"БЕКІТІЛГЕН"
"ҒіпҒіх" МҚҰ" ЖШС
Жалғыз қатысушының шешімімен
№ 05-17 Бұйрық
"01" 07 2023 жыл

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

Алматы қ.

1.Жалпы ережелер

1.1 Осы ақпараттық қауіпсіздік және "Finfix" Микроқаржы ұйымы " ЖШС интернет-ресурсы (веб-сайт) арқылы қызмет көрсету кезінде ақпаратты рұқсатсыз қол жеткізуден қорғау Саясаты (бұдан әрі- Саясат) Қазақстан Республикасының ақпараттық қауіпсіздік саласындағы қолданыстағы заңнамасының талаптарына, уәкілетті мемлекеттік органның нормативтік актілеріне, сондай-ақ "FinFix "МҚҰ" ЖШС (бұдан әрі — МҚҰ) ішкі құжаттарына сәйкес әзірленді және ұсынымдық сипатта болады.

Пайдаланушыларға ақпараттық қауіпсіздікке, алаяқтыққа және басқа да оқиғаларға байланысты жағымсыз жағдайларды болдырмау үшін құжатпен танысу ұсынылады.

1.2. Осы Саясаттың мақсаты ақпараттық қауіпсіздікке қатер төндіретін инциденттердің залалын олардың алдын алу не салдарын қолайлы деңгейге дейін төмендету жолымен азайту болып табылады. Ақпараттық қауіпсіздікті қамтамасыз ету өз алдына мақсат болып табылмайды, бірақ тәуекелдерді басқару және МҚҰ-ның ақпараттық ресурстарына қатысты қауіп-қатерлермен байланысты ықтимал экономикалық шығындарды азайту жөніндегі қажетті шараны білдіреді.

2. Саясаттың негізгі принциптері

Осы Саясат мынадай негізгі қағидаттарға негізделеді:

- Заңдылық - ақпараттық қауіпсіздікті қамтамасыз етуге бағытталған барлық іс-әрекеттер Қазақстан Республикасының қолданыстағы заңнамасына қатаң сәйкес жүзеге асырылады. МҚҰ ақпаратын қорғау объектілеріне жағымсыз әсерлерді анықтау, алдын алу, оқшаулау және бейтараптандырудың заңда көзделген барлық әдістері қолданылады.

- Бизнес-ақпараттық қауіпсіздікке бағдарлану МҚҰ негізгі қызметін қолдау құралы ретінде қарастырылады. Қорғау шараларын іске асыру бизнес-процестердің жұмыс істеуіне айтарлықтай кедергі келтірмеуге тиіс.

- Үздіксіздік-ақпараттық қауіпсіздікті қамтамасыз ету ағымдағы бизнес-процестерді үзбей немесе тоқтатпай жүзеге асырылады. Барлық шаралар ұйымның күнделікті қызметіне біріктірілуі керек.

- Кешенділік - ақпаратты қорғау ақпараттық ресурстардың өмірлік циклінің барлық кезеңдерін, соның ішінде оларды құруды, өңдеуді, сақтауды, беруді және жоюды, сондай-ақ тиісті жүйелердің жұмыс істеуінің барлық режимдерін қамтиды.

- Негізділік және экономикалық орындылық-пайдаланылатын қорғау құралдары мен әдістері ғылым мен техниканың дамуының өзекті деңгейіне сәйкес келуі, экономикалық тұрғыдан негізделген және белгіленген тәуекел деңгейіне барабар болуы тиіс. Ақпараттық қауіпсіздік шараларын іске асыруға арналған шығындар тиісті қатерлерді іске асырудан болатын ықтимал залалдан аспауға тиіс.

- Басымдық - ақпараттық ресурстар олардың маңыздылығы мен сезімталдық дәрежесі бойынша сараланауға жатады. Бұл бар ресурстарды және ықтимал қауіптерді бағалауды ескере отырып, ең маңызды активтерді қорғауға бағыттауға мүмкіндік береді.

