БЕКІТЕМІН
«ОҚМА» АҚ ректоры
Ж. Сейтжанова
«___» _____ 2026 ж.

«ОҚМА» АҚ-ДА КОРПОРАТИВТІК СЕКТОРҒА АРНАЛҒАН КИБЕРГИГИЕНА ЕРЕЖЕСІ

П 508- 2026

Күні	Көшірме	Басылым
		Бірінші

г. Шымкент

Көшіруге және/немесе үшінші тұлғаға беруге тыйым салынады.

1. **«ОҚМА» АҚ** компьютерлік-тестілеу және баспа орталығы **ӘЗІРЛЕП, ҚОЛДАНЫСҚА ЕНГІЗІЛДІ**
хаттама №7 02.03. 2026 ж.

2. **«ОҚМА» АҚ** Сапа бойынша Кеңестің шешімімен **БЕКІТІЛДІ**
хаттама №4 26.03 2026 ж.

Кезеңді тексеру мерзімі – 3 жыл

Көшіруге және/немесе үшінші тұлғаға беруге тыйым салынады.

МАЗМҰНЫ

ҚҰЖАТ ПАСПОРТЫ..... 4
1. НОРМАТИВТІК ЖӘНЕ ҚҰҚЫҚТЫҚ НЕГІЗДЕР..... 5
2. БЕЛГІЛЕР МЕН ҚЫСҚАРТУЛАР..... 5
3. ТЕРМИНДЕР МЕН АНЫҚТАМАЛАР..... 5
4. ЖАЛПЫ ЕРЕЖЕЛЕР 6
5. КИБЕРГИГИЕНАҒА ҚОЙЫЛАТЫН НЕГІЗГІ ТАЛАПТАРЫ..... 8
6. ҚОЛЖЕТІМДІЛІКТІ БАСҚАРУ 9
7. КИБЕРИНЦИДЕНТТЕРГЕ ӘРЕКЕТ ЕТУ..... 9
8. ОҚЫТУ ЖӘНЕ ХАБАРДАРЛЫҚТЫ АРТТЫРУ 10
9. МОБИЛЬДІК ҚҰРЫЛҒЫЛАРДЫ ПАЙДАЛАНУ САЯСАТЫ (BYOD)..... 10
10. МЕССЕНДЖЕРЛЕРДІ ПАЙДАЛАНУ САЯСАТЫ..... 11
11. ЖАУАПКЕРШІЛІК..... 12

Көшіруге және/немесе үшінші тұлғаға беруге тыйым салынады.

ҚҰЖАТ ПАСПОРТЫ

Құжаттың атауы: «ОҚМА» АҚ-да корпоративтік секторға арналған кибергигиена ережесі

Қысқаша сипаттамасы: «ОҚМА» АҚ-да корпоративтік секторға арналған кибергигиена ережесі

Тақырып: Ақпараттық қауіпсіздік
Мәртебесі: Бірінші
Бекітілген күні: « ___ » _____20_____ж.
Қолдану мерзімінің аяқталу күні: « ___ » _____ 20_____ж.
Аудит күні: Жыл сайын

Көшіруге және/немесе үшінші тұлғаға беруге тыйым салынады.

1. НОРМАТИВТІК ЖӘНЕ ҚҰҚЫҚТЫҚ НЕГІЗДЕР

Осы Ереже келесі нормативтік құжаттардың талаптарын ескере отырып әзірленді:

— «Дербес деректер және оларды қорғаау туралы» Қазақстан Республикасының 2013 жылғы 21 мамыр № 94-V ҚРЗ Заңы;

— «Оңтүстік Қазақстан медицина академиясы» АҚ ақпараттық қауіпсіздік туралы 2026 жылғы П-504 ережесі;

— Қазақстан Республикасының «Қазақстан Республикасының ұлттық қауіпсіздігі туралы», «Мемлекеттік құпиялар туралы», «Терроризмге қарсы іс-қимыл туралы», «Электрондық құжат және электрондық цифрлық қолтаңба туралы», «Ақпараттандыру туралы», «Техникалық реттеу туралы», «Лицензиялау туралы», «Бұқаралық ақпарат құралдары туралы» заңдары;

— Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысымен бекітілген «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптар туралы» және ақпараттық қауіпсіздікті қамтамасыз ету мәселелерін реттейтін Қазақстан Республикасының және Университеттің өзге де нормативтік актілері.

