АТ БӨЛІМІНІҢ ҚЫЗМЕТКЕРЛЕРІ ҮШІН АУТЕНТИФИКАЦИЯ РӘСІМДЕРІН ҰЙЫМДАСТЫРУ ҚАҒИДАЛАРЫ

Астана

2023 ж.

1. Терминдер мен қысқартулар

Бұл қағидаларда келесі негізгі ұғымдар мен терминдер қолданылады:

Жүйелік әкімші – АЖ жүйелік әкімшілендіру және техникалық қолдау қызметтерін ұсынатын тұлға.

Өз әрекеттері үшін дербес жауапкершілік қағидатын сәйкестендіру, аутентификациялау және сақтау мақсатында АЖ жүйелік әкімшісі пайдаланушыға құпия сөздермен дербес бірегей атаулар (есептік жазба) беруі тиіс.

Пайдаланушы құпия сөздерді пайдалану, ауыстыру және тоқтату процестерін ұйымдастырушылық және техникалық қамтамасыз ету АЖ жүйелік әкімшісіне жүктеледі.

Ақпараттық ресурстар – ақпараттық жүйелерде қамтылған, тиісті бағдарламалық қамтамасыз етумен біріктірілген электрондық жүйеленген ақпарат (деректер қоры);

Құпия сөздің бұзылуы – құпия сөздің таралуы немесе жария етілуі;

АЖ пайдаланушысы – авторизацияны талап ететін өзіне қажетті электрондық ақпараттық ресурстарды алу үшін **АЖ-ға** жүгінетін субъект;

Ұйым – «Qazaq Green» ЖЭК қауымдастығы ЗТБ.

2. Жалпы ережелер

Өз әрекеттері үшін дербес жауапкершілік қағидатын сәйкестендіру, аутентификациялау және сақтау мақсатында АЖ жүйелік әкімшісі пайдаланушыға құпия сөздермен дербес бірегей атаулар (есептік жазба) беруі тиіс.

Пайдаланушылардың, АЖ жүйелік әкімшісінің және қызметкерлердің құпия сөздермен жұмыс істеу кезіндегі іс-әрекеттерін бақылау АЖ-ны сүйемелдеуге жауапты ақпараттық қауіпсіздік жөніндегі маманға жүктеледі.

Жаңа жүйелік әкімшіні жұмысқа қабылдау кезінде ақпараттық қауіпсіздік жөніндегі маман жүйелік әкімшіні АЖ ақпараттық қауіпсіздігінің жұмыс істеуіне және саласында байланысты нормативтік құжаттамамен таныстыруы және АЖ әкімшілендіру үшін құпия сөздерді беруді жүзеге асыруы тиіс (жабық конвертте логиндер мен құпия сөздер туралы ақпаратты беру арқылы). Жүйелік әкімші жоғарыда көрсетілген ақпаратты алғаннан кейін осы қағидаларға сәйкес құпия сөздерді дереу ауыстырып, содан кейін жаңа құпия сөздерді ақпараттық қауіпсіздік жөніндегі маманға беруі тиіс. Ақпараттық қауіпсіздік жөніндегі маман жаңа логиндер мен құпия сөздер туралы ақпаратты жабық конвертке ресімдейді. Корпоративтік желіні

пайдаланушылардың құпия сөздерін беруді жүзеге асыру фактілері осы қағидаларға 1-қосымшаға сәйкес арнайы құрылған журналда тіркелуі тиіс. АЖ рөлдеріне сәйкес пайдаланушылардың құпия сөздерін беру, ауыстыру фактілері АЖ құпия сөздерін беру электрондық журналында ескеріледі. Құпия сөздерді берудің электрондық журналында мынадай өрістер болуы тиіс: реттік нөмірі; құпия сөзді кім берді, жүргізілетін операция, операцияны жүргізу күні мен уақыты.

