Бекітілді
Бас дәрігердің бұйрығымен
Жамбыл облысы әкімдігінің
денсалық сақтау басқармасы
«Жамбыл облыстық ЖИТС-тің
алдын алу және онымен
күрес жүргізу
орталығы»
_____ Б.Д.Кыдырбаев
№_____ «____»_____2025 ж.

Сапа менеджменті жүйесі
«Құжатталған процедура»
«Ақпараттық қауіпсіздік саясаты»»

Тараз қ
2025 ж.

	Мазмұны	беті.
1	Жалпы ережелер	3
2	Қолдану саласы	3
3	Терминдер, анықтамалар және қысқартулар	3
4	Құжаттарға сілтемелер	4
5	Жауапкершілік	4
6	Ақпараттық қауіпсіздік саясатының мақсаты мен міндеттері	5
7	Ақпаратты қорғау бойынша нұсқаулық	5
8	Құпия сөздерді қорғау ережелері	6
9	Антивирустық қорғаныс ұйымдастыру бойынша нұсқаулық	6
10	Жұмыс станцияларында электрондық поштаны және Интернет қызметтерін пайдалану нұсқаулығы	7
11	Қызметкерлердің төтенше жағдайлардағы әрекеттері жөніндегі регламент	8
12	Резервтік көшіру, резервтік файлдарды сақтау және төтенше жағдайларда деректерді қалпына келтіру ережелері	9
13	Компьютерлік жабдықты техникалық қызмет көрсету ережелері	10
14	Компьютерлік жабдық пен бағдарламалық қамтамасыз етуді пайдалану бойынша пайдаланушы нұсқаулығы	10
15	Жеке компьютермен жұмыс істеу кезінде қауіпсіздік техникасы	11
16	Қосымша	12

1. Жалпы ережелер

1.1. Осы ақпараттық қауіпсіздік саясаты (әрі қарай – «Саясат») «Жамбыл облысы әкімдігінің денсаулық сақтау басқармасы қарасты Коммуналдық мемлекеттік мекеме «Жамбыл облыстық ЖИТС-ты алдын алу және күрес орталығы» (әрі қарай – Жамбыл ОЦ ЖИТС)» әзірленген және Қазақстан Республикасының қолданыстағы заңнамасына және нормативтік-құқықтық актілеріне сәйкес жасалған.

1.2. Осы ақпараттық қауіпсіздік саясаты (әрі қарай – Саясат) ақпаратты, соның ішінде конфиденциалды деректерді және ақпараттық процестерді қорғауға бағытталған алдын алу шараларының кешенін анықтайды.

1.3. Осы Саясат ақпараттық қауіпсіздік жүйесінің қазіргі жағдайын, жақын арадағы даму перспективаларын, мақсаттары мен міндеттерін, пайдалануды, жұмыс режимдерін, сондай-ақ ақпараттандыру нысандары үшін қауіп-қатерлерді талдауды ескереді.

2. Қолдану саласы

Осы Саясат қызметкерлерге қолданылады және сапа менеджменті жүйесінің (СМЖ) құжаттар жинағына кіреді.

3. Терминдер, анықтамалар және қысқартулар

(Бұл бөлімде ақпараттық қауіпсіздік саласында қолданылатын негізгі терминдер, олардың анықтамалары және қысқартулар көрсетіледі.)

3.1 Терминдер

Ақпараттық қауіпсіздік	Ақпараттық ресурстарды, ақпараттық жүйелерді, ақпараттық-телекоммуникациялық инфрақұрылымды рұқсатсыз қол жеткізуден және пайдаланудан қорғау процесі
Ақпараттық жүйе	Ақпаратты сақтау, өңдеу, іздеу, тарату, беру және ұсыну үшін аппараттық-құрылымдық кешенді қолданатын жүйе
Рұқсат етілмеген қол жеткізу	Қорғалатын ақпаратқа мүдделі субъектінің оны құқықтық құжаттар немесе ақпарат иесі, меншік иесі белгілеген құқықтар мен қол жеткізу ережелерін бұзу арқылы алу әрекеті

3.2 Қысқартулар мен белгілеулер

АРМ	Автоматтандырылған жұмыс орны
ВС	Есептеу жүйесі
ИБ	Ақпараттық қауіпсіздік
ИС	Ақпараттық жүйе
ЛИС	Зертханалық ақпараттық жүйе LIS K-Lab
МЗ РК	Қазақстан Республикасының Денсаулық сақтау министрлігі

ОИКН	АИТЫ-инфекциясын ақпараттандыру және компьютерлік бақылау бөлімі
ЗОИКН	АИТВ-инфекциясын ақпараттандыру және компьютерлік бақылау бөлімінің меңгерушісі
ПК	Жеке компьютер
ПО	Бағдарламалық қамтамасыз ету
Система электронного слежения за случаями АИТВ- инфекции	АИТВ- инфекциясын электрондық бақылау
ОТ	Ұйымдастыру техника

