



БЕКІТІЛДІ

М.Х.Дулати атындағы Тараз
университеті" Ке АҚ Ғылыми кеңесінің
шешімімен
(25.12.2024ж. №5 хаттама)

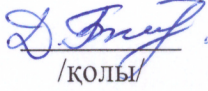
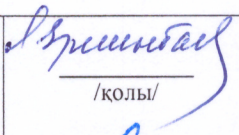
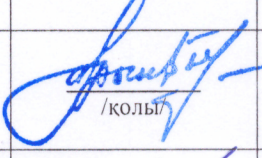
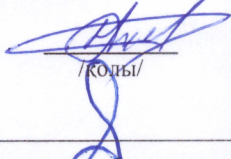
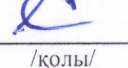

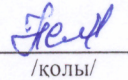
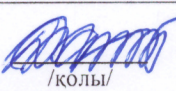
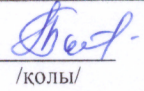
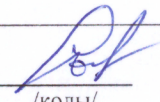
"М.Х. ДУЛАТИ АТЫНДАҒЫ ТАРАЗ УНИВЕРСИТЕТІ" Ке АҚ АҚПАРАТТЫҚ ҚАУІПСІЗДІК САЯСАТЫ

Тіркеу № 16

ТАРАЗ, 2024

«М.Х. Дулати атындағы Тараз университеті» Ке АҚ зияткерлік меншігі болып табылады.
Қайта басуға және/немесе одан әрі үшінші тұлғаларға беруге тыйым салынады

АЛҒЫ СӨЗ

1.ӘЗІРЛЕУШІЛЕР	Жобалық басқару және цифрландыру орталығының басшысы Төлегенова Д.М.	 /КОЛЫ/	20.12.24 ж.
2.ЕНГІЗІЛДІ	Жобалық басқару және цифрландыру орталығымен		
3.ТЕКСЕРУ КЕЗЕҢДІЛІГІ	3 жыл		
4.ОРНЫНА ЕНГІЗІЛГЕН	Алғаш рет		
5.ТАРАТУ	факультеттерге, кафедраларға, құрылымдық бөлімдерге		
6.БЕКІТІЛДІ ЖӘНЕ КОЛДАНЫСҚА ЕНГІЗІЛДІ	"М.Х.Дулати атындағы Тараз университеті" Ке АҚ Ғылыми кеңесінің шешімімен (25.12.2024ж. №5 хаттама)		
7.КЕЛІСІЛДІ:	Басқарма мүшесі – академиялық мәселелер бойынша проректор Еркинбаева Л.К.	 /КОЛЫ/	24.12.24 ж.
	Басқарма мүшесі – ғылым және цифрландыру жөніндегі проректор Орынбаев С.А.	 /КОЛЫ/	24.12.24 ж.
	Басқарма мүшесі – әлеуметтік – мәдени даму жөніндегі проректор Тұрлыбек А.Е.	 /КОЛЫ/	24.12.24 ж.
	Басқарма мүшесі – инфрақұрылымды дамыту жөніндегі проректордың м.а. Есмаханов Б.М.	 /КОЛЫ/	24.12.24 ж.
	Басқарма мүшесі – Стратегиялық даму және интернационалдандыру жөніндегі проректор Есимова Ш.А.	 /КОЛЫ/	23.12.24 ж.
	Техникалық қолдау және IT қолдау орталығының басшысы Жаукашканов А.Қ.	 /КОЛЫ/	23.12.24 ж.
	Стратегиялық даму басқармасының басшысы Дарибаев Ж.Е.	 /КОЛЫ/	23.12.24 ж.
	Аккредиттеу, рейтинг және сапаны қамтамасыз ету бөлімінің басшысы Балкибаева Г.А.	 /КОЛЫ/	23.12.24 ж.
	Заң қызметінің басшысы м.а. Самбетов С.Т.	 /КОЛЫ/	20.12.24 ж.

Бұл құжат «М.Х.Дулати атындағы Тараз университеті» Ке АҚ Басқарма Төрағасы–Ректордың рұқсатынсыз толық немесе ішінара көшірілмейді, көбейтілмейді және таратылмайды.

МАЗМҰНЫ

1. Қолдану саласы.....	4
2. Нормативтік сілтемелер.....	5
2.1 Нормативтік құжаттар.....	5
3. Негізгі терминдер, қысқартулар және белгілер.....	5
3.1 Негізгі терминдер.....	5
3.2 Қысқартулар.....	5
4. Жауапкершілік және өкілеттіктер.....	5
5. Жалпы ережелер.....	6
6. Саясаттың мақсаты.....	7
7. Талаптар мен ұсыныстар.....	8
8. Жоспарлау.....	10
9. Сәйкестендіру.....	11
10. Ақпараттың тұтастығы.....	11
11. Ақпараттың қолжетімділігі.....	12
12. Тәуекелдерді басқару.....	14
А қосымшасы. Танысу парағы.....	18
Б қосымшасы. Өзгерістерді тіркеу парағы	18

1. ҚОЛДАНЫЛУ САЛАСЫ

Осы "М.Х. Дулати атындағы Тараз университеті" Ке АҚ Ақпараттық қауіпсіздік саясаты - университетте ақпаратты қорғау жөніндегі негізгі қағидаттарды, бағыттар мен талаптарды айқындайды, ақпараттық қауіпсіздік режимін қамтамасыз ету үшін негіз болып табылады және ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі тиісті ережелерді, қағидаларды, нұсқаулықтарды әзірлеу кезінде басшылық ретінде қызмет етеді.

Ақпаратты, оның ішінде құпия мәліметтерді және/немесе дербес деректерді автоматтандырылған әзірлеу жүзеге асырылатын Қоғамның (орталық аппараттың және өңірлік өкілдердің) барлық құрылымдық бөлімшелері мен персоналымен таратылады және қолдануға міндетті.

Талаптары тиісті шарт/келісім (SLA) негізінде ақпарат пен қызметтердің қатысушылары мен тұтынушылары ретінде жұртшылықпен бірге кіретін басқа ұйымдар мен мекемелерге де қолданылады.