3. Саясаттың Мазмұны

Осы Саясат мыналарды белгілейді:

- қауіптерді азайту мен алдын алуды қоса алғанда, МҚҰ ақпараттық қауіпсіздігін қамтамасыз етудің негізгі шаралары;

- интернет-ресурс арқылы қарыз алушыларды екі факторлы аутентификациялау және верификациялау тәртібі;

- шарттық міндеттемелер аяқталғаннан кейін кемінде 5 жыл ішінде олардың тұтастығы мен құпиялылығын қамтамасыз ете отырып, электрондық хабарламалар мен құжаттарды қауіпсіз сақтау қағидалары;

- үшінші тұлғалар тарапынан мүмкін болатын құқыққа қарсы іс-қимылдардың алдын алу жөніндегі шаралар.

4. Саясаттың әрекет ету объектілері

Саясат мыналарға қолданылады:

- МҚҰ қызметкерлері, оның ішінде тағылымдамадан өтушілер мен практиканттар;

- МҚҰ ақпараттық жүйелеріне қолжетімділігі бар қарыз алушылар мен өзге де тұлғалар;

- шарттық негіздер бойынша МҚҰ-мен өзара іс-қимыл жасайтын контрагенттер мен серіктестер;

- МҚҰ ақпараттық ресурстары - деректер базасы, жүйелік құжаттама, басшылық, саясат және рәсімдер, соның ішінде құпия және жалпыға қолжетімді ақпарат.

5. Ақпараттық инфрақұрылым

Қорғаныс объектілеріне мыналар жатады:

-МҚҰ IT-жүйелері, ақпаратты өңдеу, сақтау, беру және көрсету құралдары;

- байланыс арналары, телекоммуникациялық жүйелер, ақпараттық тасымалдағыштар;

- техникалық және бағдарламалық қорғау құралдары;

- IT-инфрақұрылым элементтері орналасқан Үй-жайлар мен объектілер.

6. Осы Саясат жалпыға қолжетімді құжат болып табылады және МҚҰ https://kopaksha.kz/. **ресми Интернет-ресурсында орналастырылады.**

7. Ақпараттық қорғаудың сенімді жүйесін құру процесі

Ақпараттық қауіпсіздіктің сенімді жүйесін құру процесі аяқталған әрекет емес. Қорғаудың жеткілікті деңгейін ұстап тұру үшін жүйенің параметрлерін үнемі конфигурациялау, сондай-ақ оны сыртқы және ішкі ортада пайда болатын жаңа қауіптерге бейімдеу қажет.

8. Ақпараттық қауіпсіздікті қамтамасыз ету шаралары

8.1. МҚҰ ақпараттық қауіпсіздігін қамтамасыз етудің негізгі шаралары:

- әкімшілік-құқықтық және ұйымдастырушылық шаралар;
- физикалық қауіпсіздік шаралары;
- бағдарламалық-техникалық шаралар.

8.2. Әкімшілік-құқықтық және ұйымдастырушылық шаралар мыналарды қамтиды (бірақ олармен шектелмейді):

- ҚР заңнамасы мен ішкі нормативтік құжаттар талаптарының сақталуын бақылау;

- ақпараттық қауіпсіздік саясатын қолдайтын Қағидалардың, әдістемелер мен нұсқаулықтардың орындалуын әзірлеу, енгізу және бақылау;

- бизнес-процестердің саясат талаптарына сәйкестігін бақылау;
- ақпараттық жүйелермен жұмыс және ақпараттық қауіпсіздік талаптарын сақтау мәселелері бойынша МҚҰ қызметкерлерін ақпараттандыру және оқыту;
- инциденттерге ден қою, олардың салдарын оқшаулау және азайту;
- ақпараттық қауіпсіздік саласындағы жаңа тәуекелдерді талдау;
- ұжымдағы моральдық-іскерлік ахуалды мониторингілеу және жақсарту;
- төтенше жағдайлар туындаған жағдайда іс-қимыл тәртібін айқындау;
- қызметкерлерді жұмысқа қабылдау және жұмыстан шығару кезінде алдын алу іс-шараларын жүргізу.