4 Құжаттарға сілтемелер

СТ РК ISO 15189-2015	«Медициналық зертханалар. Сапа мен құзыреттілік талаптары»
ҚР 2009 жылғы 18 қыркүйектегі № 193-IV Кодексі	«Халық денсаулығы және денсаулық сақтау жүйесі туралы»
ҚР 2015 жылғы 24 қарашадағы № 418-V Заңы	«Ақпараттандыру туралы»
ҚР 2013 жылғы 21 мамырдағы № 94-V Заңы	«Жеке деректер және оларды қорғау туралы»
ҚР Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 Қаулысы	Ақпараттық-коммуникациялық технологиялар саласындағы біртұтас талаптар және ақпараттық қауіпсіздікті қамтамасыз ету

5 Жауапкершілік

5.1. Осы Саясатты бекітуге жауапкершілік бас дәрігерге жүктеледі.
5.2. Осы Саясатта көрсетілген процестерді енгізу және басқаруға жауапкершілік ВИЧ инфекциясына қатысты ақпараттандыру және компьютерлік бақылау бөлімінің меңгерушісіне (әрі қарай – РОИКН) жүктеледі.
5.3. Осы Саясатты әзірлеуге жауапкершілік ЗОИКН-ге жүктеледі.
5.4. Барлық қызметкерлер осы Саясаттың талаптарына сүйенеді

6 Ақпараттық қауіпсіздік саясатының мақсаты мен міндеттері

6.1. Осы Саясаттың барлық ережелерінің негізгі мақсаты – ақпараттық қауіпсіздікті сенімді қамтамасыз ету, нәтижесінде ақпараттық қызметтің салдарынан материалдық, физикалық немесе басқа да зиянның алдын алу.

6.2. Белгіленген мақсаттарға жету үшін келесі міндеттер орындалады:

Есептеу жүйесінің (ЕС) жұмысында сыртқы тұлғалардың араласуын болдырмау;

Ақпаратқа, сондай-ақ аппараттық, бағдарламалық-аппараттық және бағдарламалық құралдарға тіркелген пайдаланушылардың қолжетімділігін шектеу;

Бағдарламалардың орындау ортасының тұтастығын бақылау (өзгеріссіздігін қамтамасыз ету) және бұзылған жағдайда қалпына келтіру;

Жүйені зиянды кодтардың, оның ішінде компьютерлік вирустардың енуінен қорғау;

Қызметтік ақпарат пен жеке деректерді өңдеу, сақтау және байланыс арналары арқылы беру кезінде ағуынан, рұқсат етілмеген жариялануданнемесе бұрмалаудан қорғау;

Ақпарат алмасуға қатысатын пайдаланушылардың аутентификациясын қамтамасыз ету;

Ақпараттық қауіпсіздік қауіптерін, зиян келтіру мүмкіндігі мен себептерін уақтылы анықтау;

Ақпараттық қауіпсіздік қауіптері мен жағымсыз тенденцияларға жедел әрекет ету механизмін құру;

Физикалық және заңды тұлғалардың заңсыз әрекеттерінен келтірілген зиянды азайту және локализациялау, теріс әсерді төмендету және ақпарат қауіпсіздігі бұзылуының салдарын жою.

6.3. Ақпараттық қауіпсіздік саласындағы нормативтік құжаттар жинағына келесі құжаттар енгізіледі:

Толық саясаттың атауы	**Іске асу жиілігі**	**Жауаптылар**		
		Барлығы	**ОИКН**	**Қаржылық бухгалтер**
Пайдаланушылардың өтініш журналын жүргізу	Өтініштер бойынша	+	+	
Төтенше жағдайларды тіркеу журналы	Төтенше жағдайлар анықталған кезде		+	
Бағдарламалық-аппараттық құралдар мен ақпараттық жүйелерді жүйелік-техникалық қызмет көрсету регламенті	Қажет болған жағдайда		+	

7. Ақпаратты қорғау нұсқаулығы

Ақпараттық қауіпсіздікті, соның ішінде коммуникациялық құралдарды рұқсатсыз қол жеткізуден қорғау мақсатында келесі шаралар қарастырылған:

Өндірістік мақсаттар үшін негізгі кешенге кірмейтін қолданбалы бағдарламалық қамтамасыз етуді пайдалану;

Қызметкерлерге Қазақстан Республикасының ақпараттық қауіпсіздік саласындағы заңнамалық нормалары бойынша нұсқаулықтан және қосымша оқытудан өтуін қамтамасыз ету, соның ішінде жаңа жұмысқа келген қызметкерлерге;

Тауарлар, жұмыстар және қызметтер жеткізушілерімен жасалған келісімшарттарда берілген мәліметтердің құпиялылығын сақтау міндетін бекіту;

Ғимараттар мен құрылымдарды сенімді қорғау жүйесін құру (бейнебақылау), қауіпсіздік инженері бекітіледі.

