Қожа Ахмет Ясауи атындағы Халықаралық қазақ-түрік университеті

«БЕКІТЕМІН»
Қожа Ахмет Ясауи атындағы Халықаралық
қазақ-түрік университетінің президенті,
профессор _____ Б.Абдрасилов
«__» _____ 2020 ж.

САПА МЕНЕДЖМЕНТІНІҢ ЖҮЙЕСІ

УНИВЕРСИТЕТ САЯСАТЫ

ҚС-ХҚТУ-01-2020

АХМЕТ ЯСАУИ УНИВЕРСИТЕТІНІҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІК САЯСАТЫ

Түркістан 2020

КІРІСПЕ

1. IT Департаментімен ӘЗІРЛЕНДІ ЖӘНЕ ЕНГІЗІЛДІ

2. Әзірлегендер – IT Департаментінің директоры Т.Карипов
   – IT Департаментінің директор орынбасары А.Кожихов

3. . Қожа Ахмет Ясауи атындағы Халықаралық қазақ-түрік университеті Сенат қаулысымен 28 қаңтар 2020 жылғы № 6 хаттамасында қаралды және бекітілді.

4. ЕНГІЗІЛДІ – 2020ж.

5. Тексеру мерзімі – 2023 ж.

МАЗМҰНЫ

1 ҚОЛДАНЫЛУ САЛАСЫ

1.1. Университеттің барлық оқытушыларына және қызметкерлеріне қолданылады.

2 МАҚСАТЫ

2.1. Қожа Ахмет Ясауи атындағы Халықаралық қазақ-түрік университетінде ақпараттық қауіпсіздікті қамтамасыз ету.

3 НОРМАТИВТІ СІЛТЕМЕЛЕР (СІЛТЕМЕЛІК ҚҰЖАТТАР)

3.1. Ақпараттық қауіпсіздікке жауап беретін мамандар Қазақстан Республикасының Дербес деректер және оларды қорғау туралы 2013 жылғы 21 мамырдағы № 94-V Заңының (Дербес деректер және оларды қорғау туралы заң) талаптарына, дербес деректердің ақпараттық жүйелерінде өңдеу кезінде дербес деректерді қорғауға қойылатын талаптарға («Дербес деректер және оларды қорғау туралы» Заңның 2-тарауы) сәйкес ақпараттық жүйе ақпаратының пайдаланылуын бақылауды қамтамасыз етуі тиіс.), Ақпараттандыру туралы «Қазақстан Республикасының 2015 жылғы 24 қарашадағы № 418-V Заңы».

3.2. «Ақпараттандыру туралы» 2015 жылғы 24 қарашадағы № 418-V Қазақстан Республикасының Заңы;

3.3. Қазақстан Республикасының 2003 жылғы 7 қаңтардағы № 370-II Заңы 25.11.2019 ж. «электрондық құжат және электрондық цифрлық қолтаңба туралы»);

3.4. «Қазақстан Республикасының ақпараттық қауіпсіздігінің 2016 жылға дейінгі тұжырымдамасы туралы» Қазақстан Республикасы Президентінің 2011 жылғы 14 қарашадағы № 174 Жарлығы;

3.5. «Ақпараттық қауіпсіздікті қамтамасыз етудің жедел орталықтары мен Ақпараттық қауіпсіздікті ұлттық үйлестіру орталығы арасындағы ақпараттық қауіпсіздікті қамтамасыз ету үшін қажетті ақпарат алмасу қағидалары» Қазақстан Республикасының Қорғаныс және аэроғарыш өнеркәсібі министрінің 2018 жылғы 19 наурыздағы № 48/НҚ бұйрығы. Қазақстан Республикасының Әділет министрлігінде 2018 жылғы 11 мамырда №16886;

3.6. Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы №832 қаулысымен бекітілген Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптары;

3.7. ҚР СТ ISO / IEC 27002-2015 ақпараттық технология Ақпараттық қауіпсіздік менеджменті жүйесінің қауіпсіздігін қамтамасыз ету әдістері мен құралдары.

4 ЖАУПКЕРШІЛІК

4.1. IT Департаментінің ақпараттық қауіпсіздік бөлімі осы саясаттың барлық тармақтарының орындалуын қамтамасыз етеді.

4.2. IT Департаментінің ақпараттық қауіпсіздік бөлімі университеттің ақпараттық жүйесінің ақпараттық қауіпсіздігі саласындағы бастамаларды басқаруды және қолдауды қамтамасыз етуі тиіс.

4.3. Ақпараттық қауіпсіздікке жауап беретін мамандар пайдаланылатын ақпараттық жүйелерде бақылау шараларын үйлестіруді қамтамасыз етуі тиіс.

4.4. Ақпараттық қауіпсіздік бөлімі ақпараттық қауіпсіздік бойынша ерекше рөлдер мен міндеттерді білуі тиіс.

4.5. Қызмет көрсетуші персонал, ақпараттық қауіпсіздік саясаты тармақтарының талаптары бұзылған жағдайда Қазақстан Республикасының қолданыстағы заңнамасына сәйкес әкімшілік немесе өзге де жауапкершілікке тартылады.

4.6. Ақпараттық қауіпсіздікке жауап беретін мамандар ақпараттық қауіпсіздік бойынша бекітілген құжаттарды университеттің қызмет көрсетуші персоналы мен ақпараттық жүйелерін пайдаланушыларға жеткізуді және бақылауды қамтамасыз етуі тиіс.

4.7. Ақпараттық қауіпсіздікке жауап беретін мамандар ақпараттық қауіпсіздік туралы хабардарлықты қолдау жөніндегі жоспарлар мен бағдарламаларға бастамашылық жасауы тиіс.

4.8. Ақпараттық жүйелердің әкімшілеріне жауапкершілік "функциялар мен өкілеттіктерді бекіту жөніндегі лауазымдық нұсқаулықтарға" сәйкес олардың жауапкершілік аймақтарына сәйкес жүктеледі.

4.9. Ақпараттық жүйелердің әкімшілері:

• ақпараттық жүйе ресурстарына қол жеткізу үшін сәйкестендіру және аутентификациялау рәсімдерінің міндеттілігін қамтамасыз ету;

• авторланбаған пайдаланушыларға ақпараттық жүйелерге қол жеткізу құқығын алуға жол бермеу және белгіленген тіркеу нысандарын толтырғаннан кейін ғана пайдаланушыларға кіру аттары мен бастапқы парольдерді ұсыну;

• жабдықтарды, соның ішінде арнайы желіаралық бағдарламалық құралдарды қорғауды қамтамасыз ету;

• қауіп-қатер бар оқиғаларға жедел және тиімді әрекет ету, қауіп-қатерді көрсету және тәртіп бұзушыларды анықтау бойынша шаралар қабылдау, ақпараттық қауіпсіздікке жауап беретін мамандарды қорғауды бұзу әрекеттері туралы тіркеу және хабардар ету.

