centercredit

# Политика
# информационной безопасности
# АО «Банк ЦентрКредит»

**Басқарманың**
**21.12.2021 ж. № 3-1221-03**
**шешімімен мақұлданған**

**Директорлар кеңесінің**
**13.01.2022 ж. № 3-0113-01**
**қаулысымен бекітілген**

На русском языке

# «Банк ЦентрКредит» АҚ-тың Ақпараттық қауіпсіздік саясаты

**Мазмұны:**



## 1. Жалпы қағидалар

1. Осы Ақпараттық қауіпсіздік саясаты (бұдан әрі – Саясат) Банктің ақпараттық қауіпсіздікті басқару жүйесінің (бұдан әрі – АҚБЖ) мақсаттарын, міндеттерін және іс-әрекет ету саласын айқындайтын, «Банк ЦентрКредит» АҚ-тың (бұдан әрі – Банк) ақпараттық қауіпсіздікті басқару жүйесінің негізін қалайтын құжат болып табылады.

2. Банк ақпараттық қауіпсіздікті қамтамасыз ету процесін басқаруға арналған, Банктің жалпы басқару жүйесінің бөлігі болып табылатын АҚБЖ құруды және оның қызмет етуін қамтамасыз етеді.

3. АҚБЖ банктің бизнес-процесі үшін ықтимал залалдың ең төменгі деңгейіне жол беретін Банктің ақпараттық активтерін қорғауды қамтамасыз етеді.

4. Саясат Қазақстан Республикасының заңнамасына, соның ішінде екінші деңгейдегі банктердің ақпараттық қауіпсіздігін қамтамасыз ету талаптарын реттейтін нормативтік құқықтық актілерге, сонымен қатар ақпараттық қауіпсіздік саласындағы халықаралық стандарттардың талаптарына сәйкес әзірленген.

5. Банктің ақпараттық қауіпсіздігін басқару жүйесінің процестеріне қойылатын және осы Саясатта сипатталған талаптар «Банктердің, Қазақстан Республикасының бейрезидент-банктері филиалдарының және банк операцияларының жекелеген түрлерін жүзеге асыратын ұйымдардың ақпараттық қауіпсіздігін қамтамасыз етуге қойылатын талаптарды, Ақпараттық жүйелердегі бұзушылықтар, іркілістер туралы мәліметтерді қоса алғанда, ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты беру қағидалары мен мерзімдерін бекіту туралы» Қазақстан Республикасы Ұлттық Банкі Басқармасының 2018 жылғы 27 наурыздағы №48 қаулысының «Ақпараттық қауіпсіздікті басқару жүйесінің процестеріне қойылатын талаптар» атты 11-бөліміне сәйкес әзірленген Банктің ішкі нормативтік құжаттарында толық сипатталған.

## 2. Ақпараттық қауіпсіздікті басқару жүйесінің мақсаттары, міндеттері және негізгі принциптері

6. АҚБЖ мақсаты – ақпараттық қауіпсіздікті қамтамасыз ету процесін арттыру, конфиденциалдылықтың талап етілген деңгейін қамтамасыз ету, маңызды ақпараттық активтердің тұтастығы және қолжетімділігі және салдарынан ақпараттық қауіпсіздік тәуекелдерін және оған байланысты залалды азайту.

7. АҚБЖ міндеттеріне төмендегілер жатады:

1) ақпараттық активтерді санатқа бөлу;

2) ақпараттық активтерді пайдалану құқығын беруді ұйымдастыруды;

3) ақпараттық инфрақұрылымның қауіпсіздігін қамтамасыз ету;

4) ақпараттық қауіпсіздікті және ақпараттық қауіпсіздіктің оқыс оқиғалары бойынша қауіп пен осалдықты анықтау және талдау, қақтығыстарға қарсы тұру және тергеу бойынша іс-шараларды қамтамасыз етуге қатысты қызметке мониторинг жүргізу;

5) ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты, оған қоса ақпараттық жүйелердегі бұзылулар, ақаулар туралы мәліметтерді талдау;

6) ақпаратты криптографиялық қорғау құралдарын басқару тәртібін белгілеу;

7) үшінші тұлғалар ақпараттық активтерді пайдаланған кезде ақпараттық қауіпсіздікті қамтамасыз ету;

8) ақпараттық қауіпсіздіктің жай-күйіне ішкі тексерулер жүргізу.