Пайдаланушылардың ЭЕМ-ын рұқсатсыз қол жеткізуден қорғау бағыттары:

Пайдаланушыларды тіркеу құралдарын құру;

Лицензияланған антивирус бағдарламалық қамтамасыз етуді пайдалану, антивирус бағдарламаларын үнемі жаңарту. Антивирус бағдарламалары жұмыс станцияларын, орталық серверлерін және ақпарат тасымалдағыштарын зиянды кодтар үшін тексеру үшін қолданылады;

Бағдарламалық өнімдер мен аппараттық құралдарды пайдалану алдында олардың жұмыс қабілеттілігін тексеру. Пайдалануға жарамсыз бағдарламалық және аппараттық құралдар қабылданбайды;

Төтенше жағдайларда (өрт, су тасқыны, жер сілкінісі) және басқа да төтенше жағдайларда қолданылатын қорғау құралдарын енгізуге байланысты шараларды қабылдау. Төтенше жағдайларды бақылау журналға жазу арқылы жүзеге асырылады.

8. Пароль арқылы қорғау ережелері

8.1. Осы ережелер персонал компьютерлері мен ақпараттық жүйе әкімшілерінің жеке парольдерді пайдалану, ауыстыру және тоқтату, есептік жазбаларды жою процестерінің ұйымдастырушылық-техникалық қамтамасыз етілуін реттейді.

Жеке парольді қалыптастыру ережелері

8.2. Жеке парольдерді пайдаланушылар мен жүйе әкімшілері мына талаптарды ескере отырып таңдайды:

Пароль оңай болжанатын символдар комбинациясын қамтымауы керек (аты-жөні, туған күні, автокөлік нөмірлері, телефондар және басқа мәліметтер), сондай-ақ стандартты пернетақта орналасуы (zyxwvuts, 123, 123321, qwerty). Ұсынылады: кездейсоқ таңдалған символдардан тұратын парольдер. Бұрын қолданылған парольдер алты ай ішінде қайта пайдаланылмайды;

Жеке парольді жариялауға болмайды. Қызметтік құпияға қатысты парольді жариялағаны үшін қызметкерге тәртіптік жауапкершілік қолданылады.

Парольді енгізу

8.3. Парольді енгізу регистрді және пернетақта орналасуын ескере отырып жүзеге асырылады.

8.4. Парольді енгізу кезінде оны үшінші тұлғалардың тануы немесе техникалық құралдар арқылы ашылуы мүмкіндігі болдырылмайды. Пароль автоматтандырылған тіркеу процесіне енгізілмейді.

Парольді сақтау

8.5. Қызметкерлер парольді сақтау кезінде келесі талаптарды сақтайды:

Жеке пароль, сондай-ақ басқа ақпараттық ресурстарға, оның ішінде интернет-ресурстарға арналған парольдер жарияланбайды;

Корпоративтік желідегі, интернет-ресурстардағы, ашық халықаралық интернет-ресурстардағы, пошта және басқа ақпараттық жүйелердегі логиндер мен парольдерді пайдалану рұқсат етілмейді.

8.6. Жұмыстан шыққан пайдаланушылардың ЕС-ке қолжетімділігін ОИКН тоқтатады. Кадр бөлімі қызметкердің жұмыстан шығуы туралы ОИКН-ға кемінде 3 жұмыс күні бұрын хабарлайды.

9. Антивирус қорғауды ұйымдастыру нұсқаулығы

9.1. Антивирус бағдарламалары корпоративтік есептеу желісіндегі барлық персоналды компьютерлер мен серверлерге ОИКН мамандары арқылы орнатылады.

9.2. Антивирус құралдарын баптау келесі талаптарды қамтамасыз етуі керек:

Компьютерді әр қайта жүктегенде (серверлер үшін – қайта іске қосқанда) антивирус мониторы автоматты түрде іске қосылуы;

Белгілі бір уақытта локалдық дискілерді толық антивирус тексеруі (сканерлеу);

Антивирус базаларын күнделікті белгілі уақытта жаңарту;

Зиянды файлдарды емдеу немесе емдеуге болмайтын жағдайда жою;

Пайдаланушыны күдікті немесе зақымдалған объектілер туралы хабардар ету;

Электрондық немесе оптикалық тасымалдағыштардан алынған барлық файлдарды және желіден алынған файлдарды зиянды кодтарға тексеру;

Электрондық поштадағы кез келген тіркемелер мен жүктелетін ақпаратты қолданбас бұрын зиянды бағдарламалық қамтамасыз етуге тексеру, бұл әртүрлі нүктелерде орындалуы мүмкін (пошта серверлері, персоналды компьютерлер, желіге кіру).

Антивирус бақылауын жүргізу тәртібі

9.3. Компьютерлерге және жергілікті есептеу желісіне жүйелік және қолданбалы бағдарламаларды орнату (өзгерту) тек ОИКН мамандары арқылы жүзеге асырылады.