2. БЕЛГІЛЕР МЕН ҚЫСҚАРТУЛАР

Осы Ережеде келесі белгілер мен қысқартулар пайдаланылды:

— «ОҚМА» АҚ – «Оңтүстік Қазақстан медицина академиясы» акционерлік қоғамы;

— АЖ – ақпараттық жүйелер;

— БҚ – бағдарламалық қамтамасыз ету;

— АҚ – ақпараттық қауіпсіздік.

3. ТЕРМИНДЕР МЕН АНЫҚТАМАЛАР

Осы Ережеде келесі терминдер тиісті анықтамаларымен қолданылады:

— кибергигиена — пайдаланушылардың ақпараттық ортада қауіпсіз мінез-құлық қағидаларының жиынтығы;

— ақпараттық қауіпсіздік — ақпараттың ішкі және сыртқы қауіптерден қорғалу жағдайы;

— киберинцидент — ақпараттық жүйелердің (бұдан әрі – АЖ) қауіпсіздігін бұзатын оқиға;

Көшіруге және/немесе үшінші тұлғаға беруге тыйым салынады.

— дербес деректер — белгілі бір жеке тұлғаға қатысты мәліметтер;

— кибершабуыл — АЖ-ға, желілерге немесе құрылғыларға олардың жұмысын бұзу, рұқсатсыз қол жеткізу, деректерді ұрлау, өзгерту немесе жою мақсатында жасалатын қасақана әсер ету;

— құпия ақпарат — қолжетімділігі шектеулі ақпарат;

— есептік деректер — пайдаланушының логині мен құпиясөзі;

— фишинг — алдау арқылы деректерді алу тәсілі;

— әлеуметтік инженерия — пайдаланушыға психологиялық әсер ету;

— кибербуллинг — цифрлық қудалау;

— цифрлық активтер — ұйымның ақпараттық ресурстары;

— ЭЦҚ — электрондық цифрлық қолтаңба;

— BYOD (Bring Your Own Device) — қызметтік мақсаттарда жеке құрылғыларды пайдалану.

4. ЖАЛПЫ ЕРЕЖЕЛЕР

Осы Ереже «Оңтүстік Қазақстан медицина академиясы» АҚ - да (бұдан әрі — «ОҚМА» АҚ) кибергигиенаны қамтамасыз ету бойынша бірыңғай талаптарды айқындайды.

Ереже «ОҚМА» АҚ-тың ақпараттық ресурстарын қорғауға, киберқауіптерді азайтуға және деректердің таралуының алдын алуға бағытталған. Осы Ереженің талаптары «ОҚМА» АҚ-тың Ақпараттық жүйеге (бұдан әрі — «ОҚМА» АЖ) қол жеткізе алатын барлық қызметкерлерге, білім алушыларға және өзге де тұлғаларға міндетті болып табылады.

Осы Ереже ресми бекітілген сәттен бастап күшіне енеді және «ОҚМА» АҚ-тың барлық қызметкерлері, білім алушылары және АЖ-ні пайдаланушылары үшін міндетті түрде орындалуға тиіс.

Осы Ережені қайта қарау және өзектендіру жылына кемінде бір рет, сондай-ақ Қазақстан Республикасының заңнамасына, ішкі нормативтік құжаттарға өзгерістер енгізілген жағдайда немесе «ОҚМА» АҚ-тың талаптары өзгерген кезде жүзеге асырылады.

Осы Ереженің талаптарының сақталуын және орындалуын бақылау «ОҚМА» АҚ-тың киберқауіпсіздік және АЖ жөніндегі маманына жүктеледі, ол белгіленген нормалардың орындалуын мониторингтеу, үйлестіру және бақылауды жүзеге асырады.