8. АҚБЖ құру және оның қызмет етуі келесі негізгі принциптерге сәйкес жүзеге асырылады:

1) заңдылық – ақпараттық қауіпсіздікті қамтамасыз ету үшін қабылданатын кез келген іс-әрекеттер қолданыстағы заңнаманың негізінде, заң рұқсат ететін Банктің ақпараттық активтеріне теріс әсер ететін жағдайларды анықтау, олардың алдын алу, оқшаулау және жою әдістерін қолдану арқылы жүзеге асырылады;

2) бизнеске бағдарлау – ақпараттық қауіпсіздік негізгі қызметті қолдау процесі ретінде қаралады, ақпараттық қауіпсіздікті қамтамасыз ету бойынша кез келген шаралар бизнесті жүргізу үшін маңызды кедергілерге әкеп соқпауы тиіс;

3) кешенділік – барлық өмірлік циклі ішінде, оларды пайдаланудың барлық технологиялық кезеңдерінде және барлық қызмет ету режимінде ақпараттық активтердің қауіпсіздігін қамтамасыз ету;

4) негізділік және экономикалық мақсаттылық – пайдаланылатын мүмкіндіктер мен қорғаныс құралдары ғылым мен техниканың дамуының сәйкес кезеңінде іске асырылуы, белгіленген қауіпсіздік деңгейінің көзқарасымен негізделген болуы қажет және белгіленген талаптар мен нормаларға сәйкес келуі тиіс. Барлық жағдайда ақпараттық қауіпсіздікті қамтамасыз ету бойынша шаралар мен технологиялық шешімдердің құны қорғалатын ақпараттық активтердің құнынан аспауы қажет;

5) бейімділік – олардың маңыздылығына сәйкес ақпараттық активтерді қорғау әдістері мен құралдарын анықтау және қолдану;

6) қажетті білім мен артықшылықтың төмен деңгейі – пайдаланушы өз өкілеттіктері шегінде қызметін орындау үшін қажет болатын ақпараттық активтерге ғана артықшылықтардың ең төмен деңгейі мен пайдалану рұқсатын алады;

7) мамандану – ақпараттық қауіпсіздікті қамтамасыз ету бойынша шараларды іске асыруды және технологиялық шешімдерді пайдалануды кәсіби тұрғыда даярланған мамандар жүзеге асыруы қажет;

8) ақпараттылық және жауапкершілік – барлық деңгейдегі басшылар және орындаушылар ақпараттық қауіпсіздіктің барлық талаптары жөнінде хабардар болуы қажет және осы талаптарды орындау, сонымен қатар ақпараттық қауіпсіздіктің белгіленген шараларын сақтау үшін жеке жауап береді;

9) Бірлесіп әрекет ету және үйлестіру – ақпараттық қауіпсіздік шаралары Банктің сәйкес құрылымдық бөлімшелерінің бірлесіп әрекет етуі, алдыға қойылған мақсаттарға қолжеткізу үшін күшін үйлестіру, сонымен қатар сыртқы ұйымдармен, кәсіби қауымдастықтармен және қоғамдастықтармен, мемлекеттік органдармен, заңды және жеке тұлғалармен қажетті байланыс орнату негізінде жүзеге асырылады;

10) растау – ақпараттық қауіпсіздік және АҚБЖ тиімділігі бойынша талаптардың орындалуын растайтын куәліктер жедел қолжеткізу және қалпына келтіру мүмкіндігімен әзірленуі және сақталуы қажет.

## 3. Ақпараттық қауіпсіздікті басқару жүйесінің әрекет ету саласы

9. АҚБЖ қолданыс аймағы болып клиенттерге қызмет көрсетуге тікелей бағдарланған, клиенттер үшін құнды болып табылатын және пайда алуды қамтамасыз ететін, бизнес-процестердің жіктеуішін айқындайтын процедурада белгіленген Банктің негізгі бизнес-процестері танылады.