9.4. Компьютерге орнатылатын (өзгертілетін) бағдарламалық қамтамасыз ету компьютерлік вирустар жоқтығы тексерілген болуы керек. Орнатудан кейін дереу антивирус тексеруі жүргізіледі.

9.5. Кез келген ақпарат (мәтіндік файлдар, деректер файлдары, орындалатын файлдар), телекоммуникациялық арналар арқылы алынған және берілген ақпарат, сондай-ақ сырттан алынған тасымалдағыштағы ақпарат (магниттік дискілер, таспалар, CD-ROM және т.б.) міндетті антивирус бақылауына жатады.

9.6. Тасымалдағыштағы ақпарат тек қолданар алдында тексеріледі.

Ерекше назар аудару қажет: уақытша жұмысқа қабылданған тұлғаларға (студенттер, уақытша ауыстыратын қызметкерлер) тиесілі тасымалдағыштар. Бұл тұлғалардың жұмысы жергілікті есептеу желісінің ресурстарын қолданғанда тікелей бақылауда жүргізілуі керек.

10. **Жұмыс станцияларында электрондық пошта және Интернет қызметтерін пайдалану нұсқаулығы**

10.1. Электрондық пошта жүйесі мен Интернет арқылы жасалған, жіберілген немесе алынған барлық хабарламалар мен материалдар, сондай-ақ басқа ақпараттық ресурстар ұйымға тиесілі болып саналады және олар қызметкерлердің жеке меншігі бола алмайды.

10.2. Басшылық қызметкерлерге жасалған, алынған немесе жіберілген кез келген хабарламаларды бақылау (қарау, жою) құқығын өзінде қалдырады және осы әрекеттерді орындауға нақты қызметкерлерді уәкілеттей алады.

10.3. Ақпараттық қауіпсіздікке қауіп төнетін фактілер немесе ықтимал қауіптер анықталған жағдайда, ЗОИКН дереу басшылықты хабардар етеді.

10.4. Электрондық пошта мен Интернет қызметтерін пайдалану кезінде келесі әрекеттерге тыйым салынады:

Ресурстарды коммерциялық кәсіпорындарды насихаттау немесе жарнамалау, діни немесе саяси идеяларды тарату, қызметтік міндеттерге қатысы жоқ басқа мақсаттар үшін пайдалану;

Қорлаушы немесе провокациялық хабарламалар жасау (сексуалды қудалау, нәсілдік қорлау, жыныстық белгі бойынша кемсіту, жас немесе сексуалдық бағдар, дін немесе саяси көзқарас, ұлттық немесе денсаулық жағдайына қатысты қорлаушы пікірлер, Қазақстан Республикасының заңымен тыйым салынған ақпарат);

Қызметтік іс-әрекетке қатысы жоқ графикалық, видео, орындалатын және т.б. файлдарды тіркеу; 15 МБ-тан асатын файлдарды жіберу;

Мемлекеттік құпия және басқа да қызметтік немесе құпия ақпаратты шифрламай сұрау немесе жіберу;

Жеке мақсатта топтық хабарламаларды пайдалану;

Пирамидалық хаттар, «бақыт» хаттары, жарнамалық және қызметтік іс-әрекетке қатысы жоқ басқа ақпараттарды тарату;

Зиянды файлдар мен бағдарламаларды, авторлық құқықпен қорғалған бағдарламалық қамтамасыз ету мен материалдарды тарату;

Басқа пошта жүйелері мен пайдаланушылардың есептік жазбаларын пайдалану;

Басқа пайдаланушылардың электрондық хабарламаларына қол жеткізу (басшылық рұқсат еткен жағдайларды қоспағанда);

Интернет хабарламаларына файлдарды тіркеу;

Интернетте қорлаушы және провокациялық мәлімдемелерді тарату;

Террористік, экстремистік, антиконституциялық немесе басқа деструктивтік мазмұндағы веб-сайттарды қарау;

Сенімсіз, зиянды сайттарды немесе қызметтік міндеттерге қатысы жоқ ақпарат бар сайттарды қарау;

Зиянды файлдар мен бағдарламалар, авторлық құқықпен қорғалған бағдарламалар мен материалдар, мультимедиялық файлдарды жүктеу немесе беру;

Интернет-чат қызметтерін пайдалану;

Компьютерлерді Интернетке үшінші тарап провайдерлері арқылы қосу (басшылықтың жазбаша рұқсатынсыз), сондай-ақ рұқсат етілмеген модемдік қосылымдарды пайдалану.

11. Қызметкерлердің төтенше жағдайларда әрекет ету тәртібі

11.1. Осы ереже МО-дағы пайдаланушылардың төтенше (кризистік) жағдайларда әрекет ету тәртібін белгілейді. Ол ақпараттық жүйенің жұмыс қабілеттілігін сақтау, ақпаратты қалпына келтіру және өңдеу процесін қалпына келтіру шараларын қамтиды. Сондай-ақ, жүйе персоналының әртүрлі пайдаланушыларының әрекеттерін сипаттайды, салдарларды жою және зиянды азайту мақсатында.