Талаптары қоғамның барлық құрылымдық бөлімшелерінің басшылары мен қызметкерлеріне және міндетті түрде сақтау үшін белгілерге қолданылады.

Саясат Университеттің ақпараттық жүйелеріне қолжеткізе алатын барлық қызметкерлерге, студенттерге, серіктестерге және үшінші тұлғаларға қолданылады.

Қызметкерлер:

- Университеттің барлық тұрақты, уақытша және келісімшарттық қызметкерлері.
- Азаматтық-құқықтық шарттар негізінде жұмыс істейтіндер.
- Тағылымдамадан өтушілер мен практиканттарды қоса алғанда, келісімшарт бойынша немесе уақытша жұмыс істейтін адамдар.

Студенттер:

- Университеттің ақпараттық жүйелеріне қолжеткізе алатын барлық тіркелген студенттер.
- Бакалавриат, магистратура және докторантура студенттері.
- Ақпараттық ресурстарға қашықтан қолжеткізе алатын Қашықтықтан оқытуға немесе алмасу бағдарламаларына қатысатын студенттер.

Серіктестер және үшінші тұлғалар:

- Сыртқы ұйымдар, кеңесшілер, мердігерлер және университеттің ақпараттық жүйелерімен өзара әрекеттесетін кез келген басқа адамдар.
- Серіктестік білім беру және ғылыми-зерттеу мекемелері.
- Қызметтердің сыртқы жеткізушілері және келісімшарттық міндеттемелер бойынша университеттің ақпараттық ресурстарына қол жеткізе алатын мердігерлер.

Саясат университеттің барлық ақпараттық ресурстарын, соның ішінде компьютерлік жүйелерді, желілерді, мәліметтербазасын және құжаттарды қамтиды.

Компьютерлік жүйелер:

- Деректерді сақтау және өңдеу үшін пайдаланылатын серверлер.
- Қызметкерлер мен студенттер пайдаланатын жұмыс үстелдері мен ноутбуктер.
- Университеттің ақпараттық жүйелеріне қолжеткізе алатын планшеттер мен смартфондар сияқты мобильді құрылғылар.

Желілер:

- Құрылғылардың ішкі байланысын қамтамасыз ететін жергілікті желілер (LAN).
- Университеттің әртүрлі кампустары мен қашықтағы нысандарын байланыстыратын ғаламдық желілер (WAN).
- Интернетке және университеттің ішкі ресурстарына қолжеткізуді қамтамасыз ететін сымсыз желілер (Wi-Fi).
- Қауіпсіз қашықтан қолжеткізу үшін пайдаланылатын виртуалды жеке желілер (VPN).

Мәліметтер базасы:

- Университет қызметіне қатысты ақпаратты қамтитын барлық мәліметтер базасы.
- Студенттер мен білім беру бағдарламалары туралы ақпаратты қамтитын оқу мәліметтер базасы.
- Зерттеу нәтижелері мен жарияланымдарды қамтитын ғылыми-зерттеу дерекқорлары.
- Университеттің қызметкерлері мен операциялары туралы ақпаратты қамтитын әкімшілік мәліметтер базасы.

Құжаттар:

- Келісімшарттар, келісімдер және ресми құжаттар сияқты құпия ақпаратты қамтитын физикалық құжаттар.
- Серверлерде, жұмыс станцияларында және бұлттық оймаларда сақталатын электрондық құжаттар.
- Оқу және ғылыми-зерттеу қызметі шеңберінде құрылатын және өңделетін құжаттар, сондай-ақ әкімшілік құжаттар.

2. НОРМАТИВТІ СІЛТЕМЕЛЕР (СІЛТЕМЕЛІК ҚҰЖАТТАР)

2.1 Осы ақпараттық қауіпсіздік саясатын әзірлеуде келесі нормативтік құжаттарға сілтемелер жасалды:

ҚР заңы	Қазақстан Республикасының «Дербес деректер және оларды қорғау туралы» Заңы – жеке және дербес деректерді өңдеу мен қорғау саласындағы негізгі талаптар мен ережелерді анықтайды.
ҚР заңы	Қазақстан Республикасының «Ақпараттандыру туралы» Заңы – ақпараттық технологияларды қолдану, ақпараттық жүйелердің қауіпсіздігін қамтамасыз ету және электрондық үкіметті дамытуға арналған негізгі құқықтық нормаларды белгілейді
ҚР Қаулысы	Қазақстан Республикасының «Ақпараттық қауіпсіздік талаптарын бекіту туралы» Қаулысы – мемлекеттік және жеке секторларда ақпараттық қауіпсіздік шараларын ұйымдастыру бойынша міндетті талаптарды анықтайды.
ҚР Қаулысы	Қазақстан Республикасы Үкіметінің «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы» 20.16.2016.жылғы №832 Қаулысы – ақпараттық қауіпсіздік пен ақпараттық-коммуникациялық технологиялар саласында бірыңғай талаптарды белгілейді.
Стандарт	ISO/IEC 27001 стандарты – ақпараттық қауіпсіздік менеджменті жүйесін құру және қолдау бойынша халықаралық стандарт.
Стандарт	ISO/IEC 27002 стандарты – ақпараттық қауіпсіздікті басқару тәжірибесіне негізделген нұсқаулықтар, соның ішінде ақпараттық қауіпсіздікті қамтамасыз ету бойынша ұсыныстарды қамтиды.
ҚР кодексі	Қазақстан Республикасының Қылмыстық кодексі – ақпараттық жүйелерге заңсыз қол жеткізуге және дербес деректерді рұқсатсыз пайдалануға қатысты құқықтық жауапкершілікті қарастырады.

