«PROcredit» микроқаржы ұйымы»

Жауапкершілігі Шектеулі Серіктестігі

«Бекітілді»
ЖШС «PROcredit» микроқаржы ұйымы»
Бұйрық № 08/1-IT
«24» сәуір 2023 жыл

Интернет-ресурс арқылы қызмет көрсету кезінде ақпараттық қауіпсіздік және ақпаратты рұқсатсыз қол жеткізуден қорғау саясаты.

Редакция 02

Алматы қаласы
2023 жыл

1. Жалпы ережелер

1. Осы Қауіпсіздік және ақпаратты рұқсатсыз қол жеткізуден қорғау саясаты «МҚҰ PROcredit» ЖШС интернет-ресурсы (веб-сайты) арқылы қызмет көрсету кезінде (бұдан әрі – Саясат деп аталады) Қазақстан Республикасының ақпараттық қауіпсіздік саласындағы қолданыстағы заңнамасының нормаларына сәйкес әзірленді. Уәкілетті органның актілері және «МҚҰ PROCredit» ЖШС-нің ішкі құжаттары (бұдан әрі – МҚҰ деп аталады).
2. Саясаттың негізгі мақсаты ақпараттық қауіпсіздікті қамтамасыз етуге қатер төндіретін оқиғалардан келтірілген залалды олардың алдын алу немесе олардың зардаптарын барынша азайту жолымен барынша азайту болып табылады. Ақпараттық қауіпсіздік өзінің түпкіліктісі болып табылмайды, оны қамтамасыз ету МҚҰ-ның қолда бар ақпараттық ресурстарына төнген қауіп-қатердің барлық түріне байланысты тәуекелдер мен экономикалық шығындарды азайту үшін қажет. Бұл мақсатта ақпараттың негізгі қасиеттерін сақтау қажет, атап айтқанда:
    - қол жетімділік — тиісті өкілеттіктері бар субъектілердің ақпаратқа уақтылы кедергісіз қол жеткізу мүмкіндігімен сипатталатын мүлік;
    - құпиялылық — осы ақпаратқа қол жеткізе алатын субъектілер тобына шектеу қою қажеттігін көрсететін және жүйенің (ортаның) осы ақпаратты оған қол жеткізуге өкілеттігі жоқ субъектілерден құпия сақтау мүмкіндігімен қамтамасыз ететін мүлік;
    - бүтіндік — оның өмір сүруінде дөпсіз түрде (белгілі бір бекітілген күйге қатысты өзгеріссіз) тұратын ақпараттың қасиеті.

3. Осы Саясат мынадай құжаттардың негізінде әзірленді:
    - ISO/IEC 27001:2022 Ақпараттық технологиялар — Қауіпсіздік техникасы — Ақпараттық қауіпсіздікті басқару жүйелері — Талаптар;
    - ISO/IEC 27002:2022 Ақпараттық технологиялар – Қауіпсіздік техникасы – ақпараттық қауіпсіздікті басқару ережелері мен ережелері.
    - Қазақстан Республикасының Ұлттық Банкі Басқармасының 2019.11.28 No 217 қаулысы.

4. Саясаттың негізгі қағидаттары мыналар болып табылады:
    - заңдылық – ақпараттық қауіпсіздікті қамтамасыз ету үшін қабылданған кез келген іс-әрекеттер қолданыстағы заңнама негізінде, заңмен рұқсат етілген барлық әдістерді пайдаланып, МҚҰ-ның ақпаратты қорғау объектілеріне теріс әсерін анықтау, алдын алу, оқшаулау және жолын кесу үшін жүзеге асырылады;
    - Бизнеске баса назар аудару – ақпараттық қауіпсіздік негізгі қызметті қолдау процесі ретінде қарастырылады. Ақпараттық қауіпсіздікті

қамтамасыз ету жөніндегі кез келген шаралар МҚҰ қызметіне елеулі кедергі келтірмеуге тиіс;

- үздіксіздік – ақпараттық қауіпсіздік жүйесін басқару құралдарын пайдалану, МҚҰ-ның ақпаратты қорғауды қамтамасыз ету жөніндегі кез келген іс-шараларды іске асыру МҚҰ-ның қолданыстағы бизнес-процестерін үзбей немесе тоқтатпай жүзеге асырылуы тиіс;
- күрделілік – ақпараттық ресурстардың өмірлік цикл бойы, оларды пайдаланудың барлық технологиялық кезеңдерінде және барлық жұмыс режимдерінде қауіпсіздігін қамтамасыз ету;
- Техникалық-экономикалық орындылық - қолданылатын қорғаудың мүмкіндіктері мен құралдары ғылым мен техниканың тиісті даму деңгейінде іске асырылуы тиіс, қауіпсіздіктің белгіленген деңгейі тұрғысынан негізделген және талаптар мен стандарттарға сәйкес келуге тиіс. Барлық жағдайларда ақпараттық қауіпсіздік шаралары мен жүйелерінің құны тәуекелдің кез келген түрлерінен болуы мүмкін залалдың мөлшерінен кем болуы тиіс;
- басымдылық – ақпараттық қауіпсіздікке төнетін нақты және әлеуетті қауіп-қатерлерді бағалау кезінде маңыздылық дәрежесі бойынша МҚҰ-ның барлық ақпараттық ресурстарын санаттау (рейтингтеу).