Жұмыстан шығарылған, басқа құрылымдық бөлімшеге, филиалға, өңірлік орталыққа ауыстырылған пайдаланушылардың есептік жазбаларын жоюды жүйенің әкімшісі ұйымның кадр қызметінен жазбаша хабарлама алған сәттен бастап дереу жүргізуі тиіс.

Қызметкер жұмыстан шығарылғаннан, басқа құрылымдық бөлімшеге, филиалға, өңірлік орталыққа ауыстырылғаннан кейін **3** сағат ішінде ұйымның кадр қызметі жүйелік әкімшіге жасалған бұйрық туралы хабарлауы тиіс.

Кейбір пайдаланушылардың аутентификациясы ақпараттық қауіпсіздікті пайдалануға ұсынылған және ұйым аталған құралдарды әзірлеушілерден (жеткізушілерден) орталықтан сатып алған арнайы қорғаныс аппараттық-бағдарламалық құралдарын пайдалана отырып қамтамасыз етілуі мүмкін.

3. Нормативтік сілтемелер

Осы құжатты әзірлеу үшін құқықтық қамтамасыз ету және негіздемелер бөлігінде мынадай құжаттар пайдаланылды:

1. «Ақпараттандыру туралы» Қазақстан Республикасының 2015 жылғы 24 қарашадағы № 418-V ҚРЗ Заңы;
2. «Техникалық реттеу туралы» Қазақстан Республикасының 2004 жылғы 9 қарашадағы Заңы;
3. ҚР СТ ИСО/МЭК 27001-2015 «Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық қауіпсіздіктің менеджмент жүйесі. Талаптар».

4. Жеке құпия сөзді қалыптастыру қағидалары

Жеке құпия сөздерді пайдаланушылар мен АЖ жүйелік әкімшісі келесі талаптарды ескере отырып өз бетінше таңдауы керек:

Құпия сөз келесі талаптарға сай болуы керек:

- құпия сөздің ұзындығы кемінде 8 таңба болуы керек;
- құпия сөз таңбаларының ішінде жоғарғы және төменгі регистрлердегі әріптер, сандар немесе арнайы таңбалар болуы керек;

- құпия сөзде таңбалардың оңай есептелетін тіркесімдері (аты, тегі, автоматтандырылған жұмыс орнының – АЖО атауы және т.б.), сондай-ақ жалпы қабылданған қысқартулар (ЭЕМ, ЖЕЖ, USER және т.б.), сондай-ақ туған күндер болмауы керек;
- құпия сөз ретінде «бос» құпия сөзді пайдалануға тыйым салынады;
- құпия сөзді өзгерткен кезде жаңа мән алдыңғы мәннен кем дегенде 3 позицияда ерекшеленуі керек;
- пайдаланушының ешкімге жеке құпия сөзін айтуға құқығы жоқ;
- бұрын қолданылған құпия сөздерді таңдауға тыйым салынады;
- іскерлік және іскерлік емес мақсаттар үшін бірдей құпия сөзді пайдалануға тыйым салынады;
- пайдаланушының жеке құпия сөздерін жариялауға құқығы жоқ;
- пайдаланушыға рұқсат беру кезінде құпия сөзсіз тек логинді (пайдаланушы атын) пайдалануға тыйым салынады;
- кездейсоқ таңбалар жиынтығынан құпия сөздерді пайдалану ұсынылады.

Кейбір қызметкерлер үшін өндірістік қажеттілік туындаған жағдайда бірнеше бірегей атауларды (есептік жазбаларды) пайдалануға рұқсат етіледі.

Уақытша құпия сөзді алмас бұрын пайдаланушыға жеке құпия сөзді жария етпеу туралы міндеттемеге қол қою ұсынылады (2-қосымша).

Уақытша құпия сөзді алу үшін пайдаланушы жеке басын куәландыратын құжатты немесе қызметтік куәлікті ұсынуы керек.

Пайдаланушы өзінің құпия сөзін өз бетінше есте сақтауы керек және оны ешбір түрде сақтап, басқа адамдарға бермеуі керек.