3. НЕГІЗГІ ТЕРМИНДЕР, ҚЫСҚАРТЫЛҒАН СӨЗДЕР ЖӘНЕ БЕЛГІЛЕР**3.1 Негізгі терминдер**

Осы Саясат мақсатында мынадай терминдер мен анықтамалар пайдаланылады:

Ақпараттық қауіпсіздік	-ақпараттың құпиялылығы, тұтастығы және қолжетімділігі қамтамасыз етілетін қорғалу жағдайы.
Құпиялылық	-белгілі бір адамдардың оған қолжеткізуін шектейтін ақпараттың қасиеті.
Тұтастық	— ақпаратты өңдеу процесінде оның сенімділігі мен өзгермейтіндігінен тұратын қасиет.
Қолжетімділік	-ақпаратты қажетті уақытта және қажетті жерде мақсатына қарай пайдалану мүмкіндігінен тұратын қасиет.
Ақпараттық қауіпсіздікке қауіп	-ақпараттық қауіпсіздікті бұзудың ықтимал немесе нақты қауіпін тудыратын жағдайлар мен факторлардың жиынтығы.
Ақпараттық қауіпсіздіктің осалдығы	-ақпараттық қауіпсіздікті бұзу үшін пайдаланылуы мүмкін қажетті қауіпсіздік деңгейінің болмауы немесе осалдығы.
Ақпараттық қауіпсіздік тәуекелі	-ақпараттық қауіпсіздік қатерін іске асыру ықтималдығы мен ықтимал залал шамасының үйлесімі.
Тәуекелдерді басқару процестері	-ақпараттық қауіпсіздік тәуекелдерін анықтауға, бағалауға және азайтуға бағытталған дәйекті әрекеттер жиынтығы.
Жаңартулар	–қателерді түзету, осалдықтарды жою немесе жаңа мүмкіндіктерді қосу үшін бағдарламалық құралға немесе аппараттық құралға Енгізілген өзгерістер.

3.2 Қысқартылған сөздер

Осы құжатта төменде келтірілген қысқартылған сөздер пайдаланылады:

Университет	<i>М.Х. Дулати атындағы Тараз университеті</i> (Университет имени М.Х. Дулати): Бұл құжатта Университет деп Тараз қаласында орналасқан М.Х. Дулати атындағы коммерциялық емес акционерлік қоғам түріндегі оқу орнын айтамыз.
АҚ	<i>Ақпараттық қауіпсіздік</i> (Информационная безопасность): Талап ететін ережелер мен бақылауларды орнату арқылы деректерді рұқсатсыз қол жеткізуден, пайдаланудан және өзгеруден қорғау.
ДҚ	<i>Деректер қоры</i> (База данных): Университеттің ақпараттық ресурстары, соның ішінде студенттердің мәліметтері мен зерттеу деректері.
ЖК	<i>Жеке компьютер</i> (Персональный компьютер): Университеттегі қызметкерлер мен студенттердің жұмыс істейтін құрылғылары.
ISMS	<i>Ақпараттық қауіпсіздікті басқару жүйесі</i> (Information Security Management System): Ақпараттық қауіпсіздік саясатын іске асыруды басқару және бақылау жүйесі.
VPN	<i>Виртуалды жеке желі</i> (Virtual Private Network): Университеттің ішкі желілеріне қауіпсіз қашықтан қол жеткізуге арналған технология.
SLA	<i>Қызмет көрсету деңгейінің келісімі</i> (Service Level Agreement): Қызметтерді жеткізу және талаптар деңгейін көрсетуге арналған келісім.

4. ЖАУАПКЕРШІЛІК ЖӘНЕ ӨКІЛЕТТІЛІК

4.1 Университеттің осы саясаты М.Х.Дулати атындағы Тараз университетінің Ғылыми кеңесінің шешімімен бекітіледі.

4.2 Осы саясаттың талаптарға сай енгізілуіне жобалық басқару және цифрландыру орталығы жауапты болады.

4.3 Осы стандарттың «Құжатталған ақпаратты басқару» 01 стандартының талаптарына сәйкес болуына құжатты әзірлеуші және жауапты болады.

4.4 Құжаттаманы басқару үдерісінің нақты кезеңдерін орындау жөніндегі қызметті ұйымдастыру мен үйлестіру үшін және соңғы нәтижелердің сапасы үшін бөлімше басшылары, сондай-ақ наты кезеңді орындауға қатысушы болып табылатын лауазымды тұлғалар жауап береді.

4.5 Бөлімшедегі осы құжаттың сақталуына және рұқсатсыз көшірілуіне және қызметтік ақпараттың жария етілуіне тиісті бөлімшелердің басшылары жауапты болады.

4.6 Осы құжатты әзірлеу, ресімдеу, келісу және бекіту, сондай-ақ оған өзгерістер енгізу УСТ-ның 01-тармағына сәйкес жүргізілуге тиіс.

4.7 Түпнұсқаны университеттің аккредиттеу, рейтинг және сапаны қамтамасыз ету бөліміне сақтауға беру үшін әзірлеуші жауапты болады.

4.8 Осы саясаттың ескерілген жұмыс даналарын жобалық басқару және цифрландыру орталығы университеттің факультеттеріне және кафедраларына, құрылымдық бөлімдеріне таратады. Саясаттың көбейтілуіне «Dulaty university» баспасының директоры жауап береді.

4.9 СМЖ құжатына енгізілген өзгерістер «Өзгерістерді тіркеу парағында» тіркелуі тиіс.

4.10 Осы университет саясаттың бақылау данасын аккредитация, рейтинг және сапаны қамтамасыз ету бөлімінде сақтау жауапкершілігі бөлім басшысына жүктеледі.

4.11 Осы саясатты бұзған жағдайда арнайы құрылған комиссия шешімімен жауапқа тартылады.

5. ЖАЛПЫ ЕРЕЖЕЛЕР

5.1. Осы "М.Х. ДУЛАТИ атындағы Тараз университеті" коммерциялық емес акционерлік қоғамының ақпараттық қауіпсіздік саясаты (бұдан әрі - саясат) Қазақстан Республикасының қолданыстағы заңнамасына, "М.Х.ДУЛАТИ атындағы Тараз университеті" коммерциялық емес акционерлік қоғамының (бұдан әрі - Университет) нормативтік актілеріне және басқа да ішкі ережелеріне сәйкес әзірленді.

5.2. Осы Саясатта құпия ақпараттың мынадай анықтамасы қолданылады: "құпия ақпарат" пайдаланушылардың дербес деректері, бағдарламалық өнімдер дерекқорындағы деректер туралы кез келген және барлық ақпаратты, сондай-ақ университеттің және оның клиенттерінің (клиенттік база) қызметіне қатысты кез келген ақпаратты, білімді, ноу-хауды, коммерциялық ақпаратты, қандай да бір баға белгілеуді білдіреді осылайша қызметкерге өндірістік қызмет нәтижесінде белгілі болды.