Мақсаттары мен міндеттері.

Негізгі мақсат – «ОҚМА» АҚ ақпараттық ресурстарын ішкі және сыртқы қауіптерден кешенді қорғауды қамтамасыз ету, кибертәуекелдер деңгейін төмендету, деректердің таралуының алдын алу және АЖ үздіксіз жұмыс істеуін қамтамасыз ету, сондай-ақ қызметкерлер мен білім алушылар

Көшіруге және/немесе үшінші тұлғаға беруге тыйым салынады.

арасында АҚ мәдениетін қалыптастыру.

Қойылған мақсатқа қол жеткізу үшін келесі міндеттерді шешу қажет:

— «ОҚМА» АҚ ақпараттық ресурстарын рұқсатсыз қол жеткізуден, деректердің таралуынан, жойылуынан және бұрмалануынан қорғауды қоса алғанда, ішкі және сыртқы қауіптерден кешенді қорғауды қамтамасыз ету;

— кибершабуылдардың алдын алу және олардың салдарын барынша азайтуға бағытталған ұйымдастырушылық және техникалық АҚ шараларын енгізу арқылы кибертәуекелдер деңгейін төмендету;

— ақпаратты қорғауға саналы және жауапты көзқарасқа негізделген қызметкерлер мен білім алушылар арасында тұрақты АҚ мәдениетін қалыптастыру;

— «ОҚМА» АҚ ақпараттық жүйелері мен сервистерінің үздіксіз жұмыс істеуін қамтамасыз ету;

— Қазақстан Республикасының заңнамасы мен ішкі нормативтік құжаттардың талаптарына сәйкес дербес деректерді, қызметтік және өзге де құпия ақпаратты қорғау;

— қызметкерлер мен білім алушылар тарапынан «ОҚМА» АҚ цифрлық инфрақұрылымына деген сенім деңгейін арттыру;

— ақпараттық жүйелермен қауіпсіз жұмыс істеу регламенттерін, нұсқаулықтарын және стандарттарын қамтитын тиімді кибергигиена жүйесін енгізу және қолдау;

— АҚ және кибергигиена мәселелері бойынша қызметкерлер мен білім алушыларды тұрақты оқыту, нұсқама жүргізу және хабардарлығын арттыру;

— киберинциденттердің алдын алуға бағытталған профилактикалық іс-шараларды ұйымдастыру және өткізу (фишинг-симуляциялар, пайдаланушылардың білімін тестілеу);

— «ОҚМА» АҚ ақпараттық жүйелері мен процестеріндегі ықтимал осалдықтарды анықтау, талдау және азайту;

— корпоративтік және жеке құрылғыларды (BYOD саясаты аясында) пайдалану кезінде АҚ талаптарының сақталуын қамтамасыз ету;

— пайдаланушылардың кибергигиена талаптарын сақтауын бақылау және бұзушылықтар анықталған жағдайда тиісті әрекет ету шараларын қолдану;

— киберинциденттерге жедел әрекет ету процесін ұйымдастыру (уақтылы анықтау, оқшаулау және салдарын жою);

— «ОҚМА» АҚ цифрлық активтерін (деректер базалары, АЖ, желілік инфрақұрылым) қорғауды қамтамасыз ету;

— киберқауіпсіздік мәселелері бойынша «ОҚМА» АҚ құрылымдық бөлімшелері арасында өзара іс-қимылды қамтамасыз ету.

Көшіруге және/немесе үшінші тұлғаға беруге тыйым салынады.