Пайдаланушыларға ашық электрондық пошта хабарларымен құпия сөзді беруге немесе оларды үшінші тараптан электрондық пошта хабарларымен ашық нысанда беруге тыйым салынады.

Пайдаланушы құпия сөзді алған кезде құпия сөзді беру және қабылдау журналына қол қоюы керек.

5. Құпия сөзді енгізу (кіру)

Құпия сөзді енгізу регистрді ескере отырып (жоғарғы-төменгі) және пернетақтаның ағымдағы орналасуын (EN-RU және т.б.) ескере отырып жүзеге асырылады.

Құпия сөзді енгізу кезінде оны бөгде адамдар тану немесе техникалық құралдар арқылы құпия сөзді бұзу мүмкіндігін болдырмау қажет.

Құпия сөздерді енгізген кезде логин мен құпия сөздің сенімділігі тексеріледі. Құпия сөз дұрыс енгізілмеген жағдайда жүйеге кіру жүргізілмейді.

6. Құпия сөздерді ауыстыру тәртібі

Жүйеге алғаш кірген кезде пайдаланушы уақытша құпия сөзді өзгертуге міндетті. Құпия сөзді таңдау кезінде құпия сөзді қалыптастыруға қойылатын келесі талаптарды басшылыққа алу қажет:

– құпия сөзде кемінде 8 таңбадан тұруы керек;

– құпия сөзде жай және бас әріп таңбалары, сондай-ақ сандар және (немесе) арнайы таңбалар (#, $, @ және т.б.) болуы керек;

– құпия сөз жалпы қабылданған қысқартулар (мысалы, admin, system, user, sys, god), сондай-ақ жеке және басқа да жалпыға қолжетімді мәліметтер (мысалы, күндер, есімдер, атаулар) сияқты оңай есептелетін таңбалар тізбегін қамтымауы керек;

– құпия сөз пернетақтада орналасу реті оңай есептелетін таңбалар тобын қамтымауы керек (мысалы, 1234, qWerty, qwerty123, 321369);

– құпия сөзді өзгерткен кезде жаңа мән алдыңғы мәннен кем дегенде 4 позицияда ерекшеленуі керек.

Құпия сөз иесі негізгі құпия сөзді құпия сақтау үшін жеке жауап береді. Құпия сөзді басқа адамдарға, оның ішінде құрылымдық бөлімше қызметкерлеріне хабарлауға, оны жазуға, сондай-ақ электрондық хабарламаларда ашық мәтінмен жіберуге тыйым салынады.

Құпия сөзді ешқашан компьютерлік жүйеде қорғалмаған түрде сақтауға болмайды. Иесі құпия сөздердің жазбаларын (мысалы, қағазда, бағдарламалық қамтамасыз ету файлдарында немесе портативті құрылғыда) қауіпсіз сақтауға кепілдік бермей және сақтау әдісін мақұлдамай жасаудан аулақ болу керек.

Есептік жазбалардың бұғатталуын бақылауды жүйелік әкімші есептік жазбаларды тіркеу журналының жазбаларына сәйкес жүзеге асырады.

Ұйымның ақпараттық жүйесінің пайдаланушысы / әкімшісі айына кемінде бір рет негізгі құпия сөзді өзгертуі керек. Негізгі құпия сөзді тек пайдаланушының өзі немесе ұйымның ақпараттық жүйесінің әкімшісі жасай алады. Құпия сөздерді компьютерлік бағдарламалардың және үшінші тараптардың жасауына тыйым салынады.

Әкімші ұйымның ақпараттық жүйелеріне қол жеткізу үшін өзінің аутентификациялық деректерін мөрленген конверттегі қағаз тасығышта АҚБЖ жөніндегі басшылықтың өкіліне береді, ол, өз кезегінде, оларды кілтке жабылатын қоймада сақтайды.