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

- техникалық қауіпсіздік құралдарын пайдалануды қоса алғанда, күзетілетін объектілерді тәулік бойы күзетуді ұйымдастыру;

- күзетілетін объектілердің өртке қарсы қауіпсіздігін қамтамасыз ету;

- МҚҰ қызметкерлері мен үшінші тұлғалардың қолжетімділігі шектеулі үй-жайларға (мысалы, серверлік бөлмелер) кіруін бақылау.

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

- лицензияланған бағдарламалық қамтамасыз етуді және сертификатталған ақпаратты қорғау құралдарын пайдалану;

- периметрді қорғау құралдарын қолдану (брандмауэрлер және т. б.);

- кешенді антивирустық қорғауды қолдану;

- барлық қолданылатын бағдарламалау тілдерін қолдайтын статикалық талдау құралдарын қолдана отырып, бастапқы кодты, компоненттерді және кітапханаларды талдау;

- ақпараттық жүйелерде енгізілген ақпараттық қауіпсіздік құралдарын пайдалану;

- деректердің тұрақты сақтық көшірмесі;

- пайдаланушылардың, әсіресе артықшылықты пайдаланушылардың қол жеткізу құқықтары мен әрекеттерін бақылау; - ақпаратты криптографиялық қорғау жүйелерін қолдану; - аппараттық құралдардың үздіксіз жұмысын қамтамасыз ету.

9. Ақпараттық қауіпсіздік тәуекелдерін бағалау

9.1 Микроқаржы ұйымы (МҚҰ) ақпараттық қауіпсіздік тәуекелдерін бағалау үшін мынадай іс-шаралар жүргізеді:

- маңызды ақпараттық активтер тізбесін қалыптастыру;

- маңызды ақпараттық активтер үшін ақпараттық қауіпсіздік тәуекелдерін бағалау.

9.2. Сыни ақпараттық активтер тізбесіне тұтастығы немесе қолжетімділігі ақпараттық қауіпсіздік инциденттерімен байланысты шығындардың маңыздылығының белгіленген деңгейінен асатын құпиялылықты бұзудан болған залалдар енгізіледі.

9.3. Маңызды ақпараттық активтерге қатысты ақпараттық қауіпсіздік тәуекелдеріне бағалау жүргізу мақсатында МҚҰ мынадай процестердің іске асырылуын қамтамасыз етеді:

- ақпараттық қауіпсіздік қатерлерін сәйкестендіру;

- әрбір маңызды активке сәйкес келетін қауіп көздерін анықтау;

- маңызды ақпараттық активтердің осалдығын анықтау;

- ақпараттық қауіпсіздік тәуекелдерін басқарудың қолданыстағы шараларын талдау;

- тиісті көздер тарапынан қауіптерді іске асыру ықтималдығын бағалау;

- ақпараттық қауіпсіздік тәуекелдерінің жалпы деңгейін бағалау.

9.4. Маңызды ақпараттық активтерге қатысты ақпараттық қауіпсіздік қатерлерін сәйкестендіруді ақпараттық қауіпсіздік бөлімшесі жүзеге асырады. Әрбір осындай актив үшін ықтимал қауіптерге талдау жасалады.

9.5. Қауіптердің тиісті көздерін сәйкестендіруді белгілі және ықтимал қауіп көздерін ескере отырып, ақпараттық қауіпсіздік бөлімшесі де жүзеге асырады.

9.6. Маңызды ақпараттық активтердің осалдығын анықтауды МҚҰ ақпараттық қауіпсіздік жөніндегі бөлімшесі мынадай ақпаратты ескере отырып жүргізеді:

- ақпараттық активтің конструктивтік ерекшеліктері;

- активтің физикалық орналасуы;

- бағдарламалық жасақтамадағы белгілі қателер;

- конфигурация қателері;

- активті пайдалану процесіндегі кемшіліктер

9.7. Тәуекелдерді басқарудың қолданыстағы шараларын сәйкестендіруді осалдықтарды жоюға және ықтимал инциденттердің салдарын барынша азайтуға бағытталған ұйымдастырушылық және техникалық іс-шараларды ескере отырып, ақпараттық қауіпсіздік жөніндегі бөлімше жүзеге асырады.