5. КИБЕРГИГИЕНАҒА ҚОЙЫЛАТЫН НЕГІЗГІ ТАЛАПТАРЫ

Кибергигиенаға қойылатын негізгі талаптар «ОҚМА» АҚ-да ақпараттық жүйелері мен цифрлық ресурстарымен жұмыс істеу кезінде пайдаланушылардың қауіпсіз мінез-құлқының міндетті ережелерін белгілейді. Бұл талаптар рұқсатсыз қол жеткізудің, деректердің сыртқа шығуының және өзге де киберинциденттердің алдын алуға бағытталған. Аталған талаптар есептік деректерді басқару саясатын сақтауды, тек рұқсат етілген бағдарламалық қамтамасыз ету мен құрылғыларды пайдалануды, электрондық коммуникацияларға мұқият қарауды, сондай-ақ ақпаратты қорғау бойынша белгіленген шараларды қатаң орындауды және кез келген күдікті әрекеттер немесе қауіптер туралы уақтылы хабарлауды қамтиды.

Пайдаланушылар міндетті:

- әрбір ақпараттық жүйе үшін күрделі және бірегей құпиясөздерді пайдалану, олар белгіленген ең төменгі таңбалар санынан кем болмауы тиіс және рұқсатсыз қол жеткізудің алдын алу мақсатында әріптер, сандар және арнайы таңбалардың комбинациясынан тұруы қажет;
- құпиясөздерді кемінде 90 күнтізбелік күнде бір рет тұрақты түрде ауыстыру, сондай-ақ оның бұзылуына (компрометациясына) күдік туындаған жағдайда дереу өзгерту;
- есептік деректердің (логиндер, құпиясөздер, растау кодтары) құпиялылығын қамтамасыз ету, оларды үшінші тұлғаларға бермеу, ашық түрде жазбау және қауіпсіз емес орындарда сақтамау;
- пайдаланушы уақытша болмаған әрбір жағдайда жұмыс станцияларын, ноутбуктерді және өзге де құрылғыларды бұғаттау, оның ішінде экранды автоматты түрде бұғаттау функциясын пайдалану;
- қызметтік қызметте тек белгіленген тәртіппен бекітілген рұқсат етілген және лицензияланған бағдарламалық қамтамасыз етуді пайдалану;
- электрондық поштамен, интернет-ресурстармен және корпоративтік жүйелермен жұмыс істеу кезінде ақпараттық қауіпсіздік талаптарын сақтау;
- жұмыс құрылғыларында орнатылған антивирустық бағдарламалық қамтамасыз етуді және өзге де ақпаратты қорғау құралдарын пайдалану, оларды рұқсатсыз өшірмеу;
- кез келген күдікті әрекеттер, хабарламалар, қол жеткізу әрекеттері немесе ықтимал киберинциденттер туралы киберқауіпсіздік және ақпараттық жүйелерді қорғау жөніндегі маманды дереу хабардар ету.

Пайдаланушыларға тыйым салынады:

- белгісіз немесе күмәнді дереккөздерден келген электрондық хаттарды, тіркемелерді ашуға және сілтемелерге өтуге, сондай-ақ тексерілмеген жіберушілерден алынған файлдарды іске қосуға;

- лицензияланбаған, рұқсат етілмеген немесе зиянды бағдарламалық қамтамасыз етуді орнатуға, жүктеуге немесе пайдалануға, сондай-ақ киберқауіпсіздік және ақпараттық жүйелерді қорғау жөніндегі маманмен келісілмеген бағдарламалық қамтылымды қолдануға;

- жұмыс құрылғыларына белгісіз немесе рұқсат етілмеген сыртқы ақпарат тасымалдағыштарын (USB-жинақтағыштар, қатты дискілер және т.б.) қосуға, сондай-ақ жеке құрылғыларды рұқсатсыз пайдалануға;

- ақпараттық қауіпсіздіктің белгіленген құралдарын, соның ішінде аутентификация жүйелерін, антивирустық қорғауды, желілік экрандарды және өзге де қауіпсіздік құралдарын айналып өтуге әрекет жасауға;

- қызметтік, құпия немесе дербес ақпаратты қорғалмаған байланыс арналары немесе үшінші тарап сервистері арқылы тиісті рұқсатсыз беруге;

- ақпараттық қауіпсіздікке қауіп төндіруі немесе «ОҚМА» АҚ-ның саясатын бұзуы мүмкін жағдайларда корпоративтік ақпараттық ресурстарды жеке мақсатта пайдалануға;

- жауапты бөлімшелермен келісімсіз құрылғылар мен бағдарламалық қамтамасыз етудің қауіпсіздік баптауларын өз бетінше өзгертуге.