5.3. Осы Саясат университеттің материалдық құндылықтары ретінде ақпараттық активтерді кездейсоқ немесе қасақана өзгертуден, ашудан немесе жоюдан қорғау мақсатында, сондай-ақ ақпараттың құпиялылығын, тұтастығы мен қолжетімділігін сақтау, тапсырыс берушілермен және серіктестермен ақпараттық өзара іс-қимыл процестерін қамтамасыз ету мақсатында қажетті шаралар қабылдауды көздейді.

5.4. Ақпараттық қауіпсіздіктің сақталуына университеттің әрбір қызметкері жауапты болады. Қызметкер өзінің қызметтік міндеттерін орындау үшін қажетті ақпаратпен уақтылы және толық қамтамасыз етілуі керек.

5.5. Осы Саясатта "қызметкер" термині университеттің барлық қызметкерлері, оның ішінде университетте азаматтық-құқықтық сипаттағы шарттар бойынша жұмыс істейтіндер деп түсініледі. Осы саясатты қолдану осындай шартта шартталуы тиіс.

5.6. Ақпараттық қауіпсіздік университет қызметінің маңызды аспектілерінің бірі болып табылады. Ұйым ақпараттың құпиялылығын, тұтастығын және қолжетімділігін, сондай-ақ рұқсатсыз кіруден, пайдаланудан, ашудан, өзгертуден, жоюдан немесе деректердің жоғалуынан қорғауды қамтамасыз етуге тырысады.

5.7. Осы саясат еңбекшарты жасалған күні университеттің әрбір қызметкерінің назарына жеткізілуі тиіс.

6. САЯСАТТЫҢ МАҚСАТЫ

6.1. Осы Саясаттың мақсаттары:

- Университеттің құпия ақпаратын сақтау.
- Қызметкерлерді ақпараттық қауіпсіздік туралы оқытуды және хабардар етуді қамтамасыз ету.
- Ақпараттық қауіпсіздік жүйесіне тұрақты тексерулер мен аудиттер жүргізу.
- Университеттің ақпараттық ресурстарының құпиялылығын сақтау.
- Университеттің тапсырыс берушілері мен және серіктестері мен өзара іс-қимыл процесінде кез келген нысанда берілген ақпараттың құпиялылығын сақтау.
- Бизнес қызметін қолдау үшін университеттің ақпараттық ресурстарына қолжетімділікті қамтамасыз ету.
- Пайдаланушылардың Университеттің ақпараттық ресурстарымен байланысты тәуекелдер туралы хабардарлығын арттыру.
- Университеттегі ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметкерлердің жауапкершілік дәрежесі мен міндеттерін анықтау.
- ISO/IEC 27001, ISO/IEC 27002-2023 халықаралық стандарттарына сәйкес жүйелердің ақпараттық қауіпсіздігін және деректерді қорғауды қамтамасыз ету.
- "Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы" Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысын сақтау.

6.2. Университет бөлімшелерінің басшылары осы Саясат ережелерінің сақталуына тұрақты бақылауды қамтамасыз етуі тиіс:

- Ақпараттық қауіпсіздік саясатының сақталуын бақылау үшін әр бөлімшеде жауапты тұлғаларды тағайындау.
- Ақпараттық қауіпсіздік мәселелері бойынша тұрақты кеңестер мен есептер өткізу.
- Ақпараттық қауіпсіздіктің сақталуын мерзімді тексерулерді ұйымдастыру, кейіннен аталған тексерудің нәтижелері бойынша есепті университет басшылығына ұсыну.
- Ақпаратты қорғау шараларын үйлестіру және бақылау үшін ақпараттық қауіпсіздікті басқару жүйесін (ISMS) енгізу.

7. ТАЛАПТАР МЕН ҰСЫНЫСТАР

7.1. Ұйымдастыру шаралары

7.1.1. АҚ үшін жауапты адамды тағайындау:

- Осы саясатты іске асыруға және оның орындалуын бақылауға жауапты ақпараттық қауіпсіздік бөлімінің басшысы тағайындалсын.
- Ақпаратты қорғау жөніндегі шараларды әзірлеу мен енгізуді қоса алғанда, АҚ бөлімі басшысының міндеттері мен өкілеттіктерін айқындау.
- Ақпаратты қорғау жөніндегі күш-жігерді үйлестіру үшін әртүрлі департаменттердің өкілдерін қамтитын ақпараттық қауіпсіздік комитетін құру.
- АҚ саласындағы ағымдағы мәселелер мен әзірлемелерді талқылау үшін комитеттің тұрақты кездесулерін анықтаңыз.

•

7.1.2. Оқыту және хабардарлықты арттыру:

- АҚ мәселелері бойынша қызметкерлер мен студенттер үшін тұрақты тренингтер мен оқытулар өткізу.
- Пайдаланушылардың әртүрлі санаттарына бағытталған АҚ негіздері бойынша Оқу материалдары мен курстарын әзірлеу.
- АҚ мәселелері бойынша материалдарды (брошюралар, плакаттар, электрондық таратылымдар) әзірлеу және тарату.
- Барлық мүдделі тараптардың хабардарлығын қамтамасыз ету үшін әртүрлі байланыс арналарын пайдаланыңыз.

•

7.1.3. Қолжеткізуді басқару:

- 7.1.3.1. Аутентификация мен авторизацияны пайдалану арқылы ақпараттық жүйелерге қолжеткізуді бақылауды қамтамасыз ету.
- 7.1.3.2. Маңызды жүйелер үшін көп факторлы аутентификацияны (MFA) енгізу.
- 7.1.3.3. Қызметкерлердің лауазымдық міндеттеріндегі өзгерістер негізінде қолжеткізу құқықтарын үнемі қайта қарау және жаңарту.
- 7.1.3.4. Есептік жазбалар мен қолжеткізу құқықтарына мерзімді тексерулер жүргізу.