9.8. Маңызды ақпараттық активтерге қатысты ақпараттық қауіпсіздікке төнетін қатерлерді іске асыру ықтималдығын бағалауды ақпараттық қауіпсіздік жөніндегі бөлімше жүзеге асырады. Талдау барлық тиісті комбинациялар үшін жүргізіледі: қауіп көзі – қауіп-осалдық, келесі ақпаратты ескере отырып:

- маңызды ақпараттық активке (ішкі немесе сыртқы) қатысты қауіп көзінің орналасуы туралы деректер. Ішкі көздер үшін активке қол жеткізе алатын пайдаланушылар саны ескеріледі; сыртқы көздер үшін-қорғау периметрінің сыртынан қашықтан қол жеткізу мүмкіндігі;

- қауіп көзі қол жеткізу деңгейі;

- өткенде осындай қауіптерді іске асыру жиілігі туралы статистикалық деректер;

- осы актив үшін нақты қатерді іске асырудың күрделілігі туралы ақпарат;

- қаралып отырған ақпараттық активке қатысты іске асырылған қорғау шараларының болуы.

9.9. Қатерді іске асыру ықтималдығын бағалауға және әртүрлі бағаларды алуға бірнеше сарапшыларды тартқан жағдайда, қорытынды (жалпыланған) бағалау ұсынылғандардың ең үлкеніне тең, яғни қатерді іске асырудың ең жоғары ықтималдығын көрсететін болып қабылданады.

9.10. Ақпараттық қауіпсіздік тәуекелдерінің деңгейін бағалау салыстыру арқылы жүзеге асырылады:

- қауіп-қатер көздері тарапынан маңызды ақпараттық активтерге төнетін қатерлерді іске асыру ықтималдығын бағалау,

- және осы активтердің құпиялылығын, тұтастығын немесе қол жетімділігін бұзумен байланысты ықтимал шығындарды бағалау.

10. Автоматтандырылған ақпараттық жүйеге қойылатын талаптар

10.1. Автоматтандырылған ақпараттық жүйе мыналарды қамтиды:

- веб-қосымшалар серверлерін бағдарламалық қамтамасыз ету (бұдан әрі-веб-қосымша);

- бағдарламалық интерфейс серверлерін бағдарламалық қамтамасыз ету (бұдан әрі-серверлік БПҰ).

10.2. Автоматтандырылған ақпараттық жүйені әзірлеуді және/немесе пысықтауды МҚҰ әзірлеу тәртібін, кезеңдерін және қатысушылар құрамын регламенттейтін ішкі құжатқа сәйкес жүзеге асырады.

10.3. МҚҰ-да әзірленетін автоматтандырылған ақпараттық жүйенің бастапқы кодтарын сақтау резервтік көшірмені міндетті түрде қамтамасыз ете отырып, МҚҰ қорғау периметрі ішінде орналастырылған код репозиторийлерін басқарудың мамандандырылған жүйелерінде жүзеге асырылады.

10.4. Әзірлеудің міндетті кезеңі қауіпсіздікті тестілеу болып табылады, оның шеңберінде кем дегенде мынадай іс-шаралар өткізіледі:

- бастапқы кодты статикалық талдау;

- компоненттер мен үшінші тарап кітапханаларын талдау.