11.2. Ақпараттық жүйеге жағымсыз әсер ету нәтижесінде ақпараттық қауіпсіздікке қауіп төнген жағдай – төтенше (кризистік) жағдай болып саналады. Мұндай жағдай пайдаланушылардың қасақана немесе қасақана емес әрекеттерінен, апаттардан, табиғи апаттардан немесе электрмен қамтамасыз етудегі проблемалардан туындауы мүмкін.

11.3. Төтенше (кризистік) жағдайлар келесі категорияларға бөлінеді:

Қауіпті – ақпараттық жүйенің толық істен шығуына, негізгі ақпаратты жоюға немесе блоктауға әкелетін жағдай.

Мысалы:

Ғимараттағы электр энергиясын беру бұзылуы;

Сервердің істен шығуы (ақпарат жоғалтуымен);

Сервердің істен шығуы (ақпарат жоғалтусыз);

Серверде ақпараттың бір бөлігін жоғалту, бірақ жұмыс қабілеттілігін сақтау;

Локалдық желінің істен шығуы (деректерді беру физикалық ортасы).

Серіозды – жүйенің жеке компоненттері істен шыққанда, жұмысының бөлігін жоғалтқанда, өнімділіктің төмендеуі немесе бағдарламалар мен деректердің тұтастығы мен құпиялығының бұзылуы.

Мысалы:

Жұмыс станциясының істен шығуы (ақпарат жоғалтуымен);

Жұмыс станциясының істен шығуы (ақпарат жоғалтусыз);

Жұмыс станциясында ақпараттың бір бөлігін жоғалту, бірақ жұмыс қабілеттілігін сақтау;

Табиғи апаттар (өрт, су тасқыны, дауыл).

Ақпарат көздері:

Пайдаланушылар жүйеде немесе қорғаныс құралдарында күмәнді өзгерістерді анықтаған кезде;

Қорғаныс құралдары кризистік жағдайды анықтаған кезде.

11.4. Қауіпті немесе серіозды төтенше жағдай кезінде барлық пайдаланушылар дереу телекоммуникациялық құралдар арқылы хабарланады (телефон, электрондық пошта және т.б.). Одан кейінгі әрекеттер РОИКН функционалды міндеттеріне сәйкес жүзеге асырылады.

11.5. Әрбір серіозды төтенше жағдай РОИКН арқылы талданады. Нәтижесінде пайдаланушы өкілеттіктерін өзгерту, ресурстарға қолжетімділікті қайта қарау, қосымша резервтер жасау, жүйе конфигурациясын өзгерту, қорғау құралдарын баптау және басқа ақпараттық қауіпсіздік шаралары ұсынылады; қажет болған жағдайда жағдайдың себептері зерттеледі, зиян бағаланады және кінәлілер анықталады.

11.6. Серіозды және қауіпті төтенше жағдайлар істен шыққан жабдықты тез арада ауыстыру мен жөндеуді, сондай-ақ зақымдалған бағдарламалар мен деректерді резервтік көшірмеден қалпына келтіруді талап етеді.

11.7. Деректерді тез арада қалпына келтіру резервтік көшіру және көшірмелерді сақтау арқылы қамтамасыз етіледі.

11.8. Резервтік көшіруге серверлердің толық жұмыс қабілеттілігін қалпына келтіру үшін қажет деректер мен бағдарламалар жатады.

11.9. Жүйеде қолданылатын барлық бағдарламалық құралдардың орнату көшірмелері бар.

Пайдаланушылардың төтенше жағдайлардағы әрекеттері:

11.10. Төтенше жағдай анықталған кезде пайдаланушы РОИКН-ды хабардар етеді, ол жағдайды басшылыққа хабарлайды.

11.11. Өрттің белгілері анықталған кезде (түтін, көміртек газы, жалын):

МО бас дәрігері мен өрт қызметкерлеріне хабарлау;

Серверлік, телекоммуникациялық жабдықтар мен тұрақты қуат көздерін ажырату;

Қолмен өрт сөндіргіш арқылы өртті сөндіруге әрекет жасау, әсіресе серверлік бөлменің есігі ашық болғанда.

11.12. Су тасқыны кезінде:

Электр қуатын ажырату (автоматты қосқыш);

МО бас дәрігеріне инцидент туралы хабарлау.

12. Арнайы жағдайларда деректерді резервтік көшіру, сақтау және қалпына келтіру ережелері

12.1 Бұл нұсқаулық ақпаратты резервтік көшіруді ұйымдастыру талаптарын анықтайды және МО корпоративтік есептеу желісіндегі бағдарламалық және ақпараттық ресурстарды резервтік көшіру шараларын ұйымдастыруға арналған.

12.2 МО серверлік жабдықтағы деректерді резервтік көшіруді ұйымдастыру үшін жауапты тұлға – РОИКН.