4.10. Ақпараттық қауіпсіздік саясатының талаптары сапалы орындалуын және бақылауға IT Департаментінің директоры жауапты.

5 АНЫҚТАМАЛАР, ТЕРМИНДЕР ЖӘНЕ ҚЫСҚАРТУЛАР

5.1. Осы ақпараттық қауіпсіздік саясаты (бұдан әрі - саясат) Қожа Ахмет Ясауи атындағы Халықаралық қазақ-түрік университетінің ішкі нормативтік құжаты болып табылады.

5.2. Қожа Ахмет Ясауи атындағы Халықаралық қазақ-түрік университетінде пайдаланылатын ақпараттық жүйелер үшін ақпараттық қауіпсіздікті қамтамасыз етуге қойылатын талаптарды белгілейді, ақпаратты қорғау жөніндегі негізгі қағидаларды, бағыттарды және талаптарды айқындайды, ақпараттық қауіпсіздік режимін қамтамасыз ету үшін негіз болып табылады, тиісті ережелерді, нұсқаулықтарды әзірлеу кезінде басшылық етеді.

5.3. Ақпараттық қауіпсіздікті қамтамасыз ету немесе ақпаратты қорғау деп оның құпиялылығын, тұтастығын және қолжетімділігін сақтау түсіндіріледі. Ақпараттың құпиялылығы деректерге тек авторизацияланған тұлғаларға рұқсат берілген жағдайда қамтамасыз етіледі.

Осы Саясатта келесі анықтамалар, белгілер және қысқартулар келтірілген:

Аутентификация	Жүйеде іске асырылған қол жеткізудің ұсынылған деректемелерінің сәйкестігін анықтау арқылы қол жеткізу субъектісінің немесе объектісінің түпнұсқалығын растау.
Авторизация	Белгілі бір іс-әрекеттерді орындауға құқық беру; сондай-ақ

	осы іс-әрекеттерді орындауға әрекет жасаған кезде құқықтар деректерін тексеру (растау) процесі.
Мемлекеттік құпиялар	Мемлекет қорғайтын мемлекеттік және қызметтік құпияларды құрайтын мәліметтер, олардың таралуын мемлекет халықаралық құқықтың жалпы қабылданған нормаларына қайшы келмейтін тиімді медициналық, әскери, экономикалық, ғылыми-техникалық, сыртқы экономикалық, сыртқы саяси, барлау, қарсы барлау және өзге де қызметті жүзеге асыру мақсатында шектейді.
Қол жетімділік	Қол жеткізуге құқығы бар субъектілер оларды кедергісіз іске асыра алатын ақпараттың (автоматтандырылған ақпараттық жүйе ресурстарының) жай-күйі.
Ақпараттық қауіпсіздік (бұдан әрі - АҚ)	Ақпараттық ресурстар мен жүйелердің қорғалу жағдайы, ақпараттың құпиялылығын, тұтастығын және қолжетімділігін қамтамасыз ету.
АЖ	Ақпараттық жүйе.
АЖ инфрақұрылымы	Байланыс арналары, жабдықтар, бағдарламалық қамтамасыз ету, қызметкерлер мен пайдаланушылар, құжаттама, ақпараттық жүйелердің ақпараты.
Ақпараттың құпиялылығы	Қол жеткізу деңгейлері бойынша тек авторландырылған тұлғаларға ғана ақпарат беруді қамтамасыз ету.
ОЖ	Операциялық жүйе.
БҚ	Бағдарламалық қамтамасыз ету.
АЖ-мен жұмыс істейтін тұлғалар	АЖ пайдаланушылары.
ҚРҰҚ	Қазақстан Республикасы Үкіметінің Қаулысы.
ЕТҚ	Есептеу техникасы құралдары.
ҮҚК	Үздіксіз қоректендіру көзі .
Ақпараттың тұтастығы	Ақпараттың (автоматтандырылған ақпараттық жүйе ресурстарының) жай-күйі, бұл ретте оны (оларды) өзгертуді тек оған құқығы бар қасақана субъектілер ғана жүзеге асырады.
ID	идентификатор

6 РЕСУРСТАР

6.1. барлық талаптарға жауап беретін серверлік бөлме;

6.2. қажетті қуатты үздіксіз қоректендіру көзі (ҮҚК);

6.3. ішкі нормативтік құжаттар (10.15-тармақты қараңыз).

7 ҚҰЖАТТАУ

Есеп түрінде нәтижесімен ақпараттық жүйелердің ақпараттық қауіпсіздігін жыл сайын талдау.

8 ЖАЛПЫ ЕРЕЖЕЛЕР

8.1. АҚ-ны қамтамасыз етудің мақсаты АҚ қатерлерін іске асырудан экономикалық, қаржылық, әлеуметтік, институционалдық және экологиялық залалды азайту, сондай-ақ АЖ-да ақпараттың құпиялылығының, тұтастығы мен қол жетімділігінің жалпы деңгейін арттыру болып табылады.

8.2. АҚ саясаты Қожа Ахмет Ясауи атындағы Халықаралық қазақ-түрік университетінің барлық инфрақұрылымының жұмыс істеуіне қолданылады.

8.3. АҚ саясаты инфрақұрылыммен жұмыс істейтін барлық тұлғалардың, оның ішінде АЖ сүйемелдеу не дамыту жөніндегі жұмыстарды орындайтын үшінші тұлғалар үшін орындауға міндетті.

8.4. АҚ саясатының талаптарын орындауды ақпараттық жүйелердің инфрақұрылымымен жұмыс істейтін барлық адамдар қамтамасыз етеді.

8.5. АҚ-ны қамтамасыз ету жөніндегі іс-әрекеттерді АҚ-ға жауапты басшылық пен мамандар үйлестіруі тиіс.

8.6. АҚ үйлестіру мынадай қызметті жүзеге асыруға тиіс:

• АҚ-ны қамтамасыз ету бойынша орындалатын іс-әрекеттердің АҚ саясатына сәйкестігін қамтамасыз ету;

• АҚ-ны қамтамасыз ету бойынша орындалатын іс-қимылдар АҚ жөніндегі саясатқа сәйкес келмеген жағдайда іс-әрекеттерді анықтау;

• АҚ қамтамасыз ету әдіснамасы мен процестерін бекіту, мысалы, тәуекелдерді бағалау, ақпаратты жіктеу;

• Қауіп-қатерлердің елеулі өзгерістерін сәйкестендіру және ақпаратты өңдеу құралдары мен қауіп-қатерлерге ұшырату;

• АҚ бақылау шараларын іске асырудың барабарлығын бағалау және үйлестіру;

• АҚ бойынша оқытуға, дайындауға және ол туралы хабардарлыққа тиімді ықпал ету;

• АҚ инциденттерінің мониторингі мен қайта қараудан алынған ақпаратты бағалау және АҚ сәйкестендірілген инциденттеріне жауап ретінде ұсыныстар енгізу.