5. Осы Саясат мыналарды анықтайды:
   - МҚҰ-ның ақпараттық қауіпсіздігін қамтамасыз ету жөніндегі негізгі шаралар, оның ішінде ақпараттық қауіпсіздікке төнетін қатерлерді барынша азайту, яғни ақпараттық қауіпсіздік инцидентінің туындауына алғышарттар жасайтын жағдайлар мен факторлар кешені;
   - екі факторлы аутентификация және әлеуетті қарыз алушыларды интернет-ресурс (веб-сайт) арқылы тексеру әдістері;
   - микрокредит беру туралы шарт бойынша тараптардың міндеттемелері тоқтатылғаннан кейін кемінде 5 (бес) жыл ішінде олардың тұтастығы мен құпиялылығын сақтай отырып, қарыз алушыға берілетін және одан алынған электрондық хабарламалар мен өзге де құжаттарды қауіпсіз сақтауды қамтамасыз ету;
   - үшінші тұлғалардың жоспарлы құқық бұзушылықтардың алдын алу жөніндегі шаралар.
6. Осы Саясаттың ережелері объектілердің мынадай тізбесіне қолданылады:
   - МҚҰ-ның құрылымдық бөлімшелерінің қызметкерлері (тағылымдамадан өтушілерді, тағылымдамадан өтушілерді қоса алғанда);
   - МҚҰ-ның ақпараттық жүйелері мен құжаттарына қол жеткізе алатын МҚҰ және басқа да үшінші тұлғалардың қарыз алушылары, олардың бөлігінде МҚҰ-ға және олардың қызметіне тікелей қатысы бар;

- МҚҰ-мен шарттық қатынастарға ие жеткізушілерге, үшінші тұлғаларға және тараптарға;
- құпия ақпаратты, кездейсоқ және санкцияланбаған әсерлер мен олардың қауіпсіздігін бұзуға сезімтал басқа да МҚҰ-ның ақпараттық ресурстары, ақпараттық ресурстар (деректер базасы, файлдар, жүйелік құжаттама, пайдаланушы жөніндегі нұсқаулықтар, оқу материалдары, саясаттар мен рәсімдер және т.б.), оның ішінде жалпыға қолжетімді ақпарат электрондық түрде ұсынылған;

7. ақпаратты өңдеу және талдау жүйелерін, ақпарат алмасу және телекоммуникация арналарын, деректерді жеткізушілерді, ақпараттық қауіпсіздік жүйелері мен құралдарын, IT-ресурстардың элементтері орналасқан үй-жайларды қоса алғанда, ақпаратты өңдеу және талдау жүйелерін, оны өңдеуге, беруге және көрсетуге арналған аппараттық-бағдарламалық қамтамасыз етуді қоса алғанда, МҚҰ-ның ақпараттық инфрақұрылымы.
8. **Осы Саясат қоғамдық құжат болып табылады және МҚҰ https://www.altyncoin.kz/ ресми сайтында орналастырылады.**
9. Ақпаратты сенімді қорғауды құру процесі ешқашан аяқталмайды. Ақпараттық қауіпсіздіктің жеткілікті сенімді жүйесін қамтамасыз ету үшін оның параметрлерін үнемі түзетіп отыру, сыртқы және ішкі ортадан шығатын жаңа қауіптерге тойтарыс беруге бейімделу қажет.

2. Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі шаралар

10. МҚҰ ақпараттық қауіпсіздігін қамтамасыз етудің негізгі шаралары мыналар болып табылады:
    - әкімшілік, құқықтық және ұйымдастырушылық шаралар;
    - физикалық қауіпсіздік шаралары;
    - бағдарламалық және техникалық іс-шаралар.
11. Әкімшілік, құқықтық және ұйымдық шаралар мыналарды қамтиды (бірақ олармен шектелмейді):
    - Қазақстан Республикасы заңнамасының және ішкі құжаттардың талаптарының сақталуын бақылау;
    - Саясатты қолдайтын ережелерді, әдістер мен нұсқауларды әзірлеу, іске асыру және іске асырылуын бақылау;
    - бизнес-процестердің Саясат талаптарына сәйкестігін бақылау;
    - ақпараттық жүйелермен және ақпараттық қауіпсіздік талаптарымен жұмыс істеу үшін МҚҰ қызметкерлерін ақпараттандыру және оқыту;
    - инциденттерге ден қою, салдарын тежеу және азайту;

- ақпараттық қауіпсіздіктің жаңа тәуекелдерін талдау;
- ұжымдағы моральдық-іскерлік ахуалды бақылау және жақсарту;
- төтенше жағдайлар туындаған жағдайдағы іс-қимылдарды анықтау;
- МҚҰ қызметкерлерін жұмысқа қабылдау және жұмыстан босату кезінде алдын алу іс-шараларын жүргізу.