10.5 Бастапқы кодты статикалық талдау талданатын бағдарламалық жасақтамада қолданылатын барлық бағдарламалау тілдерін қолдайтын мамандандырылған сканердің көмегімен жүзеге асырылады. Сканер келесі осалдықтарды анықтауы керек:

- зиянды кодты енгізуге мүмкіндік беретін механизмдердің болуы;

- бағдарламалау тілдерінің осал операторлары мен функцияларын пайдалану;

- әлсіз немесе осал криптографиялық алгоритмдерді қолдану;

- қызмет көрсетуден бас тартуға немесе қосымшаның жұмысын баяулатуға әкелетін кодтың болуы; - қолданбаны қорғау механизмдерін айналып өту мүмкіндігі;

- құпияларды (құпия сөздерді, кілттерді және т. б.) ашық түрде пайдалану;

- қауіпсіз даму үлгілері мен тәжірибелерін сақтамау.

10.6. Компоненттер мен үшінші тарап кітапханаларын талдау қолданылатын нұсқалардағы белгілі осалдықтарды анықтау, сондай-ақ олардың тәуелділіктерін бақылау мақсатында жүзеге асырылады.

10.7. МҚҰ ішкі регламентке сәйкес анықталған осалдықтарды жоюға міндеттенеді. Бұл ретте аса маңызды осалдықтар автоматтандырылған ақпараттық жүйе (немесе оның жаңа нұсқалары) пайдалануға берілгенге дейін жойылады.

10.8. МҚҰ оларға жедел қол жеткізу мүмкіндігімен соңғы үш (3) жылда пайдалануға енгізілген автоматтандырылған ақпараттық жүйенің қауіпсіздігін тестілеудің бастапқы кодтары мен нәтижелерінің барлық нұсқаларын сақтауды қамтамасыз етеді.

10.9. Автоматтандырылған ақпараттық жүйенің клиенттік және серверлік тараптары арасында деректерді беру transport Layer Security (TLS) протоколының 1.2-ден төмен емес нұсқасын пайдалана отырып шифрланады.

10.10. Веб-бағдарлама мыналарды қамтамасыз етуі керек:

- МҚҰ тиесілілігін біржақты сәйкестендіру (домендік атауы, логотипі, фирмалық түстері);

- браузерде авторизациялық деректерді сақтауға тыйым салу;

- енгізілген құпия деректерді жасыру (мысалы, парольдер);

- пайдаланушыны киберқауіпсіздік ережелері туралы авторизация бетінде хабардар ету;

- қателерді қауіпсіз өңдеу-құпия ақпаратты көрсетпей, ең аз қажетті қате сипаттамасын бере отырып.

10.11. Серверлік БПҰ жағындағы МҚҰ мыналарды қамтамасыз етеді:

- қателер мен ерекшеліктерді қауіпсіз өңдеу-құпия ақпаратты ашпай, диагностика мүмкіндігімен;

- пайдаланушылар мен құрылғыларды сәйкестендіру және аутентификациялау;

- инъекциялар мен жалған сұрау шабуылдарының алдын алу үшін кірістердің жарамдылығын тексеру.

10.12. Автоматтандырылған ақпараттық жүйеде ақпаратқа қол жеткізу МҚҰ қызметкерлеріне қызметтік міндеттерін орындау үшін қажетті шектерде МҚҰ қызметкерлерін сәйкестендіру және аутентификациялау рәсімдерін пайдалана отырып беріледі.

10.13. Жүйеде есептік жазбалар мен парольдерді басқару, сондай-ақ МҚҰ ішкі құжаттарына сәйкес есептік жазбаларды бұғаттау функциялары іске асырылады.

10.14. Автоматтандырылған ақпараттық жүйе жаңартуларды, оның ішінде қауіпсіздік бойынша ұсынуды қамтитын техникалық қолдаумен сүйемелденеді.

10.15. Жүйе жұмыс істейтін көшірмені қалпына келтіру үшін қажетті деректердің, файлдардың және параметрлердің тұрақты сақтық көшірмесін жасайды.

10.16. МҚҰ-да ұйымдастырушылық және техникалық деңгейде автоматтандырылған ақпараттық жүйенің аудиторлық ізін жүргізу және қорғау қамтамасыз етіледі.