9 АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ БАСҚАРУ СИПАТТАМАСЫ

9.1. ҚҰПИЯЛЫЛЫҚ

9.1.1. Құпиялылықтың басты талабы, тек авторизацияланған тұлғаларға ақпарат беруді қамтамасыз ету болып табылады.

9.1.2. АЖ-де өңделетін және сақталатын ақпарат тек университет басшылығының ресми рұқсатымен ғана көшірілуге және үшінші тұлғаға беруге жатады.

9.1.3. АЖ-мен жұмыс істеу кезінде көрінетін ақпаратты бөгде адамдардың бақылау мүмкіндігі болмауы тиіс.

9.1.4. АЖ-да мемлекеттік құпияларды, коммерциялық құпияны және қолжетімділігі шектеулі өзге де ақпаратты қамтитын құжаттар орналастырылмауға тиіс.

9.1.5. Қызметтік және өзге де қорғалатын ақпаратты жазу және көшіру, оның ішінде басқа адамдарға беру үшін белгіленген тәртіппен тіркелген ақпарат көздеріне жүргізіледі.

9.1.6. АЖ-мен жұмыс істеу кезінде зиянды бағдарламалардан, вирустардан және желілік шабуылдардан қорғауды қамтамасыз ететін арнайы лицензиялық бағдарламалық немесе аппараттық құралдар пайдаланылуы тиіс.

9.1.7. Ақпарат АЖ үшін оның құндылығы, құқықтық талаптары, құпиялылық және сыни тұрғысынан жіктелуі тиіс.

10 ТАЛАПТАР

10.1. АҚ МӘСЕЛЕЛЕРІНДЕ ОҚУҒА ЖӘНЕ ХАБАРДАРЛЫҚҚА ҚОЙЫЛАТЫН ТАЛАПТАР

10.1.1. АЖ қызмет көрсетуші персоналы, АЖ пайдаланушылары мен әкімшілері АҚ саясатымен танысуы тиіс.

10.1.2. АЖ қызмет көрсетуші персонал АЖ пайдаланушыларына жұмыс құжаттамасын (АЖ парольдік қорғау туралы Нұсқаулық) ұсынуы тиіс.

10.1.3. АЖ қызмет көрсетуші персоналы пайдаланушылардың сұрауы бойынша АҚ бойынша бастапқы нұсқама жүргізуі тиіс.

10.1.4. АЖ-ның жұмыс істеуін қамтамасыз ететін қызмет көрсетуші персонал АҚ-ны сақтау бойынша үнемі нұсқамадан өтуі тиіс.

10.1.5. АЖ қызмет көрсетуші персоналы құпиялылық туралы пайдаланушылық келісімді қабылдауы тиіс.

10.1.6. АҚ-ны қамтамасыз ету мақсатында үшінші тараппен келісімде АЖ-ны басқару жөніндегі іс-шараларды келісу және айқындау қажет.

10.1.7. АҚ үшін жауапты бөлімшені, АЖ қызмет көрсетуші персоналын және барлық мүдделі тараптарды АЖ-ға қатысты АҚ оқыс оқиғалар мен әлсіздігі туралы кепілді хабардар етуді қамтамасыз ету мақсатында оқыс оқиға және қауіп-қатердің пайда болуы туралы хабарлама бойынша формальды рәсімдер іске асырылуы тиіс. Хабарламаларды тарату үшін түзетуші шараларды уақтылы қабылдауға кепілдік беретін әдіс таңдалуы тиіс.

10.1.8. АЖ қызмет көрсетуші персоналы хабарлама рәсімдерін білуі, сондай-ақ ресурстардың қауіпсіздігіне әсер етуі мүмкін оқиғалардың әртүрлі түрлері немесе әлсіз орындар туралы және олардың басталуы немесе осындай алғышарттар туралы хабарламаны жіберу қажет болатын мәліметтер болуы тиіс.

10.1.9. АЖ қызмет көрсетуші персонал және әкімшілері АҚ саласындағы кез келген оқиғалар туралы АҚ үшін жауапты тұлғаларға мүмкіндігінше тезірек хабарлауға міндетті.

10.2. АЖ АУТЕНТИФИКАЦИЯСЫ БОЙЫНША ТАЛАПТАР

АЖ әкімшілері мен пайдаланушылары оларды сәйкестендіретін және пароль таңдау және авторотациялық деректерді ұстап қалу мүмкіндігін болдырмайтын қауіпсіз аутентификациядан өтуі тиіс.

10.3. ПАЙДАЛАНУШЫ ТІРКЕЛГІЛЕРГЕ ЖӘНЕ ПАРОЛЬДЕРГЕ ҚОЙЫЛАТЫН ТАЛАПТАР

Пайдаланушылық есептік жазбаларға және парольдерге қойылатын талаптар «АЖ парольдік қорғау туралы Нұсқаулық» ішкі нормативтік құжатта келтірілген.

10.4. СЕРВЕР БӨЛМЕСІНЕ ҚОЙЫЛАТЫН ТАЛАПТАР

АЖ үшін пайдаланылатын серверлер мен белсенді желілік жабдық орналастырылатын серверлік бөлме былайша жабдықталуы тиіс:

10.4.1. кіруді басқаруды бақылау жүйесі - рұқсат етілген тұлғаларға рұқсат етілген кіруді/шығуды ұсынуға және электрлік, электрондық немесе механикалық құралдардың көмегімен бақыланатын аймақтарда авторланбаған тұлғалардың кіруіне/шығуына тыйым салуға арналған жүйе. Кіру/шығу бақылауы барлық оқиғалар мен әрекеттер есебін және тіркеуін қамтуы мүмкін;

10.4.2. бейнебақылау жүйесі - күзет бейнебақылау жүйесі серверлік бөлмелерді ағымдағы жағдайды көзбен бақылауға және бекітуге арналған. Камераларды үй-жайға кіру және шығу жолдарын, технологиялық жабдықтың жанындағы кеңістікті (ИБП, кондиционерлер, серверлік шкафтар мен телекоммуникациялық тіреулер) бақылайтындай етіп орналастыру қажет. Бейнекамералардың рұқсаты технологиялық жабдыққа қызмет көрсететін қызметкерлердің тұлғасын сенімді ажырату үшін жеткілікті болуы тиіс;

10.4.3. ауаны кондиционерлеу жүйесінің нақты тоңазытқыш қуаты серверлік үй-жайда орналасқан барлық жабдықтар мен жүйелердің жиынтық жылу бөлуінен аспауы тиіс;

10.4.4. микроклиматтың мониторинг жүйесі - параметрлерді бақылау жүйесі серверлік шкафтарда және телекоммуникациялық тіреулерде климаттық және басқа да параметрлерді бақылауға арналған. Әрбір шкафта келесі параметрлерді бақылау үшін датчиктер орнатылады:

- ауа температурасы;
- ауаның шаңдылығы;
- ауа ағынының жылдамдығы;
- ауаның түтіндеуі;
- шкаф есіктерін ашу/жабу;

10.4.5. өрт дабылы жүйесі - серверлік үй-жайдың өрт дабылы жүйесі ғимараттың (кеңсенің) өрт дабылынан бөлек орындалуы тиіс. Серверлік бөлмеде хабарлағыштардың екі түрі орнатылуы тиіс: температуралық және түтін. Хабарлағыштар үй-жайлардың жалпы кеңістігін де, фальшполмен және фальшпотолкпен түзілген қуысты да бақылауы тиіс. Өрт сигнализациясының кіші жүйесінің хабарлау сигналдары тәулік бойы күзет үй-жайына жеке пультке шығарылады. Өрт дабылы жүйесі серверлік бейнебақылау ішкі жүйесімен біріктірілуі мүмкін;

10.4.6. газбен өрт сөндіру жүйесі - серверлік автоматты газбен өрт сөндіру қондырғысымен жабдықталады, ол ғимараттың өрт сөндіру жүйесінен тәуелсіз. Газды өрт сөндіру кіші жүйесінің газды өрт сөндіру модулі серверлік үй-жайда (немесе оған жақын жерде), ол үшін арнайы жабдықталған шкафта орналастырылады. Кіші жүйені іске қосу түтіннің пайда болуына әсер ететін өртті ерте анықтау датчиктерінен, сондай-ақ үй-жайдан шығатын жерде орналасқан қол хабарлағыштарынан жүргізіледі. Жүйеде персоналдың серверлік бөлменің ішінде және сыртында орналасқан іске қосылғандығы туралы хабарлау таблосы болуы тиіс. Жүйе желдету жүйесінің қорғаныш клапандарын жабуға және жабдықтың қоректенуін ажыратуға командалардың берілуін қамтамасыз етуі тиіс. Тасымалданатын ұнтақты өрт сөндіргіштерді пайдалануға жол беріледі;

10.4.7. газ және түтін шығару жүйесі - газды өрт сөндірудің кіші жүйесі іске қосылғаннан кейін түтін мен газды серверлік үй - жайдан бұруды қамтамасыз етеді. Жүйе ғимараттың төбесіне ауа тартқышты шығара отырып, ғимараттың желдету жүйесінен бөлек орындалады. Жүйе газ-ауа қоспасын серверлік көлемнен үш есе асатын көлемде бұруды қамтамасыз етуі тиіс. Тасымалданатын түтін сорғыштарды пайдалануға жол беріледі;

10.4.8. жабдықтар мен кабельдік шаруашылықты ұйымдастыру жүйесі:

Телекоммуникациялық шкафтар мен тіреулер:

• Серверлік барлық жабдықтар жабық шкафтарда немесе ашық тіреулерде орналастырылады. Тіректердің (шкафтардың) саны қолда бар жабдықтарға және оның үлгі өлшемдеріне, монтаждау тәсілдеріне сүйене отырып анықталады;

• Температуралық режимді жақсарту үшін шкафтарды (тіреулерді) орналастыруды "ыстық" және "суық" дәліздердің пайда болуымен қатар ұйымдастырады. Шкафтар арасындағы аралықтарға жол берілмейді;

• Жабдықтарды шкафтар (тіреулер) бойынша бөлу үйлесімділік (мүмкін болатын өзара әсер ету), тұтынылатын қуаттың оңтайлы таралуын (яғни жылу бөлу), коммуникациялардың оңтайлылығын, жабдықтың габариттері мен массасын ескере отырып жүзеге асырылады;

• Жабық шкафтар, тіреулерге қарағанда, жабдыққа қол жеткізуге қосымша шектеулерді ұйымдастыруға мүмкіндік береді. Мұндай шкафтардың ішіне кіру рұқсатты бақылаудың кіші жүйесін пайдалана отырып жүзеге асырылуы мүмкін;

• Жабық шкафтар қажетті температуралық режимді қамтамасыз ету бойынша қосымша шараларды қажет етеді. Ол үшін қосымша желдеткіштер, қосылатын салқындату жүйелері, ыстық ауаны бұру модульдері қолданылады.

Коммуникацияларды ұйымдастыру:

• Сервердің ішіндегі барлық коммуникациялық кабельдер фальшпол немесе фальшпотолка қуыстарына салынған науаларға ұйымдастырылуы тиіс. Электр кабельдері мен сигналдардың науалары 50 см дейінгі қашықтыққа таратылуы тиіс;

• Телекоммуникациялық шкафтар мен тіреулерге енгізу арналары шеткі ажыратқыштармен бірге кабельдердің талап етілетін санын еркін созуды қамтамасыз етуі тиіс;

• Кабельдік арналар мен салмалы арналарды толтыру коэффициенті 50-60% аспауы тиіс;

• Тіректер мен шкафтардың ішінде кәбілдің артық ұзындығының ілуін болдырмайтын кәбілдік ұйымдастырушылар қолданылуы қажет;

• Коммуникацияларды оңайлату және жабдық ажыратқыштарының сынуын болдырмау үшін патч-панельдерді қолдану қажет;

• Барлық кабельдер, кроссалық коммуникациялар және патч-панельдер әр кабельді (разъем, порт) бірдей сәйкестендіруге мүмкіндік беретін таңбалануы тиіс.

10.4.9. үздіксіз электрмен жабдықтау жүйесі.

Электрмен жабдықтау жүйесі инфокоммуникациялық жүйелер мен ғимараттың инженерлік жүйелерінің қауіпсіз және сенімді жұмыс істеуін қамтамасыз ететін технологиялық жүйе болып табылады. Өз кезегінде, электрмен жабдықтау жүйесі қауіпсіздік құралдарымен қамтамасыз етілуі тиіс, сонымен қатар электрмен жабдықтау жүйесінің өзі жоғары қауіптілік көзі болып табылады. Электрмен жабдықтау жүйесін пайдаланудың маңызды міндеті тұтынушыларды электрмен жабдықтаумен қатар оның қауіпсіз жұмыс істеуі болып табылады.

10.5. ҚҰПИЯЛЫЛЫҚТЫ ҚАМТАМАСЫЗ ЕТУДІ БАҚЫЛАУ

Құпиялылықты қамтамасыз етуді бақылау мақсатында келесі іс-шаралар қамтамасыз етілуі тиіс:

• есеп түріндегі нәтижемен АҚ талаптарын сақтауға АЖ АҚ жыл сайынғы талдау.

• АЖ серверлерінің АҚ аспаптық құралдарымен және олар орналасқан желілермен тұрақты мониторинг жүргізу.