7.2. Техникалық шаралар

7.2.1. Желіні қорғау:

- Университет желісінің периметрін қорғау үшін брандмауэрлерді (firewalls) пайдаланыңыз.
- Кіріс және шығыс трафикті сүзу үшін қауіпсіздік саясатын орнатыңыз.
- Желілік трафикті бақылау және күдікті әрекеттерді анықтау үшін интрузияны анықтау және алдын алу жүйелерін (IDS/IPS) орналастырыңыз.
- IDS/IPS қолтаңбалары мен ережелерін олардың өзектілігін қамтамасыз ету үшін үнемі жаңартып отырыңыз.
- Барлық компьютерлер мен серверлерде антивирустық бағдарламалық жасақтаманы орнатыңыз және үнемі жаңартыңыз.
- Антивирустық мәліметтер базасын автоматы түрде жаңартуды және тұрақты сканерлеуді қамтамасыз етіңіз.

7.2.2. Шифрлау:

- Құпия ақпаратты желі арқылы беру кезінде және деректер тасымалдағыштарында сақтау кезінде қорғау үшін шифрлауды қолдану.
- Деректерді беру үшін қорғалған қосылым протоколдарын (SSL/TLS) пайдаланыңыз.
- Университеттің ақпараттық ресурстарына қашықтан қолжеткізу үшін қорғалған байланыс арналарын (мысалы, VPN) пайдалануды қамтамасыз етіңіз.
- Күшті шифрлау және аутентификация алгоритмдерін пайдаланып VPN орнатыңыз.

7.2.3. Сақтық көшірме жасау:

- Маңызды ақпараттың тұрақты сақтық көшірмесін жасау процедураларын әзірлеу және енгізу.
- Сақтық көшірмелердің кестесі мен жиілігін анықтаңыз.
- Сақтық көшірмелерді бірнеше физикалық және географиялық орналасқан жерлерде сақтаңыз.
- Қашықтағы деректер орталықтарында сақтық көшірмелерді қауіпсіз сақтауды қамтамасыз етіңіз.

- Сақтық көшірмелерден деректерді қалпына келтіру процедураларын үнемі тексеріп отырыңыз.
- Сақтық көшірмелердің денсаулығы мен өзектілігін тексеру үшін деректерді қалпына келтіруді тексеріңіз.

7.3. Оқиғаларды басқару

7.3.1. Оқиғаларды анықтау:

- АҚ инциденттерін бақылау және анықтау үшін рәсімдерді әзірлеу.
- Күдікті әрекеттерді анықтау үшін автоматтандырылған бақылау және журналды талдау жүйелерін пайдаланыңыз.
- Журналдарды жинау және талдау үшін оқиғалар мен қауіпсіздік ақпаратын басқару жүйелерін (SIEM) пайдаланыңыз.
- Оқиғаларды корреляциялау және оқиғаларды уақтылы анықтау үшін SIEM орнатыңыз.

7.3.2. Оқиғаларға жауап беру:

- Жауапты тұлғаларды хабардар етуді, тергеуді және салдарын жоюды қоса алғанда, оқиға болған жағдайда іс-қимыл тәртібін айқындау.
- Хабарлау, тергеу және инциденттерді жою бойынша қадамдарды қамтитын инциденттерге ден қою жоспарын әзірлеу.
- Оқиғаларға жауап беру тобын (CSIRT) тағайындаңыз және оны қажетті ресурстар мен өкілеттіктермен қамтамасыз етіңіз.
- CSIRT мүшелерін әртүрлі оқиғаларға жауап беру әдістеріне үйрету және сыртқы ұйымдармен өзара әрекеттесуді қамтамасыз ету.

7.3.3. Оқиғалардан кейін қалпына келтіру:

- Университет қызметіне әсерін азайту үшін АҚ инциденттерінен кейін жүйелер мен деректерді қалпына келтіруді қамтамасыз ету.
- Қалпына келтірілген деректердің тұтастығын тексеруді қамтитын жүйелер мен деректерді қалпына келтіру процедураларын жасаңыз.
- Себептерді анықтау және болашақта олардың алдын алу шараларын әзірлеу үшін инциденттерге талдау жүргізу.
- Өткізу соғыстан кейінгі бағалау (post-incidentreview) әлсіз жақтарын анықтау және АҚ шараларын жақсарту.

7.4. Сәйкестік және аудит

7.4.1. Заңнамаға сәйкестігі:

- Ақ саясаты Қазақстан Республикасының қолданыстағы заңнамасына және халықаралық стандарттарға сәйкес келуі тиіс.
- Заңнамадағы және нормативтік актілердегі өзгерістерге сәйкес саясатты үнемі жаңартып отыру.
- АҚ саласындағы нормативтік актілер мен стандарттар талаптарының сақталуын қамтамасыз ету.
- Нормативтік талаптар мәселелері бойынша қызметкерлерді оқыту және нұсқау беру.

7.4.2. Аудит және бақылау:

- АҚ шараларының тиімділігін және саясатқа сәйкестігін бағалау үшін тұрақты ішкі және сыртқы аудиттер жүргізу.
- Аудит жүргізуге және оларды өткізу жиілігін анықтауға жауаптылар тағайындалсын.

- Анықталған кемшіліктер мен сәйкессіздіктерді жою бойынша іс-қимыл жоспарын әзірлеу және енгізу.
- Түзету әрекеттерін орындау мерзімдері мен жауаптыларын анықтаңыз.

8. ЖОСПАРЛАУ

8.1. Ақпараттық қауіпсіздік шараларын жоспарлау мыналарды қамтуы керек:

8.1.1. АҚ шараларын іске асыру үшін қажетті ресурстарды анықтау:

- Техникалық, қаржылық және адами ресурстарды қоса алғанда, ақпараттық қауіпсіздік саласындағы ағымдағы және болашаққа жеттіліктерді бағалау.
- Ақпараттық қауіпсіздік жөніндегі іс-шараларды іске асыру үшін қажетті бюджетті айқындау.
- Университеттің басымдықтары мен стратегиялық мақсаттарына сәйкес ресурстарды тарату және бөлу.