6. ҚОЛЖЕТІМДІЛІКТІ БАСҚАРУ

«ОҚМА» АҚ АЖ қолжетімділік ең аз қажетті артықшылықтар қағидаты негізінде беріледі, яғни пайдаланушыға тек өзінің лауазымдық міндеттерін орындауға қажетті құқықтар мен қолжетімділік деңгейлері ғана ұсынылады.

Әрбір пайдаланушыға міндетті түрде жеке есептік жазба тағайындалады, бұл қолжетімділікті дербестендіруді және жүйедегі әрекеттерді сәйкестендіру мүмкіндігін қамтамасыз етеді.

АЖ-дағы пайдаланушылардың барлық әрекеттері оқиғалар журналдарында міндетті түрде тіркелуге тиіс, бұл олардың кейінгі талдауын, бақылауын, күмәнді белсенділікті анықтауды және инциденттер туындаған жағдайда терең талдау жүргізуді қамтамасыз етеді.

Берілген қолжетімділік құқықтары тұрақты түрде қайта қаралуға жатады, сондай-ақ қызметкер жұмыстан босатылғанда, басқа лауазымға ауысқанда немесе оның функционалдық міндеттері өзгерген жағдайда уақтылы және міндетті түрде кері қайтарылады, бұл ақпараттық ресурстарды рұқсатсыз пайдаланудың алдын алуға бағытталған.

7. КИБЕРИНЦИДЕНТТЕРГЕ ӘРЕКЕТ ЕТУ

Киберинциденттерге әрекет ету талаптары пайдаланушылардың кез келген күмәнді оқиғалар туралы уақтылы хабарлау міндетін және олар

Көшіруге және/немесе үшінші тұлғаға беруге тыйым салынады.

анықталған кезде белгіленген іс-қимыл тәртібін қатаң сақтауын көздейді. Пайдаланушыларға инциденттерді өз бетінше жоюға бағытталған әрекеттерді орындауға тыйым салынады, өйткені бұл ақпараттың бұрмалануына, дәлелдердің жоғалуына және тергеп-тексеруді қиындатуға әкелуі мүмкін.

Пайдаланушылар ақпараттық қауіпсіздік (АҚ) талаптарының ықтимал бұзылуына байланысты кез келген күмәнді оқиға туралы, соның ішінде күмәнді хаттарды алу, белгісіз бағдарламаларды анықтау, рұқсатсыз қол жеткізу әрекеттері, құрылғыны жоғалту немесе киберинциденттің өзге де белгілері туралы, оны анықтаған сәттен бастап 15 минуттан кешіктірмей дереу хабарлауға міндетті. Хабарлама киберқауіпсіздік және ақпараттық жүйелер (АЖ) жөніндегі маманға немесе жауапты бөлімшеге жіберілуі тиіс, онда оқиғаның сипаты, анықталған уақыты және қабылданған шаралар (бар болған жағдайда) туралы барынша толық және нақты ақпарат ұсынылуы қажет.

Киберинцидентті өз бетінше жоюға бағытталған әрекеттерге, соның ішінде файлдарды жоюға, жабдықты ажыратуға, жүйе баптауларын өзгертуге немесе үшінші тарап бағдарламаларын іске қосуға қатаң тыйым салынады. Мұндай әрекеттер тек ішкі регламенттерде тікелей көзделген немесе киберқауіпсіздік және АЖ жөніндегі маманның тиісті нұсқаулары болған жағдайда ғана жүзеге асырылуы мүмкін. Бұл талап инцидент салдарының ушығуын болдырмауға және тергеп-тексеруді дұрыс жүргізуді қамтамасыз етуге бағытталған.