10.6. ТҰТАСТЫҒЫ

10.6.1. Тұтастықтың басты талабы қол жеткізу деңгейлері бойынша авторизацияланған тұлғалардың ғана ақпаратты өзгертуін қамтамасыз ету болып табылады.

10.6.2. Енгізілетін жаңа бағдарламалық-аппараттық құралдар АҚ қамтамасыз етуге жауапты басшылық пен мамандар тарапынан тиісті түрде мақұлдануы тиіс.

10.6.3. Аппараттық құралдар мен бағдарламалық қамтамасыз ету енгізу алдында жүйенің басқа компоненттерімен үйлесімділікке тексерілуі тиіс.

10.7.ВИРУСҚА ҚАРСЫ ҚАУІПСІЗДІККЕ ҚОЙЫЛАТЫН ТАЛАПТАР

Антивирустық қорғауға қойылатын талаптар «антивирустық қорғауды ұйымдастыру жөніндегі Нұсқаулық» ішкі нормативтік құжатта келтірілген.

10.8. ЭЛЕКТРОНДЫҚ ПОШТА МЕН ИНТЕРНЕТТІ ҚОЛДАНУҒА ҚОЙЫЛАТЫН ТАЛАПТАР

Электрондық пошта мен Интернетті пайдалану талаптары ішкі нормативтік құжатта «ішкі станцияларда электрондық пошта мен Интернет қызметтерін пайдалану нұсқаулығы» көрсетілген.

10.9. ҚОЛ ЖЕТІМДІЛІК

10.9.1. Қол жетімділіктің басты талабы авторизацияланған адамдар онымен кедергісіз жұмыс істей алатын ақпараттың (автоматтандырылған ақпараттық жүйе ресурстарының) жай-күйін қамтамасыз ету болып табылады.

10.9.2. Штаттан тыс жағдайлар, авариялар, дүлей зілзалалар және әсер етуі мүмкін өзге де жағдайлар туындаған жағдайда үздіксіз жұмыс істеу мен қалпына келтірудің тиісті шаралары көзделуі тиіс.

10.9.3. Авариялар, дүлей зілзалалар және өзге де штаттан тыс жағдайлар осы ақпаратты кемінде 2 жыл мерзімге сақтай отырып, толық және мұқият түрде тіркелуі тиіс.

10.9.4. АҚ инциденті немесе басқа да штаттан тыс жағдай туындаған жағдайда «штаттан тыс (дағдарыстық) жағдайларда пайдаланушылардың іс-қимыл тәртібі туралы Нұсқаулықты» басшылыққа алу қажет.

10.10. ТОҚТАП ТҰРУҒА ҚОЙЫЛАТЫН ТАЛАПТАР

10.10.1. Серверлік жабдықтың істен шығуына орнықтылығы оны қайталау және жүктемені теңгеру жолымен қамтамасыз етілуі тиіс.

10.10.2. Байланыс арналарының істен шығуына орнықтылығы негізгі резервтік байланыс арнасымен қатар пайдалану жолымен қамтамасыз етілуі тиіс.

10.10.3. АЖ серверлік жабдығымен болған штаттан тыс жағдай туындаған жағдайда деректерді қалпына келтіру 2 тәуліктен аспайтын мерзімде жүргізілуі тиіс.

10.11. ҮЗДІКСІЗ ЖҰМЫС ІСТЕУ ТАЛАПТАРЫ

Үздіксіз электрмен қоректендіру қажетті қуатта ҮҚК (үздіксіз қоректендіру көзі) қамтамасыз етіледі, ол қосымшалардың жұмысын кем дегенде дұрыс аяқтауға және сыртқы электрмен қоректендіру ажыратылған кезде операциялық жүйені бұруға кепілдік беруі тиіс.

10.12. ҚУАТТАРДЫ РЕЗЕРВТЕУДІ ЖӘНЕ ҚАЙТАЛАУДЫ ҚАМТАМАСЫЗ ЕТУ ЖӨНІНДЕГІ ТАЛАПТАР

10.12.1. Деректерді сақтау жүйесі дискілердің бүтіндігін автоматты түрде кезеңдік бақылауды, нашар секторларды талдауды, әкімшінің араласуынсыз және пайдаланушылардың жұмысына әсер етпей резервтік батареялардың жай-күйін тексеруді көздеуі тиіс.

10.12.2. Деректерді сақтау жүйесі дискілерді "ыстық" ауыстыру мүмкіндігін қамтамасыз етуі тиіс.

10.13. ҚОЛ ЖЕТІМДІЛІК ЖАЙ-КҮЙІНІҢ ЖЕДЕЛ МОНИТОРИНГІН ҚАМТАМАСЫЗ ЕТУ ЖӨНІНДЕГІ ТАЛАПТАР

АЖ мониторингі күн сайын жұмыс күні ішінде мамандандырылған бағдарламалық қамтамасыз етудің көмегімен жүргізіледі, АЖ қолжетімділігінің жай-күйі өзгерген жағдайда әкімшіге "онлайн" режимінде хабарлау жүргізіледі.

10.14. АҚ ТАЛАПТАРЫНА СӘЙКЕССІЗДІКТЕР МЕН СӘЙКЕССІЗДІКТЕРДІ БАСҚАРУ

АҚ бұзылған жағдайлар мен әлсіз жерлер туралы хабарламалардан басқа АҚ бұзылған инциденттерді анықтау үшін жүйенің, ескертулердің және осалдықтардың мониторингі қолданылуы тиіс. Инциденттерді басқару рәсімдері үшін АҚ бұзушылықтары мынадай ережелер қарастырылуы тиіс:

10.14.1. Әр түрлі инциденттермен жұмыс істеу үшін келесі рәсімдерді белгілеу қажет:

- ақпараттық жүйелердің істен шығуы және сервистердің жоғалуы;
- зиянды код;
- қызмет көрсетуден бас тарту;
- толық емес немесе дәл емес деректер салдарынан қателер;
- құпиялылық пен тұтастықтың бұзылуы;
- Ақпараттық жүйелерді дұрыс пайдаланбау;

10.14.2. Үздіксіз қамтамасыз етудің әдеттегі жоспарларына толықтыру:

- инциденттің себептерін талдау және сәйкестендіру;
- оқшаулау;
- қайта көрінуді болдырмайтын қаражатты жоспарлау және енгізу
- қажет болған жағдайда инциденттер;
- инцидент әсер еткен немесе инцидент салдарын жоюға қатысатын тұлғалармен өзара іс-қимыл;
- тиісті лауазымды тұлғалардың іс-әрекеттері туралы хабардар ету;
- жүйенің іркілістерін жою және АҚ бұзу инциденттерінің салдарын жою жөніндегі іс-қимылдар мұқият формалды бақылаумен болуы тиіс.