10. Қорғаныс объектілері болып негізгі бизнес-процестердің қызмет етуі үшін қажетті маңызды ақпараттық активтер танылады, оларға төмендегілер жатады:

1) Ақпаратты өңдеудің жеке құрылғылары;
2) Ақпаратты тасымалдағыш;
3) Сыртқы компьютерлік жабдық;
4) Серверлер;
5) Желілік жабдық;
6) Телефония аппаратурасы;
7) Жеке байланыс арнасы;
8) Деректер базасы;
9) Виртуалды байланыс арнасы;
10) Шолу жүйелері;
11) Операциялық жүйелер;
12) Аппараттық құрылғылардың бағдарламалық қамсыздандыруы;
13) Қолданбалы бағдарламалық қамсыздандыру;
14) Телефониялы бағдарламалық қамсыздандыруы.

## 4. Банктің ақпараттық жүйелерінде құрылатын, сақталатын және өңделетін ақпаратты пайдалану талаптары және ақпаратқа және оның пайдаланылуына мониторинг жүргізу

11. Банктің ақпараты мен ақпараттық жүйелерін пайдалану құқығы жұмыскерлерге қызметтік міндеттерін орындау үшін қажетті көлемде ұсынылады.

12. Банктің ақпараттық жүйелерінде пайдаланушылардың дербестендірілген есептік жазбалары ғана пайдаланылады.

13. Банктің маңызды ақпараттық жүйелерін пайдалану құқығы ақпараттық жүйелерді пайдаланушылардың рұқсат беру құқығының олардың қызметтік міндеттеріне сәйкестігін қамтамасыз етуге арналған рөлдерді қалыптастыру және енгізу арқылы беріледі.

14. Банктің жұмыскері болып табылмайтын тұлғаларға (бұдан әрі – үшінші тұлғалар) Банктің ақпараттық активтерін пайдалану құқығы Қазақстан Республикасының заңнамасында көзделген жағдайларды қоспағанда, ақпараттық қауіпсіздікке қойылатын талаптарды сақтау туралы сәйкес келісімнің негізінде жұмыстарды жүргізу үшін қажетті кезеңге және көлемде беріледі. Үшінші тұлғалармен жасалатын ақпараттық қауіпсіздікке қойылатын талаптарды сақтау туралы келісім конфиденциалдылық туралы қағидаларды, ақпараттық қауіпсіздікті бұзу, сонымен қатар ақпараттық жүйелердегі ақаулар мен оның қауіпсіздігін бұзу салдарынан туындаған, үшінші тұлғалардың араласуынан туындаған залалды өтеу туралы талаптарын қамтиды.

15. Банктің ақпараттық жүйелерін пайдалану құқығын беру ақпараттық жүйелерді пайдаланушыларды сәйкестендіру және аутентификациялау арқылы жүзеге асырылады. Банктің ақпараттық жүйелерін пайдаланушыларды сәйкестендіру және аутентификациялау «есептік жазбаны (сәйкестендіргіш) – парольді» енгізу арқылы немесе көпфакторлы аутентификация әдісін қолдану арқылы жүзеге асырылады.

16. Технологиялық есептік жазбаларды пайдалануға оларды пайдалану және жаңарту үшін жеке жауап беретін тұлғаларды көрсете отырып, әрбір ақпараттық жүйеге арналған есептік жазбалардың тізбесіне сәйкес рұқсат беріледі.

17. Банк ақпараттық активтерді пайдалану құқығын басқару процесінің тиімділігін қамтамасыз ететін қажетті барлық ұйымдастырушылық және техникалық шараларды қолданады.

## 5. Ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметке мониторинг жүргізуге және ақпараттық қауіпсіздіктің оқыс оқиғалары бойынша қауіпті анықтау және талдау, қақтығыстарға қарсы тұру және тергеу бойынша іс-шараларға қойылатын талаптар

18. Банк ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою бойынша құрылымдық бөлімшені – қауіпсіздіктің оқыс оқиғаларына ден қою қызметін құруды қамтамасыз етеді.

19. Ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметке және ақпараттық қауіпсіздіктің оқыс оқиғалары бойынша қауіпті анықтау және талдау, қақтығыстарға қарсы тұру және тергеу шараларына тиісті дәрежеде мониторинг жүргізуді қамтамасыз ету мақсатында Банк төмендегілерді қамтамасыз етеді:

1) Ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою процесін автоматтандыратын бағдарламалық-техникалық құралдарды енгізілуі және олардың тиісті дәрежеде қызмет етуі;
2) Мониторинг жүргізілетін ақпараттық қауіпсіздіктің оқыс оқиғаларының тізбесін, осындай оқиға көздерін, ақпараттық қауіпсіздік оқиғаларына мониторинг жүргізу кезеңдігін, тәртібін және әдістерін анықтау;
3) ақпараттық қауіпсіздіктің оқыс оқиғаларын ақпараттық қауіпсіздік жағдайларына жатқызу тәртібін, олардың жіктеуіші мен басымдылығын анықтау;
4) стандартты ден қою процедураларын әзірлеу, өзекті жай-күйінде ұстау және ден қою қызметінің жұмыскерлерін стандартты ден қою процедураларын қолдану мәселелері бойынша ақпараттық қауіпсіздіктің оқыс оқиғаларына қатысты оқыту;
5) ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою процесіне тартылған Банктің жауапты жұмыскерлерін және (немесе) бөлімшелерін анықтау;
6) ақпараттық қауіпсіздіктің оқыс оқиғаларын жою бойынша кезек күттірмейтін шараларды қабылдау тәртібін анықтау, ақпараттық қауіпсіздіктің оқыс оқиғаларының туындау себептері мен салдарын анықтау;
7) ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою қызметіне ақпараттық қауіпсіздіктің оқыс оқиғалары анықталған жағдайда бизнес-процесті ішінара немесе толықтай тоқтату бойынша қосымша бақылау шараларын жүргізу өкілеттіктері берілсін;
8) Банктің, Банк бөлімшелерінің басқарушы жұмыскерлеріне және қаржы нарығын реттеу және қадағалау бойынша уәкілетті органға, соның ішінде ақпараттық қауіпсіздіктің оқыс оқиғаларына ішкі тергеу жүргізу туралы шешім қабылдау үшін хабарлау тәртібін белгілеу;
9) ақпараттық қауіпсіздіктің оқыс оқиғаларына ішкі тергеу жүргізу үшін қажетті материалдарды жинау және талдау;
10) ақпараттық қауіпсіздіктің оқыс оқиғаларының туындау себептерін және ақпараттық қауіпсіздіктің оқыс оқиғаларын іске асыру тәртібін анықтау;
11) ақпараттық қауіпсіздіктің оқыс оқиғаларын іске асырудың әсер ету масштабын және одан болатын залалды бағалау;
12) ақпараттық қауіпсіздіктің оқыс оқиғаларына қатысты тергеуге ден қою шараларының тиімділігін талдау;
13) ақпараттық қауіпсіздіктің оқыс оқиғаларын тергеу нәтижелері туралы қорытынды әзірлеу, онда ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпарат, сонымен қатар ақпараттық қауіпсіздіктің оқыс оқиғаларын қайта іске асырудан болуы мүмкін залалды азайту мақсатында түзету шараларын қабылдау бойынша ұсыныстар көрсетіледі.

## 6. Ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты жинауға, шоғырландыруға және сақтауға қойылатын талаптар

20. Банк ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою тәртібін іске асыруды растайтын құжаттардың, мәліметтердің және фактілердің болуын, сонымен қатар ақпараттық қауіпсіздіктің оқыс оқиғалары, ақпараттық қауіпсіздіктің оқыс оқиғаларын ішкі тергеу нәтижелері туралы ақпараттың, сонымен қатар қағаз және (немесе) электронды тасымалдағыштағы тергеу материалдарының шоғырлануын, жүйелендірілуін, тұтастығын және сақталуын қамтамасыз етеді.

21. Ақпараттық қауіпсіздіктің оқыс оқиғалары туралы, ақпараттық қауіпсіздіктің оқыс оқиғаларын ішкі тергеу нәтижелері туралы ақпаратты және тергеу материалдарын сақтау мерзімі кемінде 5 (бес) жылды құрайды.