8.1.2. Ақпаратты жақсарту жөніндегі іс-шаралар жоспарын әзірлеу және бекіту:

- Ақпараттық қауіпсіздікті жақсарту бойынша нақты қадамдар мен іс-қимылдарды қамтитын іс-шаралардың егжей-тегжейлі жоспарын әзірлеу.
- Жоспарға жаңа технологияларды енгізу, бағдарламалық қамтамасыз етуді жаңарту, қызметкерлерді оқыту және аудит жүргізу жөніндегі іс-шараларды енгізу.
- Университет басшылығының іс-шаралар жоспарын оның ресми мәртебесі мен орындалу міндеттілігін қамтамасыз ету үшін бекітуі.

8.1.3. Іс-шараларды орындау мерзімдерін және жауапты тұлғаларды белгілеу:

- Ақпараттық қауіпсіздік бойынша әрбір іс-шараны орындау үшін нақты мерзімдерді анықтау.
- Іс-шараларды бақылайтын және орындайтын жауапты адамдарды немесе топтарды тағайындау.
- Басшылыққа тұрақты есеп беруді қамтитын іс-шаралардың орындалуын бақылау және есеп беру жүйесін әзірлеу.

8.2. Іс-шаралар жоспарлары университет басшылығымен келісіліп, заңнамадағы, технологиялардағы және бизнес-процестердегі өзгерістерді есепке алу үшін үнемі қайта қаралуы керек:

- Ақпараттық қауіпсіздіктің ағымдағы жай-күйін және іс-шаралар жоспарын іске асырудағы прогресті талқылау үшін басшылықпен тұрақты кездесулер өткізу.
- Аудит нәтижелері, заңнамалық талаптардың өзгеруі, жаңа технологиялардың пайда болуы және бизнес-процестердегі өзгерістер негізінде іс-шаралар жоспарларын қайта қарау.
- Қоршаған ортадағы жаңа қиындықтар мен өзгерістерге бейімделу үшін іс-шаралар жоспарларының икемділігін қамтамасыз ету.

9. СӘЙКЕСТЕНДІРУ

9.1. Ақпараттық қауіпсіздіктің осалдықтары мен қауіптерін сәйкестендіру тұрақты негізде жүргізілуі тиіс:

- Осалдықтар мен қауіптерді анықтау үшін тұрақты тексерулер кестесін анықтау.
- Ықтимал осалдықтар мен қауіптерді анықтау мақсатында Ақпараттық жүйелер мен желілердің тұрақты мониторингі үшін рәсімдерді енгізу.

- Жаңа осалдықтар мен қауіптерді анықтау үшін қолданылатын құралдар мен әдістерді уақтылы жаңартуды қамтамасыз ету.

9.2.Осалдықтарды талдау, енуді тестілеу, қауіпсіздік аудиті сияқты АҚ тәуекелдерін бағалау үшін құралдар мен әдістерді қолданыңыз:

- Желілік және бағдарламалық жасақтаманың осалдығын үнемі талдау үшін осалдықты сканерлеу жүйелерін енгізу.
- Ықтимал шабуылдардан қорғауды бағалау және осалдықтарды анықтау үшін тұрақты ену тестілеуін (PenetrationTesting) өткізу.
- Ағымдағы қорғау шараларын және олардың белгіленген стандарттар мен үздік тәжірибелерге сәйкестігін бағалауды қамтитын қауіпсіздік аудиттерін жүргізу.
- Ақпараттық қауіпсіздік тәуекелдерін жүйелі талдау және басқару үшін ISO/IEC 27005 сияқты тәуекелдерді бағалау әдістемелерін пайдалану.

9.3.Осалдықтар мен қауіптерді сәйкестендіру нәтижелері құжатталуы және анықталған проблемаларды жою бойынша шешімдер қабылдау үшін басшылыққа ұсынылуы тиіс:

- Анықталған проблемалардың сипаттамасын, олардың ықтимал салдарын және оларды жою жөніндегі ұсыныстарды қамтитын осалдықтар мен қауіптерді сәйкестендіру нәтижелері бойынша егжей-тегжейлі есептер жасау.
- Түзету және алдын алу шараларын іске асыру бойынша шешімдер қабылдау үшін басшылыққа есептер ұсыну.
- Жауапты тұлғаларды анықтауды және орындалу мерзімдерін белгілеуді қоса алғанда, анықталған осалдықтар мен қауіптерді жою жөніндегі іс-қимыл жоспарын әзірлеу.
- Анықталған жаңа осалдықтар мен қауіп-қатерлерге, сондай-ақ оларды жою бойынша қабылданған шараларға сәйкес құжаттама мен есептілікті үнемі жаңартып отыру.

10. АҚПАРАТТЫҢ ТҰТАСТЫҒЫ

10.1. Ақпараттың тұтастығын қамтамасыз ету мыналарды қамтиды:

10.1.1. Деректерді рұқсатсыз өзгертуден қорғау үшін әдістер мен құралдарды пайдалану:

- Деректерді тек уәкілетті пайдаланушылар өзгерте алатындығын қамтамасыз ету үшін кіруді басқару жүйелерін (Access Control) енгізу.
- Сандық қолтаңбалар мен бақылау сомалары (hashing) сияқты деректердің тұтастығын тексеру үшін криптографиялық әдістерді қолдану.
- Деректерді рұқсатсыз өзгертуден қорғау жүйелерін, соның ішінде өзгерістерді анықтау жүйелерін (Change Detection Systems) енгізу.

10.1.2. Маңызды деректер мен құжаттар үшін нұсқаны басқаруды енгізу:

- Құжаттар мен деректердегі өзгерістерді бақылау үшін нұсқаны басқару жүйелерін (Version Control Systems) пайдалану.
- Рұқсатсыз немесе қате өзгерістер анықталған жағдайда деректер мен құжаттардың алдыңғы нұсқаларына кері қайтару мүмкіндігін қамтамасыз ету.
- Өзгерістер тарихын сақтау және олардың аудит пен талдауға қолжетімділігін қамтамасыз ету.

10.1.3. Тұрақты аудиттер және деректердің тұтастығын тексеру:

- Ақпараттық жүйелер мен деректердің тұтастығына тұрақты аудитті жоспарлау және жүргізу.
- Деректердің тұтастығын тексеру және сәйкессіздіктерді анықтау үшін автоматтандырылған құралдарды пайдалану.

- Аудит және тексеру нәтижелерін құжаттау және анықталған проблемалар мен оларды жою бойынша қабылданған шаралар туралы басшылыққа хабарлау.