10.14.3. Қажет болуы рәсімдерін қамтамасыз ету мақсатында сенімділігін:

• тек толық сәйкестендірілген және авторизацияланған персоналға өнеркәсіптік пайдалану ортасында жүйелер мен деректерге қол жеткізу мүмкіндігі берілген;
• төтенше жағдайлар кезінде қабылданған барлық іс-әрекеттер толық құжатпен ресімделген;
• төтенше жағдайлар кезінде қабылданған іс-әрекеттер туралы басшылыққа хабарланған және олар белгіленген тәртіппен талданды;
• бизнес-жүйелердің және бақылау жүйелерінің тұтастығы ең аз мерзімде расталған.
• АҚ бұзылған инциденттерді басқару мақсаттары басшылықпен келісілуі тиіс және инциденттерді басқаруға жауапты тұлғалар АҚ бұзылған инциденттермен жұмыс істеу кезіндегі басымдықтарды білуі тиіс.

АЖ әкімшілері анықталған осалдықтарды жедел жою қажет.

10.15. ҚҰЖАТТАМАҒА ҚОЙЫЛАТЫН ТАЛАПТАР

Әзірлеуге міндетті түрде талап етілетін ішкі нормативтік құжаттар:

• Есептеу техникасы құралдарын паспорттау және ақпараттық ресурстарды пайдалану ережесі;
• Құпия қорғау туралы Нұсқаулық;
• Штаттан тыс (дағдарыстық) жағдайларда пайдаланушылардың іс-қимыл тәртібі туралы Нұсқаулық;
• Компьютерлік жабдықтарды және бағдарламалық қамтамасыз етуді пайдалану жөніндегі Пайдаланушы нұсқаулығы;
• Антивирустық қорғауды ұйымдастыру жөніндегі Нұсқаулық;
• Сервер әкімшісінің функциялары мен өкілеттіктерін бекіту жөніндегі Нұсқаулық;
• Мамандар мен әкімшілердің серверлік бөлмеге кіру ережесі;
• Корпоративтік ақпараттық желіде пайдаланушыларды тіркеу ережелері;
• Жүйелік әкімшілердің жұмысы үшін ЖАДЫНАМА;
• Есептеуіш техника құралдарын пайдаланушыға жадынама;
• Жұмыс станцияларында электрондық пошта және Интернет қызметтерін пайдалану нұсқаулығы;
• Ақпаратты резервтік көшіру туралы Нұсқаулық.

10.16. ТӘУЕКЕЛДЕРДІ ТАЛДАУҒА ЖӘНЕ БАҒАЛАУҒА ҚОЙЫЛАТЫН ТАЛАПТАР

10.16.1. АҚ саясаты бастапқыда АҚ тәуекелдерін талдау және бағалау нәтижесінде алынған деректерге негізделуі тиіс.

10.16.2. АҚ саясатын жетілдіру мақсатында АҚ тәуекелдерін жыл сайын талдау және бағалау жүргізілуі тиіс.

10.16.3. Тәуекелдерді талдау және бағалау Қазақстан Республикасының аумағында қолданылатын стандарттарға, сондай-ақ ішкі нормативтік құжаттарға сәйкес жүргізілуге тиіс.

10.16.4. Тәуекелдерді бағалау кезінде АҚ қауіп-қатерлерін іске асырудың қаржылық жай-күйіне әсері ескерілуі тиіс. Қабылданатын шаралардың құны қауіп-қатерді іске асыру кезінде туындайтын ықтимал залалдан аспауы тиіс.

10.16.5. Тәуекелдерге талдау жүргізудің формалды рәсімі қосымшада сипатталған.

10.16.6. Шығындар мен тәуекелдер пайдаларын талдау нәтижелерінің негізінде тиісті Кәсіпорын стандарты (СТП)-ның басшылығы тәуекелді төмендету үшін неғұрлым

экономикалық тиімді шараларды айқындайды. Таңдалған шаралар АЖ үшін тиісті қауіпсіздікті қамтамасыз ету үшін техникалық, пайдалану және басқару шараларын біріктіруге тиіс.

10.16.7. Ақпаратты өңдеудің нақты құралдары мониторингінің деңгейін тәуекелдерді бағалау негізінде айқындаған жөн. Мониторинг кезінде назар аудару керек:
- келесі бөлшектерді қоса алғанда, авторизацияланған қол жеткізу:
- пайдаланушы ID;
- негізгі оқиғалардың күні мен уақыты;
- оқиғалар түрлері;
- қол жеткізу жүзеге асырылған файлдар;
- қолданылатын бағдарламалар/утилиттер;
- барлық артықшылықты әрекеттер:
- артықшылық есептік жазбаларды пайдалану, мысалы, түбірлік каталог, әкімші;
- жүйені іске қосу және тоқтату;
- енгізу/шығару құрылғысын қосу / ажырату;
- рұқсатсыз қол жеткізу;
- пайдаланушының сәтсіз немесе бұрмаланған әрекеттері;
- деректер мен басқа ресурстарды қозғайтын сәтсіз немесе бұрмаланған әрекеттер;
- желілік шлюздер мен желіаралық экрандарға қол жеткізу және хабарлау саясатын бұзу;
- басып кіруді анықтаудың жеке жүйелерінен ескерту.

10.17. АҚ САЯСАТЫН ҚАЙТА ҚАРАУ

10.17.1. АҚ саясаты дамуға, қауіпсіздік саясатын қайта қарауға және бағалауға әкімшілік жауапкершілікті бекітуге құқығы бар жауапты тұлғаға бекітілуі тиіс. Қайта қарау АЖ, АҚ саясатын жақсарту үшін бағалау мүмкіндігін және ұйымдық ортадағы, іскерлік ахуалдағы, заңды жағдайлардағы немесе техникалық ортадағы өзгерістерге жауап ретінде АҚ басқаруға көзқарасты қамтуы тиіс.

10.17.2. АҚ саясатын қайта қарау кезінде басқаруды қайта қарау нәтижелерін ескеру қажет. Қайта қарау кестесін немесе ұзақтығын қоса алғанда, қайта қарау рәсімдері айқындалуға тиіс.

10.17.3. Басқаруды қайта қарау үшін кіріс деректері:
- мүдделі тараптардан кері байланыс;
- тәуелсіз қайта қарау нәтижелері бойынша;
- алдын алу және түзету әрекеттерінің мәртебесі;
- алдыңғы қайта қарау нәтижелері;
- процестің сипаттамасы және ақпарат қауіпсіздігі саясатының сәйкестігі;
- ұйымдық ортадағы, іскерлік ахуалдағы, ресурстардың бар-жоғын, шарттық, реттеуші немесе заңды жағдайлардағы немесе техникалық ортадағы өзгерістерді қоса алғанда, АҚ-ны басқару тәсіліне әсер етуі мүмкін өзгерістерге;
- қатерлер мен осалдықтарға байланысты үрдістер;
- АҚ хабарланған инциденттеріне;
- тиісті мекемелер ұсынған ұсыныстар.

