«Jusan Bank» АҚ
ақпараттық қауіпсіздік
САЯСАТЫ

"Jusan Bank" АҚ (бұдан әрі-Банк) ақпараттық қауіпсіздікті қамтамасыз ету мәселелеріне ерекше назар аударады, ақпараттық қауіпсіздікті басқару жүйесін, ақпараттық қауіпсіздікке төнетін қатерлерден қорғаудың қолданылатын құралдары мен тәсілдерін ұдайы жетілдіреді, сондай-ақ ақпаратты қорғау саласындағы құзыретті жоғары деңгейде ұстап тұру үшін Банк қызметкерлерін үздіксіз оқытуды қамтамасыз етеді.

Осы құжат Қазақстан Республикасының заңнамасына, Payment Card Dustry Data Security Standard талаптарына сәйкес әзірленген және Банктің корпоративтік веб-сайтында ашық жариялауға арналған.

Құжат ақпарат қауіпсіздігін қамтамасыз ету мәселелеріне көзқарастар жүйесін, ақпаратты қорғау жөніндегі негізгі қағидаттарды, бағыттар мен талаптарды сипаттайды және Банк Басқармасы бекіткен ақпараттық қауіпсіздік Саясатының (бұдан әрі - Саясат) негізгі бөлімдерін қамтиды.

Саясат иесі және пайдаланушысы Банк болып табылатын барлық ақпараттық активтерді/ресурстарды, ақпаратты және құжаттарды қамтиды.

Ақпараттық қауіпсіздікті қамтамасыз ету – Банктің коммерциялық қызметін табысты жүзеге асырудың қажетті шарты. Ақпарат ең маңызды банк активтерінің бірі болып табылады.

Саясаттың ережелері арқылы қол жеткізу үшін бағытталған негізгі мақсат Банктің ақпараттық ресурстарын тиісінше қорғауды қамтамасыз ету, ақпараттық қауіпсіздік тәуекелдерін және Банктің ақпараттық ресурстарының қауіпсіздігіне қатер төндіретін оқиғалардан болатын залалды/зиянды болдырмау немесе олардың салдарын барынша азайту болып табылады.

Ақпараттық қауіпсіздік өз алдына мақсат болып табылмайды, оны қамтамасыз ету Банктің стратегиялық мақсаттарына қол жеткізу барысында ақпараттық ресурстарға төнетін қауіптердің барлық түрлерімен байланысты тәуекелдер мен экономикалық шығындарды азайту үшін қажет.

Осы мақсатта ақпараттың негізгі қасиеттерін сақтау қажет, атап айтқанда:

1) қолжетімділік – ақпараттың авторланған субъектінің сұранысы бойынша қолжетімді және пайдалануға дайын болу қасиеті;

2) құпиялылық - ақпараттың объектінің рұқсат етілмеген тұлғалары үшін қолжетімсіз және жабық болу қасиеті;

3) тұтастық - деректердің өзгермеу күйі.

Сенімді ақпараттық қорғауды құру процесі үздіксіз болып табылады.

Банктің ақпараттық қауіпсіздігін қамтамасыз ету жүйесін құру және оның жұмыс істеуі мынадай негізгі қағидаттарға сәйкес жүзеге асырылуы тиіс:

1) заңдылық-ақпараттық қауіпсіздікті қамтамасыз ету үшін қабылданатын кез келген іс-әрекеттер Банктің ақпараттық ресурстарына және ақпараттық қауіпсіздікті қамтамасыз етудің өзге де объектілеріне заңсыз, рұқсатсыз және өзге де теріс әсерлерді анықтау, алдын алу, оқшаулау және жолын кесу үшін барлық рұқсат етілген шараларды, тәсілдер мен әдістерді қолдана отырып, Қазақстан Республикасының қолданыстағы заңнамасына негізделеді;

2) бизнеске бағдарлану - ақпараттық қауіпсіздік Банктің негізгі қызметін қолдау процесі ретінде қарастырылады; ақпараттық қауіпсіздікті қамтамасыз ету бойынша қабылданып жатқан шаралар Банк қызметі үшін елеулі кедергілерге әкеп соқтырмауы тиіс;

3) үздіксіздік - ақпаратты қорғау жүйелерін басқару құралдарын қолдану, ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі кез келген іс-шараларды іске асыру Банктің ағымдағы бизнес-процестерін үзбей немесе тоқтатпай жүзеге асырылады;

4) кешенділік - ақпараттық ресурстардың ақпараттық қауіпсіздігін олардың бүкіл өмірлік циклі барысында, барлық технологиялық ресурстар мен оларды пайдалану кезеңдерінде және жұмыс істеудің барлық режимдерінде қамтамасыз ету;