12. Физикалық қауіпсіздік шаралары мыналарды қамтиды (бірақ олармен шектелмейді):

- күзетілетін объектілерді, оның ішінде техникалық қауіпсіздік техникасын пайдалануды тәулік бойы күзетуді ұйымдастыру;
- күзетілетін объектілердің өрт қауіпсіздігін ұйымдастыру;
- МҚҰ қызметкерлерінің және үшінші тұлғалардың шектеулі үй-жайларға (серверлерге) қол жеткізуін бақылау.

13. Бағдарламалық-техникалық іс-шаралар мыналарды қамтиды (бірақ олармен шектелмейді):

- лицензияланған бағдарламалық қамтамасыз етуді және сертификатталған ақпараттық қауіпсіздік құралдарын пайдалану;
- периметрді қорғау құралдарын (брандмауэр және т.б.) пайдалану;
- вирусқа қарсы кешенді қорғау құралдарын қолдану;
- Бастапқы кодты, компоненттер мен кітапханаларды сыналған бағдарламалық қамтамасыз етуде пайдаланылатын барлық бағдарламалау тілдерін талдауды қолдайтын статикалық бастапқы кодты талдау сканерін пайдалана отырып талдау.
- ақпараттық жүйелерге құрылған ақпараттық қауіпсіздік құралдарын пайдалану;
- ақпараттың тұрақты резервтік көшірмесін қамтамасыз ету;
- пайдаланушылардың, ең алдымен артықшылықты пайдаланушылардың құқықтары мен іс-әрекеттерін бақылау;
- ақпаратты криптографиялық қорғау жүйелерін қолдану;
- Аппараттық құралдардың уақытын қамтамасыз ету.

3. Ақпараттық қауіпсіздік саласындағы тәуекелдерді бағалау

14. МҚҰ ақпараттық қауіпсіздігінің тәуекелдерін бағалау үшін мынадай шаралар қабылданады:

- аса маңызды ақпараттық активтер тізбесін қалыптастыру;

- Аса маңызды ақпараттық активтер үшін ақпараттық қауіпсіздік тәуекелдерін бағалау.

15. Аса маңызды ақпараттық активтердің тізбесіне жылжымайтын мүлік объектілерінің бұзылуынан болған шығындар ақпараттық қауіпсіздікті бұзудан болған шығындардың материалдықтың белгіленген деңгейінен асатын ақпараттық активтер енгізіледі.
16. Ақпараттық қауіпсіздіктің аса маңызды активтері үшін тәуекелдерді бағалау мақсатында МҚҰ мынадай процестердің іске асырылуын қамтамасыз етеді:
    - аса маңызды ақпараттық активтерге ақпараттық қауіпсіздік қатерін анықтау;
    - аса маңызды ақпараттық активтерге қатысы бар ақпараттық қауіпсіздікке қатер төндіретін көздерді анықтау;
    - аса маңызды ақпараттық активтердің осал тұстарын анықтау;
    - ақпараттық қауіпсіздік тәуекелдерін басқару жөніндегі қолданыстағы шараларды айқындау;
    - ақпараттық қауіпсіздікке қатер төндіретін көздермен іске асырылатын аса маңызды ақпараттық активтерге ақпараттық қауіпсіздікке қатер төну ықтималдығын бағалау;
    - ақпараттық қауіпсіздік тәуекелдерінің деңгейін бағалау.
17. Ақпараттық қауіпсіздіктің аса маңызды активтеріне ақпараттық қауіпсіздік қатерін анықтауды ақпараттық қауіпсіздік бөлімшесі жүзеге асырады. Ақпараттық активтің әрбір сыни түрлері бойынша ақпараттық қауіпсіздікке төнетін қатерлерге талдау жүргізіледі.
18. Аса маңызды ақпараттық активтерге қатысы бар ақпараттық қауіпсіздік қатерлерінің көздерін анықтауды ақпараттық қауіпсіздікке төнетін қатерлердің көздерін ескере отырып, МҚҰ ақпараттық қауіпсіздік бөлімшесі жүзеге асырады.
19. Аса маңызды ақпараттық активтердің осал тұстарын анықтауды МҚҰ-ның ақпараттық қауіпсіздік бөлімшесі мынадай мәліметтерді ескере отырып жүзеге асырады:
    - ақпараттық активті салу;
    - ақпараттық активтің физикалық орналасуы;
    - бағдарлама кодындағы белгілі қателер;
    - Баптау қателері
    - ақпараттық активті пайдалану үдерісіндегі кемшіліктер.
20. Аса маңызды ақпараттық активтерге қатысты ақпараттық қауіпсіздік тәуекелін басқарудың қолданыстағы шараларын айқындауды ақпараттық қауіпсіздік бөлімшесі аса маңызды ақпараттық активтердің ақпараттық қауіпсіздігін қамтамасыз ету процесінде бар кемшіліктерді немесе оны бұзудың салдарын жоюға

бағытталған ұйымдастырушылық-техникалық іс-шаралар туралы ақпаратты ескере отырып жүзеге асырады.

