сипатындағы мәліметтерді қамтитын ақпаратты жария етпеуге міндеттенеді.

Тараптардың қолдары
Жұмыс беруші:
_____ Аты-жөні _____
«_____»_____20___ ж.
М.О.

Қызметкер:
_____ Аты-жөні _____
«_____»_____20____ ж.

Мен осы Келісімнің екінші бірдей данасын қолыма алу фактісін растаймын

Қызметкердің қолы:
_____ Аты-жөні _____
«_____»_____20___ ж.