5) негізділік - пайдаланылатын мүмкіндіктер мен қорғау құралдары тиісті және жеткілікті деңгейде іске асырылады, қауіпсіздіктің белгіленген деңгейі тұрғысынан негізделген және қойылатын талаптар мен нормаларға сәйкес келеді;

6) басымдықтар - Банктің барлық ақпараттық ресурстарын олардың мәртебесі мен маңыздылық дәрежесі бойынша санаттау (саралау);

7) артықшылықтардың ең төменгі деңгейі-пайдаланушы (Банк қызметкері) артықшылықтардың ең төменгі деңгейін алады және өзінің функционалдық міндеттері шеңберінде қызметін орындау үшін қажетті болып табылатын Банк деректеріне, ақпараттық жүйелері мен жабдықтарына ғана қол жеткізеді;

8) мамандандыру - техникалық құралдарды пайдалануды Банктің кәсіби дайындалған қызметкерлері жүзеге асырады;

9) барлық деңгейдегі бөлімшелердің басшылары мен орындаушылар ақпараттық қауіпсіздіктің барлық талаптары туралы хабардар болады және осы талаптарды орындамағаны және ақпараттық қауіпсіздіктің белгіленген шараларын сақтамағаны үшін дербес жауапты болады;

10) өзара іс- қимыл және үйлестіру - ақпараттық қауіпсіздік шаралары Банктің тиісті құрылымдық бөлімшелерінің өзара байланысы, қойылған мақсаттарға қол жеткізу үшін олардың күш-жігерін үйлестіру, сондай-ақ сыртқы ұйымдармен, кәсіптік қауымдастықтармен және бірлестіктермен, мемлекеттік органдармен, заңды және жеке тұлғалармен қажетті байланыстар орнату негізінде жүзеге асырылады;

11) растау – маңызды құжаттама және барлық жазбалар-ақпараттық қауіпсіздік талаптарының орындалуын және оны ұйымдастыру жүйесінің тиімділігін растайтын құжаттар жедел қол жеткізу және қалпына келтіру мүмкіндігімен жасалады және сақталады;

12) қорғаудың эшелондылығы - ақпараттық активті рұқсатсыз кіруден қорғауға, шабуылдарды анықтауға және оларға ден қоюға арналған, сол арқылы оқиғаның туындау қаупін төмендетуге арналған, бір-бірінің функционалын толықтыратын әртүрлі қорғау тетіктерінің кешені.

Банктегі ақпараттық қауіпсіздікті қамтамасыз етудің негізгі объектілері:

1) Қазақстан Республикасының заңнамасына және Банктің ішкі құжаттарына сәйкес банктік коммерциялық немесе заңмен қорғалатын өзге де құпияға, дербес деректерге, инсайдерлік ақпаратқа жатқызылған мәліметтерді қамтитын ақпараттық ресурстар (бұдан әрі-қорғалатын ақпарат);

2) қорғалатын ақпаратты өңдеу, беру және сақтау жүргізілетін ақпараттандыру құралдары мен жүйелері (есептеуіш техника құралдары, ақпараттық-коммуникациялық инфрақұрылым, желілер, жүйелер);

3) қорғалатын ақпаратты өңдеу, беру және сақтау жүргізілетін банктің бағдарламалық құралдары (операциялық жүйелер, деректер базасын басқару жүйелері, басқа да жалпы жүйелік және қолданбалы бағдарламалық қамтамасыз ету);

4) ақпараттық ресурстарды басқаруға және пайдалануға байланысты банктің бизнес-процестері;

5) қорғалатын ақпаратты жасау, өңдеу, беру және сақтау құралдары орналасқан жайлар;

6) Банк қызметкерлерінің жұмыс жайлары мен кабинеттері, жабық келіссөздер мен кеңестер жүргізуге арналған Банк жайлары;

7) қорғалатын ақпаратқа қолжетімділігі бар Банк қызметкерлері;

8) ашық ақпаратты өңдейтін, бірақ қорғалатын ақпарат өңделетін жайларда орналастырылған техникалық құралдар мен жүйелер.

Қорғауға жататын ақпарат түрлері:

1) қағаз тасымалдағыштарда;

2) электрондық түрде (есептеуіш техника құралдарымен өңделетін, берілетін, техникалық құралдардың көмегімен жазылатын, сақталатын және жаңғыртылатын және т. б.).

Саясаттың ережелерін Банктің барлық қызметкерлері, тағылымдамашылар, практиканттар орындау үшін міндетті, сондай-ақ Банктегі қызметімен тікелей байланысты бөлігінде, клиенттердің және Банктің ақпараттық активтеріне қол жеткізе алатын өзге де үшінші тұлғалардың назарына жеткізілуі тиіс.