21. Ақпараттық қауіпсіздік қатерлерінің көздерімен іске асырылатын ақпараттық активтерге ақпараттық қауіпсіздіктің қатерлерінің ықтималдығын бағалауды ақпараттық қауіпсіздік қауіпсіздігінің қатер көзінің, ақпараттық қауіпсіздік қатерінің және аса маңызды ақпараттық активке қатысы бар осалдықтың барлық үйлесімдері үшін ақпараттық қауіпсіздік бөлімі мынадай мәліметтерді ескере отырып жүргізеді:
    - ақпараттық қауіпсіздік қатері көзінің тиісті аса маңызды ақпараттық активтерге қатысты (ішкі немесе сыртқы) орналасқан жері туралы деректер. Ақпараттық қауіпсіздікке төнетін қауіп-қатердің ішкі көздері үшін активті пайдаланушылардың саны, ақпараттық қауіпсіздік қатерлерінің сыртқы көздері үшін - қорғау периметрінен тыс жерлерден мүмкін болатын қол жеткізудің болуы ескеріледі;
    - ақпараттық қауіпсіздік қатерінің көзіне қол жеткізу деңгейі туралы деректер;
    - ақпараттық қауіпсіздіктің аса маңызды ақпараттық активтерге бұрынғы кездегі қауіптілігінің жиілігі туралы статистикалық деректер;
    - аса маңызды ақпараттық активке ақпараттық қауіпсіздік қатерін іске асырудың күрделілігі туралы ақпарат;
    - қарастырылып отырған аса маңызды ақпараттық активтерге қатысты қорғау шараларының болуы туралы деректер.
22. Ақпараттық қауіпсіздік қатерлерінің көздерімен іске асырылатын ақпараттық қауіпсіздік қатерлерінің ықтималдығын бағалауға бірнеше сарапшы қатысқан және әр түрлі баға алған кезде ең жоғары ықтималдықты анықтайтын бағалауға тең қорытынды, қорытылған баға алынады.
23. Ақпараттық қауіпсіздік тәуекелдерінің деңгейін бағалау ақпараттық қауіпсіздікке қатер төндіретін көздермен ақпараттық қауіпсіздік қатерінің туындау ықтималдығын бағалау және құпиялылықты, тұтастықты немесе аса маңызды ақпараттық активтің болуын бұзудан тиісті ықтимал шығындарды бағалау негізінде жүзеге асырылады.

4. Автоматтандырылған ақпараттық жүйеге қойылатын талаптар

24. Клиентті сәйкестендіру және аутентификаттау үшін клиенттің жеке кабинетінде мынадай тәсілдер пайдаланылады:

1) СДАО-ның қызметін пайдалану арқылы клиентті биометриялық сәйкестендіру;

2) клиентті екі факторлы аутентификаттау.

25. Клиенттің екі факторлы аутентификаттау мынадай факторлардың кем дегенде екеуін қолдану арқылы жүзеге асырылады:
    - иелену факторын растау: клиенттің клиент тіркелген токенмен автоматты түрде генерацияланған бір реттік парольді енгізуі немесе клиенттің клиент тіркелген смарт-картаны оқу құрылғысына қосылуы немесе клиенттің клиент көрсеткен клиенттің байланыс құрылғысының абоненттік нөміріне автоматты түрде генерацияланған және берілген бір реттік парольді енгізуі, клиенттің жеке сәйкестендіру нөмірін ұялы байланыс операторының дерекқорындағы абоненттік нөмір иесінің жеке сәйкестендіру нөмірімен салыстырып тексеру немесе "электрондық үкімет" веб-порталы арқылы клиенттердің ұялы телефон нөмірлері базасындағы клиенттің жеке сәйкестендіру нөмірін салыстырып тексеру арқылы осы абоненттік нөмірдің клиентке тиесілілігі туралы ақпарат алу арқылы клиентке осы абоненттік нөмірдің тиесілілігін тексеру;
    - бөлінбеушілік факторын растау: нақты уақыт режимінде клиент тұлғасының бейнесін оның жеке басын куәландыратын құжаттағы бейнесімен салыстыру, бұл ретте клиенттің нақты уақыт режимінде бейненің орнына клиент тұлғасының статикалық бейнесін немесе бейнежазбасын пайдаланудан қорғау қамтамасыз етіледі.