10.17. Жүйені қорғау үшін лицензияланған антивирустық бағдарламалық жасақтама немесе жұмыс станцияларында, ноутбуктерде және мобильді құрылғыларда бағдарламалық ортаның тұтастығын бақылау шешімдері қолданылады.

10.18. МҚҰ микрокредит шарты бойынша міндеттемелер аяқталғаннан кейін кемінде бес (5) жыл бойы олардың тұтастығы мен құпиялылығын сақтай отырып, клиентке берілген және одан алынған электрондық хабарламалар мен өзге де құжаттардың қауіпсіз сақталуын қамтамасыз етеді. Құжаттар қалыптастырылған, жіберілген немесе алынған түрінде сақталады.

11. Электрондық хабарламалар мен өзге де құжаттарды қауіпсіз сақтау

11.1. МҚҰ ақпараттық қауіпсіздігін қамтамасыз ету мақсатында мынадай шарттар орындалады:

- ақпараттық қауіпсіздікті басқару жүйесін ұйымдастыру;

- ақпараттық активтерге қолжетімділікті ұйымдастыру;

- ақпараттық инфрақұрылымның қауіпсіздігін қамтамасыз ету;

- ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қызметке мониторинг жүргізу, қатерлерді анықтау және талдау, шабуылдарға қарсы іс-қимыл, инциденттерді тергеу;

- ақпараттық жүйелердегі бұзушылықтар мен іркілістер туралы деректерді қоса алғанда, ақпараттық қауіпсіздік инциденттері туралы ақпаратты талдау;

- ақпаратты криптографиялық қорғау құралдарын пайдалану;

- үшінші тұлғалардың ақпараттық активтерге қол жеткізуі кезінде ақпараттық қауіпсіздікті қамтамасыз ету;

- ақпараттық қауіпсіздіктің жай-күйіне ішкі тексерулер жүргізу; - ақпараттық қауіпсіздікті басқару жүйесінің процестерін іске асыру.

11.2. Қорғалатын ақпарат мүмкін:

- қағаз жеткізгіштерде орналастырылады;

- электронды түрде бар болуы (өңдеу, беру, есептеу техникасы құралдарын қолдана отырып сақтау, техникалық құралдардың көмегімен жазу және көбейту);

- телефон байланысы, факс, телекс және басқа байланыс құралдары арқылы электр сигналдары түрінде беріледі;

- ауа ортасында және қоршау конструкцияларында акустикалық және діріл сигналдары түрінде қабылданады (мысалы, жиналыстар мен келіссөздер кезінде).

11.3. Әлеуетті қарыз алушылар туралы мәліметтерді (кірістер, МӘСҚ аударымдары, зейнетақы төлемдері, кредиттік есептер және т. б. туралы деректерді қоса алғанда) беруге арналған шарттар бойынша кредиттік бюромен (КБ) өзара іс-қимыл жасау кезінде ақпараттық қауіпсіздікті қамтамасыз ету бөлігінде МҚҰ мынадай талаптарды басшылыққа алады:

11.3.1. МҚҰ КБ ақпараттық жүйесінен алынған ақпараттың құпиялылығы мен тұтастығын қамтамасыз етеді.

11.3.2. МҚҰ КБ-мен жасалған шарттарға сәйкес ақпараттық қауіпсіздік шарттарын сақтайды.

11.3.3. МҚҰ КБ ақпараттық жүйесімен өзара іс-қимыл жасау кезінде пайдаланылатын бағдарламалық қамтамасыз етудің жұмыс істеуі мен қорғалуы үшін қажетті ұйымдастыру-техникалық және технологиялық шараларды іске асырады.

11.3.4. КБ жүйесімен жұмыс істеу үшін қолданылатын жабдық рұқсатсыз кіруден қорғалуы тиіс. Сондай-ақ пайдаланылатын ақпарат тасығыштар мен желілік ресурстарды қорғау қамтамасыз етіледі.

11.3.5. МҚҰ КБ ақпараттық жүйесімен өзара іс-қимылға қатысатын жауапты тұлғалардың тізбесін айқындайды және бекітеді.