Бағдарламалық және ақпараттық ресурстарды көшіру, резервтік көшіру мен қалпына келтіруді бақылау

12.3 Ақпараттық жүйелердің жұмыс қабілетінің бұзылуы жағдайында ақпаратты және өңдеу процестерін жедел қалпына келтіру мүмкіндігін қамтамасыз ету мақсатында ақпараттық ресурстар резервтік көшіруге жатады.

12.4 Резервтік көшіруге МО басқару серверінің деректер базасы жатады, онда науқастардың жеке деректері және зертханалық зерттеулердің нәтижелері сақталады.

12.5 Деректерді резервтік көшіру серверлер мен желі пайдаланушыларының жұмысын бұзбай жүргізілуі тиіс.

12.6 ЗОИКН резервтік көшіру нәтижелерін кезең-кезеңімен тексереді.

12.7 МО басқару серверінен резервтік көшірмеден ақпаратты қалпына келтіруді ОИКН қызметкерлері жүзеге асырады.

12.8 Қолда ұстауға ағымдағы және кемінде екі алдыңғы көшірме жатады.

12.9 Көшірмелер сервер мен РОИКН компьютері үшін бөлінген дискілік массивтерде сақталады. Ақпараттық ресурстардың резервтік көшірмелеріне қол жеткізу құқығы ЗОИКН және ЛИС ақпараттық жүйесін қызмет көрсететін компания өкіліне функционалдық міндеттер мен келісімшарт талаптарына сәйкес беріледі.

13. Компьютерлік жабдыққа техникалық қызмет көрсету ережелері

Компьютерді электр және жергілікті желіден ажырату.

Компьютер жүйелік блогының корпусының қақпағын ашу.

Жүйелік блок пен орнатылған құрылғыларды сыртқы тексеру. Тексеру кезінде корпустың жағдайына, механикалық зақымдардың жоқтығына, жабындардың күйіне, бөлшектердің кеуіп, күйіп кетуіне назар аудару керек.

Байланыстар сапасын тексеру:

Блок қуат көзінің дисководтар, қатты диск және аналық платамен байланыстары;

Деректер шиналарының дисководтар, қатты диск және аналық платамен байланыстары;

Компьютер платаларының аналық платамен байланыстары.

Құрылғы беттерінен, сымдар мен кабельдерден шаң мен сыртқы бөлшектерді тазалау. Тазалау үрлегішпен немесе оргтехникаға арналған майлықтармен жүргізіледі.

Жүйелік блок ашық күйде болса, электр желісіне қосу.

Вентиляторлар, қуат блогы және процессордың жұмысын тексеру, қажет болса майлау.

Жүйелік блокты электр желісінен ажырату.

Жүйелік блок қақпағын жабу.

Компьютерді электр және жергілікті желілерге қосу.

14. Компьютерлік жабдық пен бағдарламалық қамтамасыз етуді пайдалану бойынша пайдаланушы нұсқаулығы

14.1 МО барлық пайдаланушыларына қауіпсіздік талаптары мен қараусыз қалған жабдықты қорғау әдістерін білу қажет.

14.2 Маңызды немесе критикалық қызметтік ақпаратты (қағаз немесе электрондық тасымалдағышта) қажет емес кезде сақтау және құлыптау қажет, әсіресе бөлме бос болса.

14.3 Пайдаланушы тағайындалған ОТ-ны тегіс бетке орнатуы тиіс.

14.4 ОТ желдету тесіктері бөгетсіз болуын қадағалау.

14.5 ОТ желіге UPS немесе желілік сүзгілер арқылы қосылған болуын қадағалау.

14.6 Сымдардың зақымдалмауы, сызбаға түспеуі және қысылмауын қадағалау.

14.7 Пайдаланушыларға стандартқа жатпайтын, өз қолымен жасалған немесе ақаулы сымдарды пайдалану тыйым салынады.

14.8 Ақаулы сым немесе ОТ ақауы анықталған жағдайда, инженер-программистке хабарлау.

14.9 Металл немесе басқа заттарды ОТ корпусындағы тесіктерге салуға тыйым салынады.

14.10 ОТ радиаторлар мен жылыту құрылғыларына жақын орнатуға болмайды.

14.11 ОТ жанында тамақ ішуге тыйым салынады.

14.12 Пайдаланушыларға бағдарламалық қамтамасыз етуді орнатуға, жоюға немесе модификациялауға тыйым салынады.

14.13 Пайдаланушыларға әкімші құқықтарымен жұмыс істеу тыйым.

14.14 Локалды желі жабдығын немесе ОТ басқа бөлмеге жылжытуға тыйым.

14.15 Басқа пайдаланушылардың ПК-не немесе желі жабдықтарына заңсыз кіруге тыйым.

14.16 Пайдаланушыларға ұйымның ОТ мен ПО-ны жеке мақсатта пайдалануға тыйым.