26. Жеке кабинет клиентке мынадай, бірақ олармен шектелмей, іс-қимылдарды жүзеге асыру мүмкіндігін береді:

1) клиенттің микрокредит алуға өтініш беруі;
2) микроқаржылық қызметті жүзеге асыратын ұйым туралы мәліметтерді (заңды және (немесе) нақты мекенжайы, байланыс телефондары, факс, электрондық пошта мекенжайы және басқа мәліметтер), микроқаржылық қызметті жүзеге асыратын ұйымның бірінші басшысы туралы мәліметтерді (тегі, аты, әкесінің аты (болса)) қарау;
3) клиенттің микрокредит беру туралы шартын (шарттарын) (шарт жасалғанға және жасалғаннан кейінгі) қарау;
4) клиенттің микрокредит алуға өтінішінің қаралу барысы және нәтижелері туралы ақпаратты қарау;
5) клиенттің микрокредит (микрокредиттер) бойынша ағымдағы берешегінің сомасы, клиенттің алдағы және нақты төлемдері туралы, оның ішінде негізгі борыш, сыйақы, тұрақсыздық айыбы (айыппұлдар, өсімпұлдар) сомасы туралы ақпаратты қарау;
6) клиенттің микрокредитті өтеу тәсілдері туралы ақпаратты қарау;
7) клиент пен микроқаржылық қызметті жүзеге асыратын ұйым арасында хаттар (хабарлар) алмасу.

27. Микрокредит электрондық тәсілмен берілгенге дейін микроқаржылық қызметті жүзеге асыратын ұйым:

1) клиентті Қазақстан Республикасының қылмыстық жолмен алынған кірістерді заңдастыруға (жылыстатуға) және терроризмді қаржыландыруға қарсы іс-қимыл саласындағы заңнамасына және ішкі құжаттарға сәйкес клиентті тиісінше тексеруді жүзеге асырады;

2) клиентті микрокредиттер беру қағидаларымен таныстырады;

3) клиентке микрокредитті алумен, қызмет көрсетумен және өтеумен (қайтарумен) байланысты төлемдер және аударымдар туралы толық әрі дәйекті ақпарат береді;

4) клиентке микрокредитті өтеу әдісімен танысу және таңдау үшін түрлі әдістермен (сараланған төлемдер, аннуитеттік төлемдер әдісімен немесе микрокредиттер беру қағидаларына сәйкес есептелген әдіспен) есептелген өтеу кестелерінің жобаларын ұсынады;

5) клиентті микрокредит алумен байланысты құқықтары мен міндеттер туралы хабардар етеді.

28. Микрокредит беру туралы шарт жасасу, микроқаржылық қызметті жүзеге асыратын ұйым мен клиент арасында электрондық тәсілмен микрокредит беру туралы шартқа өзгерістер мен толықтырулар енгізу клиенттің парольдарды жинақтау және енгізу немесе аутентификаттау белгілерінің (токендер, смарт-карталар, біржолғы парольдар) кемінде біреуін пайдалану арқылы жүзеге асырылады).

29. Микрокредитті электрондық тәсілмен беру микроқаржылық қызметті жүзеге асыратын ұйымның банктік шотынан клиенттің банктік шотына (төлем карточкасына) ақша аудару жолымен, сондай-ақ клиентке терминал арқылы қолма-қол ақшаны беру және (немесе) микроқаржылық қызметті жүзеге асыратын ұйымды қарыз алушы сатып алатын тауарларға немесе орындаған жұмыстарға, қызметтерге ақы төлеуді көздейтін шарт жасасқан заңды тұлғаның банктік шотына микрокредитті қарыз алушының өтініші бойынша аудару арқылы жүзеге асырылады.

30. Микроқаржылық қызметті жүзеге асыратын ұйым Қазақстан Республикасының қылмыстық жолмен алынған кірістерді заңдастыруға (жылыстатуға) және терроризмді қаржыландыруға қарсы іс-қимыл саласындағы заңнамасында көзделген негіздер бойынша клиентке микрокредит беруден бас тартады.

31. Электрондық тәсілмен микрокредиттер беру микроқаржылық қызметті жүзеге асыратын ұйымның клиентке электрондық тәсілмен микрокредит беруге негіз болған электрондық құжаттардың мазмұнындағы бұрмалаушылықтарды және (немесе) өзгерістерді анықтауды, сондай-ақ микрокредит беру құпиясын құрайтын ақпаратқа заңсыз қол жеткізуден қорғауды және клиент берген сәйкестендіру және аутентификаттау деректерін кредит алу кезінде заңсыз қайта пайдаланудан қорғауды қоса алғанда, осы

ақпараттың тұтастығын көздейтін ішкі құжаттарына сәйкес жүзеге асырылады.

32. Клиенттің сұратуы бойынша микроқаржылық қызметті жүзеге асыратын ұйым электрондық тәсілмен микрокредиттің берілгенін (алынғанын) растайтын электрондық құжаттарды жіберу және (немесе) алу туралы растауды оған микрокредит беру туралы шартта көзделген тәртіппен және мерзімдерде ұсынады.