11.3.6. Жауапты тұлғалар өз міндеттерін орындау барысында өздеріне белгілі болған ақпаратты жария етпеу және таратпау туралы міндеттемелерге қол қояды.

11.3.7. МҚҰ жауапты тұлғаларды тағайындау тәртібін, олардың құқықтарын, міндеттері мен жауапкершілігін (оның ішінде лауазымдық нұсқаулықтар арқылы) белгілейтін ішкі құжаттарды әзірлейді және бекітеді.

11.3.8. Ақпаратқа қолжетімділік МҚҰ қызметкерлеріне олардың функционалдық міндеттерін орындау үшін қажетті көлемде беріледі.

11.3.9. КБ ақпараттық жүйесіндегі есептік жазба нақты жеке тұлғаға байланысты.

11.3.10. МҚҰ жұмыс станциялары мен сайттың осы ақпараттық қауіпсіздік саясатының талаптарына сәйкестігіне жоспарлы және жоспардан тыс тексерулер жүргізеді.

11.3.11. Уәкілетті органның сұрау салуы бойынша МҚҰ КБ-мен шарттарда көзделген талаптардың сақталуын растайтын мәліметтерді ұсынады.

11.3.12. Жұмыс станциясының операциялық жүйесі:

- пайдаланушыны сәйкестендіру және аутентификациялау;

- пайдаланушылардың қол жеткізу құқықтарының аражігін ажырату;

- белгіленген құқықтарға сәйкес авторизациялау.

11.3.13. КБ ақпараттық жүйесімен өзара іс-қимыл жасау үшін МҚҰ-ға тиесілі жұмыс станциясы ғана пайдаланылады.

11.3.14. КБ жүйесіне қосылған кезде басқа интернет-ресурстарға бір мезгілде қол жеткізуге жол берілмейді.

11.3.15. МҚҰ қызметкерлері ақпараттық жүйелерге қол жеткізу кезінде пайдаланылатын дербес сәйкестендіру және аутентификация деректерінің құпиялылығын қамтамасыз етуге міндетті.

11.3.16. МҚҰ қызметкерлері КБ ақпараттық жүйесімен жұмыс барысында алынған ақпараттың құпиялылығын сақтауға міндетті.

11.4. Ақпараттық қауіпсіздікті қамтамасыз ету үшін жауапкершілік МҚҰ-ның барлық құрылымдық бөлімшелеріне олардың өкілеттіктері шеңберінде және осы Саясатқа және байланысты ішкі құжаттарға сәйкес жүктеледі.

11.5. Осы Саясаттың және онымен байланысты құжаттардың талаптарын бұзғаны үшін МҚҰ-ның ішкі нормативтік актілеріне және Республиканың қолданыстағы заңнамасына сәйкес жауапкершілік көзделген.

12.Ақпараттық қауіпсіздікті бұзудың алдын алу шаралары

12.1. Киберқауіпсіздік оқиғаларының алдын алуда бағдарламалық қамтамасыз етуді әзірлеу, Ақпараттық жүйелер компоненттерін және қаржы секторының инфрақұрылымын жобалау кезінде ұлттық және халықаралық талаптарды сақтау маңызды рөл атқарады. МҚҰ киберқауіпсіздік тәуекелдерін тұрақты бағалауды жүргізеді, ол оларды барынша азайту жөніндегі шараларды әзірлеу және енгізу, сондай-ақ іске асырылған қорғау шараларының тиімділігін бағалау үшін негіз болады.

12.2. Алдын алу (алдын алу) кезеңінде алынған нәтижелер, сондай-ақ болған оқиғаларды өңдеу тәжірибесі ескеріледі. Киберқауіпсіздік оқиғаларының сипатын, ауқымын және салдарын уақтылы бағалау жүргізіледі. Салдарын азайту мақсатында:

- мүдделі тараптарды жедел хабардар ету жүзеге асырылады;

- әрекет ету бойынша іс-қимылдар үйлестіріледі.