8. ОҚЫТУ ЖӘНЕ ХАБАРДАРЛЫҚ

«ОҚМА» АҚ-тың барлық қызметкерлері мен білім алушылары цифрлық ортада қауіпсіз мінез-құлық дағдыларын қалыптастыруға, сондай-ақ кибертәуекелдер деңгейін төмендетуге бағытталған кибергигиена және ақпараттық қауіпсіздік мәселелері бойынша жыл сайын міндетті оқытудан өтеді. Оқыту әртүрлі форматтарда жүргізілуі мүмкін: дәстүрлі (офлайн) сабақтар, қашықтан оқыту курстары, сондай-ақ мамандандырылған білім беру платформаларын пайдалану арқылы өзіндік оқу. Соның ішінде киберқауіпсіздік саласындағы қазақстандық мамандар әзірлеген citizensec.kz кибергигиена және киберқауіпсіздік порталы да қолданылады.

Хабардарлықты арттыру жүйесі шеңберінде пайдаланушылардың білім деңгейін бағалау, білімдегі олқылықтарды анықтау және оларды жою мақсатында тұрақты түрде тестілеу жүргізіледі. Тестілеу нәтижелері оқыту бағдарламаларын жетілдіру және «ОҚМА» АҚ-та ақпараттық қауіпсіздік мәдениетінің жалпы деңгейін арттыру үшін пайдаланылады.

Көшіруге және/немесе үшінші тұлғаға беруге тыйым салынады.

9. МОБИЛЬДІ ҚҰРЫЛҒЫЛАРДЫ ПАЙДАЛАНУ САЯСАТЫ (BYOD)

Жеке мобильді құрылғыларды пайдалану саясаты (BYOD — Bring Your Own Device) «ОҚМА» АҚ ақпараттық ресурстарына қол жеткізу кезінде қызметкерлер мен білім алушылардың жеке мобильді құрылғыларын пайдалану, рұқсат беру және қорғау тәртібін айқындайды.

Аталған саясат жеке смартфондар, ноутбуктер және басқа да құрылғыларды пайдалану кезінде корпоративтік деректердің қауіпсіздігін қамтамасыз етуге, сондай-ақ ақпараттың таралуы, рұқсатсыз қол жеткізу және киберқауіптер тәуекелдерін азайтуға бағытталған. Жеке құрылғыларды пайдалану тек ақпараттық қауіпсіздік (АҚ) талаптары сақталған жағдайда, негізгі қорғаныс құралдары (құпиясөз, биометриялық аутентификация, антивирустық бағдарламалық қамтамасыз ету) болғанда және корпоративтік жүйелерге тек қорғалған байланыс арналары арқылы қосылу қағидалары орындалғанда ғана рұқсат етіледі.

Осы саясат шеңберінде пайдаланушылар келесі талаптарды сақтауға міндетті:

— тек қорғалған мобильді құрылғыларды пайдалануға рұқсат етіледі;

— құпиясөздің немесе биометриялық қорғаныстың болуы міндетті;

— root-қолжетімділігі немесе jailbreak қолданылған құрылғыларды пайдалануға тыйым салынады;

— корпоративтік ресурстарға қол жеткізу тек қорғалған байланыс арналары арқылы жүзеге асырылады;

— құрылғы жоғалған жағдайда пайдаланушы дереу киберқауіпсіздік және ақпараттық жүйелер жөніндегі маманға хабарлауға міндетті;

— «ОҚМА» АҚ корпоративтік деректерге қолжетімділікті шектеуге немесе оларды қашықтан жоюға (MDM) құқылы.

10.МЕССЕНДЖЕРЛЕРДІ ПАЙДАЛАНУ САЯСАТЫ

Мессенджерлерді пайдалану саясаты «ОҚМА» АҚ-тың қызметтік қызметінде жедел хабар алмасу құралдарын қауіпсіз және бақыланатын қолдану қағидаларын айқындайды.