33. Микроқаржылық қызметті жүзеге асыратын ұйым клиентке берілген және одан алынған электрондық хабарлар мен өзге құжаттардың тұтастығы мен конфиденциалдылығын сақтай отырып, олардың микрокредит беру туралы шарт бойынша тараптардың міндеттемелері тоқтатылғаннан кейін кемінде 5 (бес) жыл бойы қауіпсіз сақталуын қамтамасыз етеді.

34. Электрондық хабарларды және өзге құжаттарды сақтау олар қалыптастырылған, клиентке берілген немесе одан алынған форматта жүзеге асырылады.

35. Микрокредит беру құпиясын құрайтын ақпаратқа заңсыз қол жеткізу, оны заңсыз өзгерту, үшінші тұлғалар тарапынан заңсыз әрекеттерді не өзге де микрокредиттермен заңсыз (алаяқтық) әрекеттерді жүзеге асыру анықталған жағдайда, микроқаржылық қызметті жүзеге асыратын ұйым мұндай әрекеттердің себептері мен салдарын жою үшін екі жұмыс күні ішінде шаралар қабылдайды, сондай-ақ бұл туралы бір жұмыс күні ішінде клиентті және уәкілетті органды хабардар етеді.

36. Микроқаржылық қызметті жүзеге асыратын ұйым енгізген қылмыстық құқық бұзушылық жасауға ықпал еткен мән-жайларды жою жөнінде шаралар қабылдау туралы ұсынымның не құқық қорғау органдары ұсынған қарыз алушыны жәбірленуші деп тану туралы қаулының негізінде микроқаржылық қызметті жүзеге асыратын ұйым күнтізбелік үш күннен кешіктірмей:

- клиенттің микрокредиті бойынша берешекті өндіріп алуды және талап-арыз жұмысын тоқтатады;
- микрокредит бойынша берешектің болуы туралы жазбаларды жою арқылы клиенттің кредиттік бюролардағы кредиттік тарихына түзетулер енгізеді.

37. Микроқаржылық қызметті жүзеге асыратын ұйым құқық қорғау органдарының ұйғарымы және (немесе) қаулысы және (немесе) микроқаржылық қызметті жүзеге асыратын ұйымның өтініші бойынша қабылданған, заңды күшіне енген сот шешімі бар микрокредит бойынша клиенттің берешегін есептен шығару туралы шешім қабылдайды.

5. Электрондық хабарламалар мен басқа да құжаттарды қауіпсіз сақтау

38. МҚҰ ақпараттық қауіпсіздігін қамтамасыз ету мақсатында мынадай шарттар сақталады:

- ақпараттық қауіпсіздікті басқару жүйесін ұйымдастыру туралы;
- ақпараттық активтерге қол жеткізуді ұйымдастыру туралы;
- ақпараттық инфрақұрылымның қауіпсіздігін қамтамасыз етуге;
- ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі іс-шараларды және қауіп-қатерлерді анықтау және талдау, шабуылдарға қарсы іс-қимыл жасау және ақпараттық қауіпсіздік инциденттерін тергеу жөніндегі іс-шараларды бақылау;
- ақпараттық қауіпсіздік инциденттері туралы ақпаратты, оның ішінде ақпараттық жүйелердегі бұзушылықтар, істен шығулар туралы ақпаратты талдау;
- ақпаратты криптографиялық қорғау құралдарымен;
- ақпараттық активтерге үшінші тұлғалар қол жеткізген жағдайда ақпараттық қауіпсіздікті қамтамасыз етуге;
- ақпараттық қауіпсіздіктің жай-күйіне ішкі аудит жүргізуге;
- ақпараттық қауіпсіздікті басқару жүйесінің процестері туралы.

39. Қорғауға жататын ақпарат:

- қағазға орналастыруға;
- электрондық түрде бар (компьютерлік техника құралдарымен өңделген, берілетін және сақталатын, техникалық құралдармен жазылған және қайта шығарылатын);
- телефон, телефакс, телекс, т.б. арқылы, электр сигналдары түрінде беріледі;
- кездесулер мен келіссөздер кезінде ауадағы акустикалық және діріл сигналдары түрінде және конструкцияларды қоршап тұру.

40. Жасалған келісімдер шеңберінде кредиттік бюродан (бұдан әрі – КБ деп аталатын) әлеуетті қарыз алушылар туралы ақпаратты (ресми кірістер туралы деректер, Мемлекеттік әлеуметтік сақтандыру қорынан берілетін трансферттер, республикалық бюджеттен зейнетақы төлемдерінің саны мен орташа мөлшері туралы, кредиттік есеп деректері және басқа есептер) беру туралы келісімдер бөлігінде ХҚҰ қызметін ұйымдастыру кезінде ақпараттық қауіпсіздікті қамтамасыз етуге қойылатын талаптар:

41. МҚҰ КБ ақпараттық жүйесінен алынған ақпараттың құпиялылығын және тұтастығын қамтамасыз етуге тиіс.

42. МҚҰ КБ-мен жасалған Келісімдердің талаптарына сәйкес ақпараттық қауіпсіздіктің тиісті деңгейін қамтамасыз етуге тиіс.