10.2. Жүйелер мен деректердегі барлық өзгерістер жазылып құжатталуы керек:

- Жүйелер мен деректердегі барлық өзгерістерді міндетті түрде тіркеуді қамтитын өзгерістерді (Change Management) тіркеу рәсімдерін енгізу.
- Өзгертулер журналдарын (Change Logs) құру және жүргізу, өзгертулердің күнін, уақытын, бастамашысын және енгізілген өзгерістердің сипаттамасын көрсету.
- Аудит және талдау үшін өзгерістер журналдарына қолжеткізуді қамтамасыз ету.

10.3. Қызметкерлердің қаскүнемдік әрекеттері мен қателіктерін қоса алғанда, ішкі және сыртқы қауіптерден қорғау жөніндегі шараларды енгізу:

- Ұйым ішіндегі күдікті әрекеттерді бақылау және анықтау процедураларын әзірлеу және енгізу.
- Маңызды жүйелер мен деректерге қолжеткізу кезінде қауіпсіздік деңгейін арттыру үшін екі факторлы аутентификация механизмдерін (2FA) енгізу.
- Қызметкерлерді ақпараттық қауіпсіздік қағидаттарына, соның ішінде деректермен қауіпсіз жұмыс істеу және инциденттерге ден қою ережелеріне үйрету.
- Ақпараттық жүйелердегі осалдықтарды анықтау және жою үшін ішкі және сыртқы ену тестілеуін (PenetrationTesting) жүйелі түрде өткізу.

11. АҚПАРАТТЫҢ ҚОЛЖЕТІМДІЛІГІ

11.1. Ақпараттың қолжетімділігін қамтамасыз ету мыналарды қамтиды:

11.1.1. Бизнес-процестердің үздіксіздігін қамтамасыз ету жөніндегі шараларды әзірлеу және енгізу:

- Маңызды бизнес-процестерді анықтау және олардың үздіксіздігін қамтамасыз ету жоспарларын әзірлеу.
- Күтпеген жағдайлар кезінде негізгі жүйелер мен сервистердің жұмысын қолдау үшін рәсімдерді енгізу.
- Бизнес-процестердің үздіксіздігін қамтамасыз ету бойынша жоспарларды үнемі тестілеу және жаңарту.

11.1.2. Деректердің сақтық көшірмесін жасау және қалпына келтіру жүйелерін енгізу:

- Деректердің сақтық көшірмесін жасау саясатын әзірлеу және енгізу, соның ішінде тұрақты сақтық көшірме жасау.
- Маңызды сақтық көшірме деректерін және олардың көшіру жиілігін анықтау.
- Апаттар кезінде деректердің жоғалуын болдырмау үшін резервтік көшірмелерді қорғалған және географиялық жағынан алыс жерлерде сақтау.
- Деректерді сақтық көшірмелерден қалпына келтіру процедураларын олардың жұмыс қабілеттілігі мен өзектілігін қамтамасыз ету үшін үнемі тексеріп отыру.

11.1.3. Маңызды жүйелердің ақауларға төзімділігін қамтамасыз ету:

- Кластерлік технологияларды пайдалануды және деректерді репликациялауды қоса алғанда, сыни жүйелердің жоғары қолжетімділігі мен ақауларға төзімділігін қамтамасыз ету үшін шараларды енгізу.
- Серверлердің, желілік құрылғылардың және басқа да инфрақұрылым компоненттерінің үздіксіз жұмысын қамтамасыз ету стратегиясын әзірлеу және іске асыру.

- Жоғары жүктеме жағдайында жүйелердің жұмысқа дайындығын тексеру үшін стресс-тестілерді жүйелі түрде жүргізу.

11.2. Тұрақты жаттығулар мен тестілеуді жоспарлау және жүргізу апаттар мен апаттарды қалпына келтіру жоспарлары:

- Ықтимал апаттар мен апаттардың сценарийлерін әзірлеу және оларды пысықтау бойынша тұрақты жаттығулар өткізу.
- Әр тестілеуден кейін қалпына келтіру жоспарларының тиімділігін бағалау және қажетті түзетулер енгізу.
- Қызметкерлерді жедел және дұрыс әрекет етуді қамтамасыз ету үшін апаттар мен апаттар жағдайында әрекет етуге үйрету.

11.3. Уәкілетті пайдаланушылар үшін қажетті уақытта және қажетті жерде ақпараттың қолжетімділігін қамтамасыз ету:

- Уәкілетті пайдаланушылар үшін ақпаратқа уақтылы қолжеткізуді қамтамасыз ететін қолжетімділікті бақылау және басқару жүйелерін енгізу.
- Инциденттер туындаған жағдайда ақпаратқа қолжеткізуді жылдам қалпына келтіру рәсімдерін әзірлеу.
- Пайдаланушыларға тәулік бойы қолдау көрсетуді және Ақпаратқа қолжеткізуге байланысты мәселелерді жедел шешуді қамтамасыз ету.

Ақпараттың қолжетімділігін қамтамасыз ету жөніндегі шаралардың мысалдары:

- Файлдар мен дерекқорлар үшін резервтік құралдарды пайдалану.
- Бірнеше деректер орталықтарында жүйелерді орналастыру.
- Жүйелер мен желілер үшін бақылау және ескерту құралдарын пайдалану.
- Жүйелер мен желілер үшін ақауларға төзімді компоненттерді пайдалану.
- Ақпараттың қолжетімділігін қамтамасыз ету бойынша ұсыныстар:
- Қолжетімділік тәуекелдерін бағалау. Ұйым ақпараттың қолжетімділігін бұзу тәуекелдерін бағалауы және осы тәуекелдерді азайту шараларын әзірлеуі керек.
- Қызметкерлерді оқыту. Ұйым қызметкерлері ақпараттың қолжетімділігінің маңыздылығы және оны қамтамасыз ету әдістері туралы хабардар болуы керек
- Тұрақты мониторинг және аудит. Ұйым ақпаратқа қолжетімділікті қамтамасыз ету шараларының тиімділігін үнемі қадағалап отыруы керек

Ақпараттың қолжетімділігіне байланысты оқиғалардың мысалдары:

- Жүйенің немесе желінің істен шығуы.
- Жүйелерді немесе желілерді жою немесе зақымдау.
- Кибер шабуыл.
- Ақпараттың қолжетімділігіне байланысты оқиғалардың әсері:
- Қаржылық шығындар.
- Беделін жоғалту.
- Заңнаманы бұзу

12. ТӘУЕКЕЛДЕРДІ БАСҚАРУ

Кесте 12.1 Жағымсыз оқиғаны талдау. «Ықтималдық» бағасы

Балл	Сипаттама
1	Екіталай (іс жүзінде мүмкін емес)

2	Едәуір ықтимал
3	Ықтимал
4	Өте ықтимал

Кесте 12.2 Жағымсыз оқиғаны талдау. «Күрделілік» бағасы

Балл	Сипатама
1	Өте төмен (жағымсыз оқиғаның салдары сыртқы тараптарға көрінбейді)
2	Орташа (тұтынушылардың қанағаттанбауының болмашы жағдайлары; салдарын жоюға шамалы шығындар; университет беделіне залалдың болмауы)
3	Жоғары (айыппұлдар, салдарды жою үшін айтарлықтай шығындар. Мүдделі тараптардың наразылығы)
4	Апатты (қызметті тоқтата тұру, беделін жоғалту)

Кесте 12.3 -Тәуекелдің қолайлылығы бойынша шкала

Күрделілік Ықтималдық	1	2	3	4
1	1	2	3	4
2	2	4	6	8
3	3	6	9	12
4	4	8	12	16

Кесте 12.4 – Тәуекелдерді басқару

№	Процесс	Тәуекел/ жағымсыз оқиға	Тәуекелдің қызметке әсерінсіз ипаттау/үрдіс	Тәуекелді бағалау			Тәуекелді төмендету бойынша шаралар (тәуекелді өлшеу)	Жауапты	Орындау мерзімдері
				Жағымсыз оқиғаның болу ықтималдығы / жиілігі (В)	Мамандығы / жағымсыз оқиғаның әлеуетті немесе нақты салдары (С)	Баға (В*С)			
1	Құпия ақпараттың жоғалуы	Құпия ақпараттың сыртқа шығуы беделге нұқсан келтіруі және қаржылық айыппұлға әкелуі мүмкін		3	4	12	Қол жеткізуді басқарудың қатаң жүйесін енгізу, қызметкерлерге ақпараттық қауіпсіздік бойынша оқыту	Ақпараттық қауіпсіздік бөлімінің басшысы	Токсан соңына дейін
2	Вирус шабуылдары	Вирус шабуылдары деректердің жоғалуына және жүйе өнімділігінің төмендеуіне әкелуі мүмкін		4	3	12	Антивирус бағдарламалық қамтамасыз етуді орнату, антивирус базаларын жүйелі түрде жаңарту және тексеру	IT-бөлімі	Токсан сайын
3	Деректердің тұтастығының бұзылуы	Деректердегі қателер ақпараттың бұрмалануына, шешім қабылдауға әсер етуі мүмкін		2	3	6	Деректердің тұрақты резервтік көшірмесін жасау және тұтастықты бақылауды орнату	Деректерге жауапты тұлға	Ай сайын
4	Сындарлы маңызды	Жүйелердің істен шығуы оқу және әкімшілік		3	4	12	Төтенше жағдай	IT-бөлімі	Жарты жылда

	жүйелердің қолжетімсіздігі	үдерістерге әсер етуі мүмкін					дайларжоспарын әзірлеу, резервтіккөшірмелер жасау және резервтік серверлерді орнату		
5	Ақпаратқа рұқсатсыз қол жеткізу	Бөгде адамдардың оқу деректеріне немесе студенттер мен қызметкерлердің жеке деректеріне қол жеткізу деректердің сыртқа шығуына әкелуі мүмкін		3	4	12	Көпфакторлы аутентификацияны орнату, құпия сөздерді жүйелі түрде жанарту және тіркелгілерді бақылау	Ақпараттық қауіпсіздік бөлімінің басшысы	Токсан сайын
6	Оқу порталдарына кибершабуылдар	Шабуылдар онлайн курстар мен материалдардың қолжетімсіздігіне, оқу үдерісінің үзілуіне әкелуі мүмкін		3	3	9	Желілік экрандарды (firewalls) пайдалану, желілік трафикті бақылау, SIEM жүйелерін енгізу	IT-бөлімі	Тұрақты
7	Техникалық ақаулардан деректердің жоғалуы	Құрылғылардың ақауы оқу және ғылыми-зерттеу деректерінің жоғалуына әкелуі мүмкін		3	4	12	Жүйелі резервтік көшірмелер жасау және апатты калпына келтіру жүйелерін қолдану	IT-бөлімі	Апта сайын
8	Қызметкерлердің ақпараттық қауіпсіздік бойынша төмен біліктілігі	Қызметкерлердің кәсіптіктері мен абайсыз әрекеттері деректердің кездейсоқ сыртқа шығуына немесе өзгеруіне әкелуі мүмкін		4	2	8	Қызметкерлерге ақпараттық қауіпсіздік бойынша тұрақты оқыту жүргізу және негіздерін тексеру	Кадрлар бөлімі	Жарты жылда
9	Бағдарламалық қамтамасыз етудің жанартылым ауы	Ескірген бағдарламалық қамтамасыз етуді пайдалану жүйелердің осалдығын арттыруы мүмкін		3	3	9	Барлық жүйелер мен қосымшаларды жүйелі түрде жанарту және патчтарды орнату	IT-бөлімі	Ай сайын
10	Адам факторының салдарынан жүйелердің жұмысында ақаулар	Қызметкерлердің дұрыс емес әрекеттері немесе қателері жүйелердің жұмысына әсер етуі мүмкін		2	3	6	Операцияларды көпсатылы тексеру рәсімін енгізу, белгілі тапсырмаларға қол жеткізу құжығын шектеу	Бөлім басшысы	Тұрақты

11. ҚОСЫМШАЛАР

А қосымшасы

11. ҚОСЫМШАЛАР

А қосымшасы

ТАНЫСУ ПАРАҒЫ (міндетті)

[illegible]