10.17.4. АҚ саясаты құпиялылықты, тұтастықты, қолжетімділікті қамтамасыз ету мақсатында елеулі өзгерістер пайда болған жағдайда қайта қаралуға тиіс.

10.17.5. АҚ саясатын қайта қарау Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы №832 қаулысымен бекітілген Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарға сәйкес жүзеге асырылуы тиіс.

10.18. АҚ ТАЛАПТАРЫНА СӘЙКЕСТІГІН БАҚЫЛАУ

АҚ осы саясатының талаптарын бақылауды АҚ-ға жауап беретін мамандар жүзеге асырады.

11 ӨЗГЕРІСТЕРДІ ЕНГІЗУ ТӘРТІБІ

11.1. Университеттің осы саясатын басқару және өзгерістер енгізу ҚП ХҚТУ-7.5.3-2019 сәйкес жүзеге асады.

11.2. СМЖ құжатына енгізілген өзгерістер «Өзгерістерді тіркеу парағында» тіркелуі тиіс. (Қосымша 3).

12 КЕЛІСУ, САҚТАУ ЖӘНЕ ТАРАТУ

12.1. Осы университет саясатының жұмыс данасын сақтау, тираждау және қолданушыларға жіберу жауапкершілігі IT Департаменті директорына жүктеледі. Осы университет саясатының жұмыс нұсқалары келесі адрестер бойынша жіберіледі: Вице-президенттер, Шымкент және Кентау институтының директорлары, факультет декандары, МБЭЖМ және ғылыми-зерттеу институтының директорлары, Мемлекеттік басқару және экономика жоғары мектебі бағдарламалары, кафедра меңгерушілері, құрылымдық бөлімдер.

12.2. Осы университет саясатының бақылау данасын Стратегиялық жоспарлау, рейтинг және сапа орталығында сақтау жауапкершілігі орталық басшысына жүктеледі.

13 ҚОСЫМШАЛАР

ҚОСЫМША 1

Ықтимал техникалық тәуекелдерді бағалау

Тәуекел түрі	Сипаттамасы	Өлшем және тәуекелді төмендету жөніндегі шаралар
Сервердің істен шығуы	Аппараттық немесе сервер жұмысындағы іркіліс.	Штаттық қызмет ету уақытының пайыздық үлесінде өлшенеді. Шарт жасасу кезінде кепілдік қызмет көрсетудің ұзақ мерзімін қарастыру, ал ол аяқталғаннан кейін серверлерді резервтеу
Жұмыс станциясының істен шығуы	Аппараттық немесе жұмыс станциясы жұмысындағы іркіліс.	Штаттық қызмет ету уақытының пайыздық үлесінде өлшенеді. Сертификатталған сервис орталықтары бар жетекші әлемдік өндірушілерден ғана сатып алу
Жіберу кезінде деректерді жоғалту немесе бұрмалау	Коммуникациялық хаттамалардың түзету қасиеттерін ескере отырып, телекоммуникациялық жабдықтағы іркілістерге байланысты байланыс арналары арқылы беру кезінде деректерді ішінара жоғалту немесе бұрмалау.	Жоғалған немесе бұрмаланған деректер үлесінде өлшенеді. Жерүсті байланыс арналарына ауыстыру және арналарды резервтеу
Сақтау кезінде деректерді жоғалту немесе бұрмалау	Тәуекел ДБ-да деректерді сақтау тәсілін есепке ала отырып, дискінің файлдық жүйесінде іркілістер немесе жинақтағыштардағы физикалық қателер мүмкіндігімен байланысты.	Сағат ішінде істен шығулар арасында орташа уақыт өлшенеді. Ақпаратты сақтау жүйелерін ұзарту, нұсқаулыққа сәйкес мерзімді резервтік көшіру.
Технологиялардың тез моральдық ескіруі	Пайдаланушылардың ППО қабылдамауы	Өтініш берушінің БПҰ платформалық тәуелсіздігі бойынша талаптарын нақтылау
Моральдық-ескірген техниканы сатып алу	Жинақтаушы материалдардың болмауы Моральдық-ескірген жабдықтарды техникалық қолдаудың болмауы	Көрсетілетін қызметтерді жеткізушілермен шарттарға қол қою кезінде жұмыстарға егжей-тегжейлі техникалық ерекшеліктерді жасау арқылы өтініш берушінің талаптарын нақтылау
АҚ төмендеуі	Ақпараттық желілерге сыртқы әсер ету, оның ішінде хакерлер мен компьютерлік вирустардың шабуылдары	АҚ қамтамасыз ету жүйесінің мониторингі және аудиті. Акт-ортаның өзгеруін, жаңа қатерлердің, инциденттердің және проблемалардың пайда болуын ескере отырып, ақпаратты қорғау бойынша қабылданған шаралардың тиімділігіне талдау жүргізу. Қосымша қорғау шараларын енгізу

ҚОСЫМША 2

Ф-СМБ-004

ТАНЫСУ ПАРАҒЫ

№	Аты-жөні	Қызметі	Мерзімі	Қолы
1.	Карипов Т.А.	IT Департамент дирек	30.01.2020	
2	Кожихов А.	Директор орынбасар	30.01.2020	
3	Елеубаев А.	жетекші бағдарлама	30.01.2020	
4	Матеева Л.	Жетекші IT маман	30.01.2020	
5	Бабашев Ч.	Инженер	30.01.2020	
6	Музаффарова З.	IT маман	30.01.2020	
7	Бердиев С.	Менеджер	30.01.2020	
8	Сопбеков Н.	жетекші инженер	30.01.2020	
9	Нагаров А.	жет. инженер-жөнт.	30.01.2020	
10	Кудайбергенов Н.	IT инженер	30.01.2020	
11	Хидоятов С.	IT инженер	30.01.2020	
12	Абдибеков А.	IT инженер	30.01.2020	
13	Келгелбек У.	IT инженер	30.01.2020	
14	Абдулаев Р.	IT инженер	30.01.2020	
15	Байшуаев Б.	Менеджер	30.01.2020	
16	Утебаев У.	жет. бағдарламашы	30.01.2020	
17.	Губеков Л.	жет. бағдарламашы	30.01.2020	
18	Бердисултанов А.	Менеджер	30.01.2020	
19	Гулентаев О.	жетекші IT маман	30.01.2020	

ҚОСЫМША 3

Ф-СМБ-002

ӨЗГЕРІСТЕРДІ ТІРКЕУ ПАРАҒЫ

№ Р/с	Өзгеріс енгізу туралы шешім		Парақ нөмірі				Қағаз саны	Өзгерістерді енгізу мерзімі	Өзгерістерді жүзеге асыратын тұлға	
	Құжат	№ бұйрық	Өзгертілген	Ауыстырылған	Жаңа	Есептен шығарылған			Аты-жөні	Қолы
1	Сенат мәжілісі	10.06.2020 №6 хат. 4.5. Сенат қаулысы	4 бет	4 бет	1	1	1	11.06.20		