43. МҚҰ КБ ақпараттық жүйесімен өзара іс-қимыл жасау және одан алынған ақпаратты өңдеу үшін пайдаланылатын жүйелік және қолданбалы бағдарламалық қамтамасыз етудің жұмыс істеуі мен қорғалуы үшін қажетті ұйымдастырушылық, техникалық, технологиялық талаптар мен іс-шаралардың орындалуын қамтамасыз етеді.

44. КБ ақпараттық жүйесімен жұмыс істеуге арналған жабдықты пайдалану кезінде оны рұқсатсыз қол жеткізуден қорғау, сондай-ақ деректерді жеткізушілерді және КБ ақпараттық жүйесімен жұмыс істеу үшін пайдаланылатын желілік ресурстарды қорғау қажеттілігі ескеріледі.

45. МҚҰ жауапты тұлғалардың тізбесін анықтап, бекітсін.

46. МҚҰ-ның жауапты (жауапты) тұлғалары (тұлғалары) қол қойған олардың функционалдық міндеттерін орындау барысында белгілі болған ақпаратты жария етпеу және таратпау жөніндегі міндеттемелердің болуын қамтамасыз етуге тиіс.

47. МҚҰ-ның жауапты тұлғалардың тізбесін, олардың құқықтары мен міндеттерін (оның ішінде лауазымдық тізімдемелерді) айқындау және бекіту тәртібін айқындайтын ішкі құжаттардың болуын қамтамасыз етеді.

48. Ақпаратқа қол жеткізу МҚҰ қызметкерлеріне олардың функционалдық міндеттерін орындау үшін қажетті көлемде берілуге тиіс.

49. КБ ақпараттық жүйесінде ол анықталған жауапты тұлғаның шоты нақты жеке тұлғаға сәйкес келеді.

50. МҚҰ-ның жұмыс станцияларының (сайт) Ақпараттық қауіпсіздік саясатына сәйкестігіне жоспарлы және жоспардан тыс тексерулер жүргізуі тиіс.

51. Уәкілетті органның сұрау салуы бойынша МҚҰ КБ-мен жасалған шарттарда көзделген талаптарға оның сәйкестігін растайтын ақпаратты ұсынуға тиіс.

52. Жұмыс станциясының операциялық жүйесі пайдаланушыларды сәйкестендіру және аутентификациялау, сондай-ақ берілген құқықтарға сәйкес пайдаланушылардың қол жеткізу және авторизациялау құқықтарын саралау функцияларын қамтамасыз етеді.

53. МҚҰ өзінің жұмыс станциясын пайдаланады.

54. Кредиттік бюроның ақпараттық жүйесіне қосу үшін жұмыс станциясын пайдалану кезінде басқа интернет-ресурстарға бір мезгілде қосылуға болмайды.

55. МҚҰ қызметкерлері ақпараттық жүйелерге қол жеткізу үшін пайдаланылатын жеке сәйкестендіру және аутентификация деректері құпиялылығын қамтамасыз етуге тиіс.

56. МҚҰ қызметкерлері Кредиттік бюроның ақпараттық жүйесін пайдалану процесінде өздеріне белгілі болған ақпараттың құпиялылығын қамтамасыз етуге тиіс.

57. МҚҰ ақпараттық қауіпсіздігін қамтамасыз ету үшін жауапкершілік өз өкілеттіктері шегінде және осы Саясатта белгіленген ережелерге және оның негізінде әзірленген құжаттарға сәйкес МҚҰ-ның барлық құрылымдық бөлімшелеріне жүктеледі.
58. Осы Саясаттың және оның негізінде әзірленген құжаттардың талаптарын бұзғаны үшін жауаптылық МҚҰ-ның ішкі нормативтік құжаттарына және Қазақстан Республикасының заңнамасына сәйкес қамтамасыз етіледі.

6. Ақпараттық қауіпсіздікті бұзудың алдын алу жөніндегі іс-шаралар

59. Киберқауіпсіздік инциденттерінің алдын алуда бағдарламалық қамтамасыз етуді әзірлеу, ақпараттық жүйелердің құрамдас бөліктерін және қаржы секторы инфрақұрылымын жобалау кезінде тиісті ұлттық және халықаралық талаптарды сақтау маңызды рөл атқарады. МҚҰ киберқауіпсіздік тәуекелдерін тұрақты бағалауды жүзеге асырады, ол осы тәуекелдерді барынша азайту жөніндегі шараларды әзірлеуге және қолдануға, сондай-ақ іске асырылатын шаралардың тиімділігін бағалауға негіз болады.
60. Алдын алу (алдын алу) сатысында алынған нәтижелер, сондай-ақ өңделген инциденттердің тәжірибесі ескерілуге тиіс. Киберқауіпсіздік инциденттерінің сипаты, шамасы және әсері олардың әсерін жұмсарту мақсатында уақтылы бағаланады, ішкі және сыртқы мүдделі тараптар уақтылы хабардар етіледі, сондай-ақ бірлескен ден қою шаралары үйлестіріледі. Мүдделі тараптар мыналарды қамтиды:

- Қазақстан Республикасының Ұлттық Банкі;
- МҚҰ қызметін реттейтін өзге де уәкілетті мемлекеттік және заң шығарушы органдар;
- - қарыз алушылар;
- кредиторлар мен инвесторлар;
- МҚҰ қызметін жүзеге асыру процесінде өзара іс-қимыл жасайтын құрылымдық бөлімшелердің қызметкерлері;
- қызмет көрсету провайдерлері.