14.17 Электрондық пошта мен Интернетті жеке мақсатта пайдалануға тыйым.

14.18 Өзге идентификатор мен парольді пайдалануға тыйым.

14.19 Өз идентификаторын басқаға беруге тыйым.

14.20 Диск пен файлдарды жалпы желіде ашуға тыйым.

14.21 Құпия ақпаратты рұқсат етілмеген адамдар қатысында өңдеуге тыйым.

14.22 ПК-ны қараусыз қалдыруға, экран құлыптаусыз қоюға тыйым.

14.23 Модем немесе басқа байланыс құралдарын пайдаланып өздігінен қосылуға тыйым.

14.24 Бағдарламалық қателерді немесе қорғаныс параметрлеріндегі құжатталмаған қасиеттерді мақсатты пайдалану тыйым.

14.25 Сапасыз қағазды пайдалану тыйым.

14.26 Жеке файлдарды жүйелік қалталарға немесе түбір каталогқа сақтауға тыйым.

14.27 Техникаға бөгде адамдарды кіргізуге және ОТ мен желілік құрылғыларды өз бетімен ашуға тыйым.

14.28 Сыртқы тасымалдағышты қолданар алдында тексеру.

14.29 Қатты дискідегі бос орынды қадағалау; бос орын 500 МБ-тан кем болса, инженер-программистке хабарлау.

14.30 Электрондық пошта мен мессенджерлерді Қазақстан сегментінен тыс пайдалануға тыйым.

15. Жеке компьютермен (ПК) жұмыс кезінде қауіпсіздік техникасы

15.1 Компьютер электр құрылғысы және потенциалды қауіп болып табылады. Қауіпсіздік талаптарын сақтау қажет.

15.2 Жұмыс бастамас бұрын электр желісінің, розеткалардың, жерленудің дұрыстығын және жұмыс қабілеттілігін тексеру қажет. Сапасыз немесе тозған компоненттерді пайдалану, сондай-ақ қосқыштарды модификациялау тыйым. Кабельдер артқа орналастырылуы тиіс.

15.3 Электрді өшірмей компьютер компоненттерін қосу, ажырату немесе жылжытуға болмайды. ОТ жылыту құрылғыларына жақын орналастырылмауы тиіс. Жүйелік блок, монитор мен периферияда бөгде заттар болмауы керек.

15.4 Кейбір құрамдас бөліктерде электр кернеуі ұзақ сақталады. Жеке жөндеу ұсынылмайды, ақаулар болса ОИКН-ге хабарлау қажет.

Системалық блоктың электрмен қамтамасыз етілуі

15.5 Барлық компоненттерді қуат блогы қамтамасыз етеді. Қуат блогы жүйелік блоктың жоғарғы жағында орналасқан.

Гигиеналық талаптар жүйесі

15.6 Компьютермен ұзақ жұмыс денсаулыққа әсер етуі мүмкін. Дұрыс емес орналасқан жұмыс орны тез шаршауға әкеледі.

15.7 Компьютерлік жүйенің адам организміне әсері кешенді: монитор көзге, жұмыс орны омыртқа мен бұлшықеттерге әсер етеді.

Видеожүйеге қойылатын талаптар

15.8 Монитор жұмыс орнында жарықтан шағылыссыз орнатылуы тиіс. Көз бен экран арасы 50–70 см болуы керек.

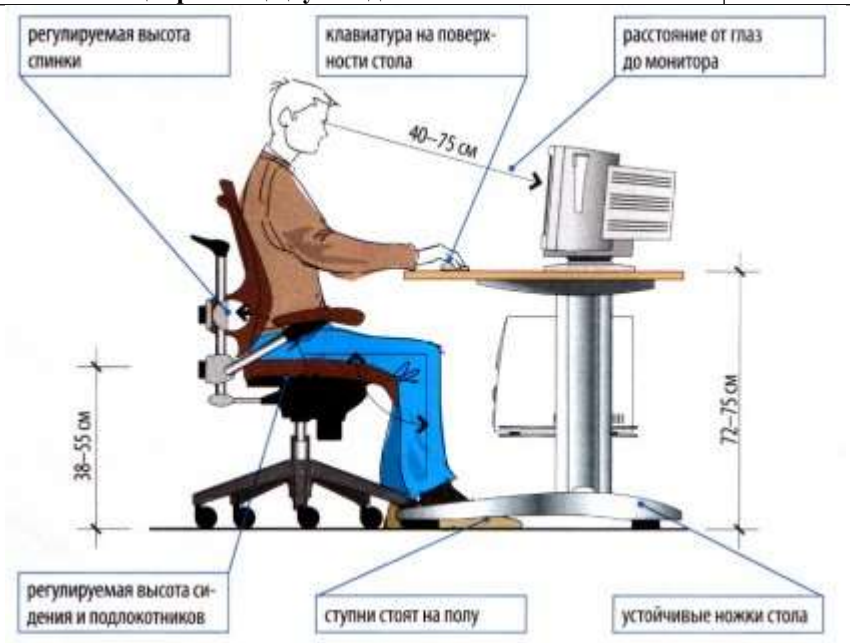
15.9 Мониторды көзден 1,5 D қашықтықта орналастыру ұсынылады (D – экран диагоналі).