Қожа Ахмет Ясауи атындағы Халықаралық қазақ-түрік университеті
2019-2020 оқу жылындағы кезектен тыс Сенат мәжілісі

№6 хаттамадан көшірме

Түркістан қаласы **10 маусым 2020 жыл**

Сағат – 15:00 сәрсенбі

Онлайн

Қатысатындар: Сенат мүшелері

Күн тәртібінде:

4. Университет стандарттары мен ережелеріне өзгерістер мен толықтырулар енгізу, бекіту туралы

Ашық дауыс беру нәтижесінде **СЕНАТ ҚАУЛЫ ЕТЕДІ:**

4.5. Университеттің Бейнебақылау жүйесі туралы Ережесі;

- Есептеу техникасы құралдарын паспорттау және ақпараттық ресурстарды пайдалану Ережесі;
- Корпоративтік ақпараттық желіде пайдаланушыларды тіркеу Ережесі;
- Мамандар мен әкімшілердің серверлік бөлмеге кіру Ережесі бекітілсін.
- Ахмет Ясауи университетінің ресми сайты бойынша Ережесі;
- Ахмет Ясауи университетінің ақпараттық қауіпсіздік саясатына өзгерістер мен толықтырулар енгізілсін *(Жауапты: IT Департаментінің директоры Т.Карипов).*

Сенат төрағасы **Б.Абдрасилов**
Сенат хатшысы **М.Асанова**

Қожа Ахмет Ясауи атындағы
Халықаралық қазақ-түрік университетінің
СЕНАТЫ
Хаттамадан көшірме дұрыс
Сенат хатшысы
«12» 06 2020 ж

М.Асанова

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

БҰЙРЫҚ

02 марта 2020 г.

Астана қаласы

ПРИКАЗ

№ 49

город Астана

Бланк сериялық нөмірсіз жарамсыз болып табылады.
Бланк без серийного номера недействителен.

«Об определении минимальных требований к программно-аппаратному комплексу и прикладному программному обеспечению, используемых в организациях образования»

В соответствии с пунктом 3 статьи 65 Закона Республикик Казахстан от 6 апреля 2016 года «О правовых актах», и в целях обеспечения единого подхода и создания условий для перехода на качественный уровень использования новых цифровых технологий в сфере образования, **ПРИКАЗЫВАЮ**:

1. Определить рекомендуемые минимальные требования к программно-аппаратному комплексу и прикладному программному обеспечению, используемых в организациях образования (далее – Цифровой портфель), согласно приложениям 1 и 2 к настоящему приказу.

2. Рекомендовать организациям образования в течение первого полугодия 2020 года привести компьютерную и периферийную технику, а также инфраструктуру и информационные системы в соответствие с Цифровым портфелем.

3. Департаменту цифровой трансформации образования Министерства образования и науки Республики Казахстан:

1) до 10 марта 2020 года довести требования Цифрового портфеля до сведения всех организаций образования;

2) в срок до 31 марта 2020 года совместно с акционерным обществом «Информационно-аналитический центр» Министерства образования и науки Республики Казахстан разработать и утвердить типовые правила

001365

1 ҚОЛДАНЫЛУ САЛАСЫ

1.1. Университеттің барлық оқытушыларына және қызметкерлеріне қолданылады.

2 МАҚСАТЫ

2.1. Қожа Ахмет Ясауи атындағы Халықаралық қазақ-түрік университетінде ақпараттық қауіпсіздікті қамтамасыз ету.

3 НОРМАТИВТІ СІЛТЕМЕЛЕР (СІЛТЕМЕЛІК ҚҰЖАТТАР)

3.1. Ақпараттық қауіпсіздікке жауап беретін мамандар Қазақстан Республикасының Дербес деректер және оларды қорғау туралы 2013 жылғы 21 мамырдағы № 94-V Заңының (Дербес деректер және оларды қорғау туралы заң) талаптарына, дербес деректердің ақпараттық жүйелерінде өңдеу кезінде дербес деректерді қорғауға қойылатын талаптарға («Дербес деректер және оларды қорғау туралы» Заңның 2-тарауы) сәйкес ақпараттық жүйе ақпаратының пайдаланылуын бақылауды қамтамасыз етуі тиіс.), Ақпараттандыру туралы «Қазақстан Республикасының 2015 жылғы 24 қарашадағы № 418-V Заңы».

3.2. «Ақпараттандыру туралы» 2015 жылғы 24 қарашадағы № 418-V Қазақстан Республикасының Заңы;

3.3. Қазақстан Республикасының 2003 жылғы 7 қаңтардағы № 370-II Заңы 25.11.2019 ж. «электрондық құжат және электрондық цифрлық қолтаңба туралы»);

3.4. «Қазақстан Республикасының ақпараттық қауіпсіздігінің 2016 жылға дейінгі тұжырымдамасы туралы» Қазақстан Республикасы Президентінің 2011 жылғы 14 қарашадағы № 174 Жарлығы;

3.5. «Ақпараттық қауіпсіздікті қамтамасыз етудің жедел орталықтары мен Ақпараттық қауіпсіздікті ұлттық үйлестіру орталығы арасындағы ақпараттық қауіпсіздікті қамтамасыз ету үшін қажетті ақпарат алмасу қағидалары» Қазақстан Республикасының Қорғаныс және аэроғарыш өнеркәсібі министрінің 2018 жылғы 19 наурыздағы № 48/НҚ бұйрығы. Қазақстан Республикасының Әділет министрлігінде 2018 жылғы 11 мамырда №16886;

3.6. Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы №832 қаулысымен бекітілген Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптары;

3.7. ҚР СТ ISO / IEC 27002-2015 ақпараттық технология Ақпараттық қауіпсіздік менеджменті жүйесінің қауіпсіздігін қамтамасыз ету әдістері мен құралдары.

3.8. «Білім беру ұйымдарында пайдаланылатын бағдарламалық-аппараттық кешенге және қолданбалы бағдарламалық қамтамасыз етуге қойылатын ең төменгі талаптарды айқындау туралы» Қазақстан Республикасының Білім және Ғылым министрлігінің 2020 жылғы 2 наурыздағы №79 бұйрығы.

4 ЖАУПКЕРШІЛІК

4.1. IT Департаментінің ақпараттық қауіпсіздік бөлімі осы саясаттың барлық тармақтарының орындалуын қамтамасыз етеді.

4.2. IT Департаментінің ақпараттық қауіпсіздік бөлімі университеттің ақпараттық жүйесінің ақпараттық қауіпсіздігі саласындағы бастамаларды басқаруды және қолдауды қамтамасыз етуі тиіс.

4.3. Ақпараттық қауіпсіздікке жауап беретін мамандар пайдаланылатын ақпараттық жүйелерде бақылау шараларын үйлестіруді қамтамасыз етуі тиіс.