Мүдделі тараптарға мыналар жатады:

- Қазақстан Республикасының Ұлттық Банкі;

- өзге де уәкілетті мемлекеттік және заң шығарушы органдар;

- қарыз алушылар;

- несие берушілер мен инвесторлар;

- МҚҰ құрылымдық бөлімшелерінің қызметкерлері;

- қызмет көрсетушілер.

12.3. Оқиғадан кейін қалпына келтіру рәсімдерін орындаумен қатар МҚҰ операциялық қызметінің үздіксіздігі қамтамасыз етіледі, соның ішінде:

- оқиғаның салдарын жою;

- ақпараттық жүйелер мен деректердің дұрыстығын растай отырып, олардың қалыпты жұмыс істеуін қалпына келтіру;

- қайталанған оқиғалардың алдын алу үшін оқиға барысында пайдаланылған осалдықтарды анықтау және жою;

- ел ішінде және қажет болған жағдайда одан тыс жерлерде ақпараттық өзара іс-қимылды ұйымдастыру.

12.4. Пайдаланушылардың хабардарлығын және МҚҰ қызметкерлерінің біліктілігін арттыру тәуекелдерді азайтуға және ақпараттық қауіпсіздік мәдениетін қалыптастыруға ықпал етеді. Оқыту іс-шараларының бір бөлігі ретінде қызметкерлер өзекті қауіптер мен олардың алдын алу әдістерін түсінуі үшін алдын алу мен әрекет етудің нақты тәжірибесін пайдалану керек.

12.5. Ақпараттық қауіпсіздіктің классикалық моделі келесі атрибуттарды қамтамасыз етуге негізделген:

- қолжетімділік-уәкілетті тұлғалар үшін ақпаратқа уақтылы және кедергісіз қол жеткізу мүмкіндігін қамтамасыз ету;

- құпиялылық-тиісті өкілеттіктері бар адамдар үшін ғана ақпаратқа қол жеткізуді шектеу, сондай-ақ оның рұқсат етілмеген субъектілерге ашылуына жол бермеу;

- тұтастық-ақпараттың бұрмалануын немесе рұқсатсыз өзгеруін болдырмайтын өзгермейтін және сенімді түрде сақталуы.

12.6. Рұқсат етілмеген қолжетімділік, микрокредит беруге байланысты ақпараттың өзгеруі немесе үшінші тұлғалар тарапынан өзге де заңсыз әрекеттер анықталған жағдайда, МҚҰ:

- себептер мен салдарларды жою бойынша дереу шаралар қабылдайды;

- бір жұмыс күні ішінде бұл туралы уәкілетті мемлекеттік органға хабарлайды.

12.7. МҚҰ өзінің сервистері мен микрокредиттеу технологияларын мақсатта пайдалануға жол бермеу жөнінде шаралар қабылдайды:

- қылмыстық жолмен алынған кірістерді заңдастыру (жылыстату) ;

- терроризмді қаржыландыру. Микрокредиттер беру және қарыз алушыларға скоринг жүргізу кезінде МҚҰ басшылыққа алады:

- "Қылмыстық жолмен алынған кірістерді заңдастыруға (жылыстатуға) және терроризмді қаржыландыруға қарсы іс-қимыл туралы" 2009 жылғы 28 тамыздағы Қазақстан Республикасының Заңымен (ПОДФТ туралы Заң);

13. Саясатқа өзгерістер енгізу тәртібі

13.1. Осы Саясатқа өзгерістер мен толықтырулар енгізу жөніндегі ұсыныстарға МҚҰ директорына жазбаша өтініш беру арқылы МҚҰ-ның кез келген қызметкері бастамашылық жасай алады.

13.2. Саясатқа өзгерістер мен толықтырулар енгізіледі:

- Қазақстан Республикасының заңнамасына өзгерістер енгізу кезінде;

- қажеттілігіне қарай, сәйкессіздіктер, олқылықтар анықталған немесе ережелерді өзектендіру қажет болған жағдайда.