61. Инциденттен кейін жедел іс-шараларды жалғастыру қалпына келтіру рәсімдерін бір мезгілде орындаумен қамтамасыз етілуі тиіс, оның ішінде:

- болған оқиғаның салдарын жою;
- ақпараттық жүйелер мен деректердің қалыпты жай-күйін олардың қалыпты жай-күйін растап қалпына келтіру;
- болашақта осындай оқиғалардың алдын алу мақсатында болған оқиғаның бір бөлігі ретінде пайдаланылған осал тұстарды анықтау және жою;

- ел ішінде және елден тыс жерлерде тиісті ақпарат алмасуды қамтамасыз ету.

62. Пайдаланушылардың да, қызметкерлердің де хабардарлығы мен құзыреттілігін арттыру (біліктілікті арттыру, оқыту) тәуекелдерді жоюға және МҚҰ-да ақпаратты қауіпсіз құру және пайдалану мәдениетін қалыптастыруға көмектеседі. Ақпараттандыруды арттыру кезеңі пайдаланушылардың нақты тәуекелдер мен оларды жұмсартудың тиімді әдістері туралы хабардар болуын қамтамасыз ету мақсатында алдын алу мен ден қоюдан алынған сабақтарға сүйенуге тиіс.

63. Ақпараттық қауіпсіздіктің классикалық моделі ақпараттың қауіпсіздігін қамтамасыз ету үшін маңызды үш атрибутты: құпиялылықты, тұтастықты және қол жетімділікті қамтамасыз етуге негізделеді.

64. Ақпараттың құпиялылығы оның иесі анықтаған тұлғалардың қатаң шектеулі саны ғана онымен таныса алатынын білдіреді.

65. Егер рұқсат етілмеген адам ақпаратқа қол жеткізе алса, рұқсатсыз қол жеткізу немесе құпиялылықты бұзу орын алады.

66. Қол жетімділік (қажетті ақпараттық қызметті ақылға қонымды мерзімде алу мүмкіндігі)

67. Тұтастық (ақпараттың өзектілігі мен дәйектілігі, оны жоюдан және рұқсатсыз өзгертуден қорғау);

68. Микрокредит беру құпиясын құрайтын ақпаратқа рұқсатсыз қол жеткізу, оны санкцияланбаған өзгерту, үшінші тұлғалардың санкцияланбаған іс-әрекеттерді орындауы анықталған жағдайда, МҚҰ мұндай әрекеттердің себептері мен салдарын жою жөнінде дереу шаралар қабылдауға, сондай-ақ ол туралы уәкілетті органға бір жұмыс күні ішінде хабарлауға тиіс.

69. МҚҰ-ның қылмыстық жолмен алынған кірістерді заңдастыру (жылыстату) және терроризмді қаржыландыру схемаларында микрокредиттер берудің қолданыстағы немесе енгізілген әдістері мен технологияларын электрондық тәсілдермен пайдалануға жол бермеу жөнінде шаралар қабылданды. Әлеуетті қарыз алушының микрокредиттер беруі және кредиттік есеп жүргізуі кезінде МҚҰ Қазақстан Республикасының 28 тамыздағы Заңында көзделген қажетті шараларды қолданады. 2009 жылғы "Қылмыстан түскен кірістерді заңдастыруға (жылыстатуға) және терроризмді қаржыландыруға қарсы күрес туралы" (бұдан әрі - " ҚЖ/ТҚҚ заңы" деп аталатын), сондай-ақ Қазақстан Республикасының Ұлттық Банкі Басқармасының "Ұлттық Банк Басқармасының қаулысына өзгерістер мен толықтырулар енгізу туралы" қаулысына сәйкес «Қаржы институттарының банктік және өзге де операциялардың жекелеген түрлеріне шектеулер енгізу туралы» Қазақстан Республикасының 2013 жылғы 25 желтоқсандағы No 292 қаулысы.

7. Саясатқа өзгерістер енгізу тәртібі

70. Осы Саясатқа өзгерістер мен толықтырулар енгізу жөніндегі ұсыныстарды МҚҰ-ның кез келген қызметкері МҚҰ директорына жазбаша түрде ұсыну арқылы бастамашылық етуі мүмкін.

71. Осы Саясатқа өзгерістер мен толықтырулар Қазақстан Республикасының заңнамасына өзгерістер енгізілуге және қажет болған жағдайда енгізілуге тиіс.