Аталған саясат құпия ақпаратты қорғауды қамтамасыз етуге, деректердің таралуының алдын алуға және қызметкерлер мен білім алушылар арасындағы цифрлық коммуникация кезінде киберқауіптер тәуекелдерін төмендетуге бағытталған.

Рұқсат етіледі:

Көшіруге және/немесе үшінші тұлғаға беруге тыйым салынады.

— қызметтік коммуникация үшін ресми корпоративтік чаттарды пайдалану.

Тыйым салынады:

— құпия ақпаратты беру;

— қызметтік құжаттарды жеке аккаунттарға жіберу;

— күмәнді сілтемелерге өту.

Қауіпсіздік талаптары:

— екі факторлы аутентификацияны (2FA) пайдалану;

— хабарлама жіберушілерді тексеру;

— тек бекітілген корпоративтік платформаларды пайдалану.

11. ЖАУАПКЕРШІЛІК

Осы Ереженің талаптарын бұзған жағдайда, «ОҚМА» АҚ-да ақпараттық жүйелерінің қызметкерлері, білім алушылары және өзге де пайдаланушылары Қазақстан Республикасының қолданыстағы заңнамасына және ішкі нормативтік құжаттарға сәйкес белгіленген жауапкершілікке тартылады. Жасалған бұзушылықтың сипатына, ауырлық дәрежесіне және оның салдарына байланысты бұзылған тәртіпті қалпына келтіруге және қайталанатын инциденттердің алдын алуға бағытталған әртүрлі ықпал ету шаралары қолданылуы мүмкін.

Ең алдымен тәртіптік жауапкершілік қолданылуы мүмкін, оған ескерту, сөгіс, қатаң сөгіс немесе «ОҚМА» АҚ-ның еңбек заңнамасына және ішкі қағидаларына сәйкес өзге де тәртіптік жаза шаралары кіреді. Заңнамада көзделген жағдайларда ақпараттық қауіпсіздік талаптарын бұзу әкімшілік жауапкершілікке әкелуі мүмкін, оның ішінде Қазақстан Республикасының нормативтік құқықтық актілерінде қарастырылған айыппұл санкциялары қолданылады. Пайдаланушының заңсыз әрекеттері салдарынан «ОҚМА» АҚ-ға материалдық залал келтірілген жағдайда, заңнамада белгіленген тәртіпке сәйкес материалдық жауапкершілік туындауы мүмкін және келтірілген залал жағдайдың мән-жайына байланысты толық немесе ішінара өтеледі.

Көшіруге және/немесе үшінші тұлғаға беруге тыйым салынады.

Әзірлеген:

Лауазымы	Аты-жөні	Күні	Қолы
Киберқауіпсіздік және ақпараттық жүйені қорғау маманы	Арынбаев С.А.	02.03.2026 ж.	

Тексерген:

Лауазымы	Аты-жөні	Күні	Қолы
Компьютерлік-тестілеу және баспа орталығының басшысы	Уксикбаев М.Т.	02.03.2026 г.	
Сапаны қамтамасыз ету және мониторинг бөлімінің меңгерушісі	Ержанов Н.Ә.	05.03.2026 г.	
Әкімшілік және құқықтық қамтамасыз ету басқармасының басшысы	Кабиштаев О.А.	12.03.2026 г.	

Келісілген:

Лауазымы	Аты-жөні	Күні	Қолы
Академиялық жұмыстар жөніндегі проректор	Анартаева М.У.	17.03.2026 г.	
Клиникалық жұмыстар жөніндегі проректор	Нурмашев Б.Қ.	17.03.2026 г	
Ғылыми және стратегиялық даму жөніндегі проректор	Аукенов Н.Е.	18.03.2026 г	
Тәрбие жұмыстары және әлеуметтік мәселелер жөніндегі проректор	Сәлім Е.Қ.	18.03.2026 г.	
Комплаенс офицер	Пернебаев Н.А.	18.03.2026 г.	

Көшіруге және/немесе үшінші тұлғаға беруге тыйым салынады.