Жұмыс орнына қойылатын талаптар

15.10 Жұмыс үстелі мен орындық пайдаланушының дұрыс орналасуын қамтамасыз етуі тиіс.

15.11 Монитор тікелей пайдаланушы алдында орналасуы қажет.

15.12 Жоғарғы деңгей көз пайдаланушының көз деңгейінен сәл жоғары болуы тиіс, экранға жоғарыдан қарау ұсынылады.



15.13. Пернетақта қолдардың саусақтарына кернеусіз, еркін орналасатындай биіктікте орналастырылуы тиіс, ал иық пен білектің арасындағы бұрыш 100°–110° болуға тиіс. Жұмыс істеу үшін арнайы пернетақта сөрелері бар компьютер үстелдерін қолдану ұсынылады. Ұзақ уақыт пернетақтамен жұмыс істегенде білектегі сіңірлердің шаршауы мүмкін.

15.14. Тышқанмен жұмыс істегенде қол ілмектен немесе ауада болмауы керек. Иық немесе кем дегенде білек қатты тірекке ие болуы тиіс. Егер жұмыс үстелі мен орындықтың қажетті орналасуын қамтамасыз ету қиын болса, арнайы тірек жастықшасы бар тышқан кілемшесін қолдану ұсынылады.

Қосымша

Қолданушыларға арналған журнал
Журнал заявок пользователей

№	Күні Дата	Тапсырыстың мәні Суть заявки	Себебі Причина	Қызметкерлердің аты-жөні /лауазымы/ Ф.И.О. сотрудника /должность	Қабылданған шаралар Принятые меры	Қолы Подпись

Штаттан тыс оқиғалар тіркелетін журнал
Журнал регистрации внештатных ситуаций

№ п/п	Қызметкерлердің аты-жөні /лауазымы/ ФИО сотрудника /должность	Күні мен уақыты Дата и время	Штаттан тыс оқиға Внештатная ситуация	Шақырған қызметкедің қолы Роспись сотрудника вызвавшего	Қабылданған шаралар Принятые меры	Қызметкердің қолы Роспись специалиста	Ескертулер Примечание

Бағдарламалық-аппараттық құралдар мен ақпараттық жүйелерді жүйелік-техникалық қызмет көрсету жөніндегі ережелер

«___»___**20 ж. бастап «»__20** ж. дейін _____ мекемесінде бағдарламалық-аппараттық құралдар мен ақпараттық жүйелерді жүйелік-техникалық қызмет көрсету бойынша профилактикалық жұмыстар жүргізіліп, келесі іс-шаралар орындалды:

-Есептеу техникасын жоспарлы техникалық қызмет көрсету жылына 4 рет – әр тоқсанда жүргізіледі.

-Есептеу техникасын жоспарлы техникалық қызмет көрсетуге келесі жұмыстар кіреді:

-Операциялық жүйелерді баптау;

-Серверге қатынау үшін есептік жазбалар мен қолжетімділік параметрлерін баптау (операциялық жүйе деңгейінде);

-Вирустарға тексеру және оларды жою;

-Жүйелік аймақты пайдаланушы файлдарынан тазалау;

-Кабельдік қосылыстардың, разъёмдердің сенімділігін тексеру, қажетсіз бұраулардың жоқтығын бақылау;

-Машинаның, перифериялық құрылғылардың және бүкіл жүйенің жұмыс өнімділігін тексеру/тестілеу;

-Корпус пен алмасып тұратын қақпақтарды ластанудан тазалау.

Өзгерістерді тіркеу парағы

КҮНІ	ӨЗГЕРІСТЕРДІҢ СЕБЕБІ
	3 жыл мерзімінің аяқталуы

Танысу парағы

Лауазым	ТАЖ	Күні	Қолы
Бас дәрігер	Кыдырбаев Б.Д.		
Бас дәрігердің орынбасары	Калметова Г.А.		
Бас дәрігердің орынбасары	Әбдібай Е.М.		
Бас бухгалтер	Сулейменова С.М.		
Бас медбике	Сатмаханова Л.О.		
Кадр маманы	Койшыбаев Е.Н.		
Эпидемиология бөлімінің меңгерушісі	Ахметова Г.Т.		
Емдеу бөлімінің меңгерушісі	Ниязалиева Ф.А.		
ИФА лаборатория меңгерушісінің м.а.	Малимов А.Ә.		
АИТВ-инфекциясын информатика және компьютерлік қадағалау бөлімінің меңгерушісі	Кемелбекова Ф.К.		
Шу қ. ИФА лаборатория филиалының меңгерушісі	Салыкбаева А.Ш.		