Жүйеге кіру деректемелерін жоғалтқан АЖ пайдаланушысы ұйымға хат негізінде басқа құпия сөзді орнату үшін ресми түрде жүйелік әкімшіден көмек сұрауы керек. АЖ-ға кіру деректемелерін жоғалтқан корпоративтік желіні пайдаланушы құпия сөз беру туралы өтінім негізінде басқа құпия сөз орнату үшін жүйелік әкімшіден ресми түрде көмек сұрауы тиіс (2-қосымша). Жүйелік әкімші қажет болған жағдайда корпоративтік желі мен АЖ пайдаланушысына кез келген уақытта (жүйеде тіркелу кезінде де, құпия сөзді пайдаланудың белгілі бір кезеңінен кейін де) құпия сөзді өзгерте алады.

Жүйе әкімшісі ескі құпия сөздердің циклдік қолданылуын тексеріп, құпия сөздердің қайта қолданылуын болдырмауы керек. Сондай-ақ, АЖ жүйелік әкімшісі пайдаланушылардың пайдаланылмаған есептік жазбаларын (логиндер мен құпия сөздерді) жоюы керек.

Жүйелік әкімші құпия сөздің қолданылу мерзімін, құпия сөзді өзгерту қажеттілігі туралы ескерту хабарламасын беруді және құпия сөздің қолданылу мерзімі 45 күн өткеннен кейін ақпараттық ресурстарға кіруді бұғаттауды көздейтін құпия сөзді өзгерту саясатын айқындайды.

АЖ жүйелік әкімшісі кез келген уақытта құпия сөзді өзгерту мүмкіндігіне ие болуы тиіс. Корпоративтік желі пайдаланушысының құпия сөзін өзгертуді жүйелік әкімші жүзеге асырады.

7. Құпия сөзді басқару

Құпия сөзді басқару жүйесі:

1) алдыңғы пайдаланушы құпия сөздерінің тарихын сақтауы және оларды қайта пайдалануға жол бермеуі;

2) құпия сөздерді сақтауы және қорғалған нысанда (шифрланған немесе хештелген) беруі тиіс.

8. Құпия сөзді сақтау

Құпия сөздердің иелеріне:

1) басқа пайдаланушыларға жеке құпия сөз туралы хабарлауға және оларды жүйеге өз есептік жазбасы мен құпия сөзі арқылы тіркеуге;

2) құпия сөздерді электрондық дәптерге, файлға және қағаз тасығыштардан басқа басқа да ақпарат тасығыштарға жазуға тыйым салынады, бұл ретте құпия сөз жазбалары бар қағаз тасығыштар сейфте сақталуы тиіс.

Есептік жазбалардың атаулары және құпия сөздерді орнату күні бар АЖ жүйелік әкімшісінің құпия сөздері тікелей басшының сейфінде мөрленген конверттерде сақталуы тиіс.

АЖ жүйелік әкімшісі және пайдаланушылар өздерінің құпия сөздерін өзгерткеннен кейін 3 сағат ішінде олардың жаңа мәндерін тиісті бөлімше басшыларына мөрленген конверттегі тиісті шоттардың аттарымен бірге беруі тиіс. Жаңа құпия сөздері бар конвертті алған кезде ескі құпия сөздері бар конверт жойылады.

АЖ-да жұмыс істейтін барлық пайдаланушылар оларды анықтайтын және авторизация кезінде құпия сөзді таңдау және деректерді ұстап қалу мүмкіндігін болдырмайтын қауіпсіз аутентификациядан өтуі тиіс.

Жүйелік құпия сөз бұзылған жағдайда АЖ әкімшісі:

1) құпия сөзді дереу өзгертуі;
2) ақпараттық қауіпсіздік жөніндегі маманға хабарлауы тиіс.

Уақытша жоқ пайдаланушының дербес компьютерінің деректеріне шұғыл қол жеткізу үшін өндірістік қажеттілік туындаған кезде мыналарға рұқсат етіледі:

1) жүйелік әкімші жоқ қызметкердің ақпараттық қауіпсіздік жөніндегі тікелей маманының нұсқауы бойынша компьютерді пайдалану үшін уақытша жоқ пайдаланушының құпия сөзін өзгертеді. Жұмысқа шыққан кезде пайдаланушы бір тәулік ішінде құпия сөзді өзгертуге міндетті. Бұл операциялар құпия сөздерді беру туралы журналда тіркеледі (1-қосымша);
2) қызметкер уақытша болмаған жағдайда тікелей басшының нұсқауы бойынша ақпараттық қауіпсіздік маманына құпия сөз салынған конвертті ашып, компьютерді пайдалану қажет. Жұмысқа шыққан кезде пайдаланушы бір тәулік ішінде құпия сөзді өзгертуге міндетті. Бұл операциялар құпия сөздерді беру туралы журналда тіркеледі (1-қосымша).

Барлық пайдаланушылар құпия сөздерді автоматтандырылған тіркеу процесіне қосуға тыйым салу қажеттілігі туралы білуі керек, мысалы, сақталған макрокомандаларды немесе функционалды пернелерді пайдалану.

Алынған құпия сөзді және дербес компьютерде жүргізілген әрекеттерді жария еткені үшін жауапкершілік осындай жағдайдан кейін құпия сөз алған адамға жүктеледі. Келген кезде уақытша болмаған пайдаланушы жүйеге алғаш кірген кезде құпия сөзді өзгертуге міндетті.

Ұзақ демалысқа (60 күннен астам) кеткен пайдаланушының есептік жазбасын ұйымның кадр бөлімшесінен жазбаша хабарлама алған сәттен бастап АЖ жүйелік әкімшісі бұғаттауы тиіс.

Компьютерде ұмытылған құпия сөзді қалпына келтіру үшін пайдаланушы есептік жазбасының бұғатын ашу туралы шешім қабылдау үшін тікелей басшыға хабарласу керек.

Құпия сөз бұзылған жағдайда пайдаланушы құпия сөзін дереу өзгертуі керек.

9. Құпия сөзді қорғауды ұйымдастыру кезіндегі жауапкершілік

АЖ-мен жұмыс істейтін қызметкерлер осы қағидалардың талаптарымен қол қоя отырып танысуы және қойылған талаптарға сәйкес келмейтін құпия сөздерді пайдаланғаны үшін, сондай-ақ құпия сөздік ақпаратты жария еткені үшін жауапкершілік туралы ескертілуі тиіс.

Жүйенің қалған пайдаланушылары есептік жазбалар мен құпия сөздерді сақтау үшін жауапкершілік алады.

Құпия мәліметтерді ұсынатын құпия ақпаратты жария еткені үшін қызметкер ҚР қолданыстағы заңнамасына сәйкес жауаптылыққа тартылады.

Есептеу техникасы,
телекоммуникациялық жабдық және
ақпараттық жүйенің бағдарламалық
қамтамасыз ету құралдарын түгендеу
және паспорттау қағидаларына
1-қосымша
202_ жылғы «__» _____ № __

Құпия сөздерді беру журналы

№	Жүйелік әкімшінің ТАӘ/қолы	Қызметкердің ТАӘ/қолы	Жүргізілетін операция	Күні
1				

Есептеу техникасы,
телекоммуникациялық жабдық және
ақпараттық жүйенің бағдарламалық
қамтамасыз ету құралдарын түгендеу
және паспорттау қағидаларына
2-қосымша
202_ жылғы «__» _____ № __

Құпия сөз беруге
ӨТІНІМ

Құрылымдық бөлімшенің атауы

_____

Корпоративтік желі пайдаланушысының ТАӘ, лауазымы

_____

Құпия сөзді беру себебі:

_____
_____
_____
_____
_____
_____
_____
_____

Күні және қолы

«____»_____ _____

ТАНЫСУ ПАРАҒЫ

№	Тегі, аты, әкесінің аты	Лауазымы	Жеке қолы	Күні
1	**2**	**3**	**4**	**5**
1				
2				
3				
4				
5				
6				
7				
8				
9				