## 7. Ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты талдауға қойылатын талаптар

22. Ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметке және ақпараттық қауіпсіздіктің оқыс оқиғалары бойынша қауіпті анықтау және талдау, қақтығыстарға қарсы тұру және тергеу бойынша іс-шараларға мониторинг жүргізу процесінің тиімділігін арттыру мақсатында Банк кемінде жылына бір рет:

1) ақпараттық қауіпсіздік тәуекелдерін бағалау, ақпараттық қауіпсіздікті қамтамасыз ету әдістері мен құралдарын түзету, бизнесті өзгерту мақсатында анықталған ақпараттық қауіпсіздіктің оқыс оқиғаларына және Банктің алғалы органы қарастыруы үшін келтірілген залалға талдау жасауды;

2) ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою процесінің метрикаларын пайдалана отырып, ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою процесін түзету мақсатында тиімділікті талдауды;

3) ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою процесінің тиімділігін бағалау нәтижелерін есепке ала отырып, ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою процесінің метрикаларын қайта қарастыруды;

4) мониторинг жүргізілуі тиіс ақпараттық қауіпсіздіктің оқыс оқиғаларының тізбесін, оқиғалар көзін, ақпараттық қауіпсіздіктің оқыс оқиғаларына мониторинг жүргізу кезеңдігін, тәртібін және әдістерін қайта қарастыруды қамтамасыз етеді.

## 8. Банктің ақпараттық қауіпсіздікті қамтамасыз етуге жауапты жұмыскерлерінің жүктелген қызметтік міндеттерін орындаған кездегі жауапкершілігі

23. Банктің АҚБЖ қатысушылары:

1) Директорлар кеңесі;
2) Басқарма;
3) Ақпараттық қауіпсіздік комитеті;
4) Ақпараттық қауіпсіздікті қамтамасыз ету орталығы (бұдан әрі - АҚҚО);
5) IT блогы;
6) Қауіпсіздікті қамтамасыз ету блогы;
7) Қызметкерлерді басқару орталығы;
8) Заң блогы;
9) Комплаенс қызметі;
10) Ішкі аудит қызметі;
11) Операциялық тәуекелдер дирекциясы;
12) Ақпараттық жүйелер мен шағын жүйелердің бизнес-иелері;
13) Құрылымдық бөлімшелердің басшылары;
14) Құрылымдық бөлімшелердің жұмыскерлері.

24. Директорлар кеңесі ақпараттық қауіпсіздік саясатын және қорғалатын ақпарат тізімін, соның ішінде қызметтік, коммерциялық және заңмен қорғалатын басқа деректер туралы ақпаратты және қорғалатын ақпаратпен жұмыс жүргізу тәртібін бекітеді.

25. Басқарма ақпараттық қауіпсіздікті басқару процесін реттейтін ішкі нормативтік құжаттарды, сонымен қатар ақпараттық қауіпсіздікті қамтамасыз ету мәселелеріне қатысты жұмыскерлердің хабардарлығын арттыру мақсатында жұмыскерлердің ақпараттық қауіпсіздік бойынша ішкі нормативтік құжаттардың талаптарын білуіне тестілеу жүргізу жоспарын бекітеді.

26. Ақпараттық қауіпсіздік комитеті ақпараттық қауіпсіздікті қамтамасыз ету мәселелері бойынша шешімдер қабылдайды және Басқарма берген өкілеттіктер аясында іс-әрекет етеді.

27. АҚҚО Банктің ақпаратының конфиденциалдылығын, түгендігін және қолжетімділігін қамтамасыз ету мақсатында келесі қызметтерді жүзеге асырады:

1) ақпараттық қауіпсіздікті басқару жүйесін ұйымдастырады, ақпараттық қауіпсіздікті және қауіп-қатерді анықтау және талдау бойынша іс-шараларды қамтамасыз ету, шабуылдарға қарсы әрекет ету және ақпараттық қауіпсіздіктің оқыс оқиғаларын тергеу бойынша Банк бөлімшелерін үйлестіреді және олардың қызметін бақылайды;

2) Банктің ақпараттық қауіпсіздік саясатын әзірлейді;

3) Банктің ақпараттық қауіпсіздігін қамтамасыз ету процесіне әдіснамалық қолдау көрсетеді;

4) өзінің өкілеттіктері аясында Банктің ақпараттық қауіпсіздігін басқару, қамтамасыз ету және бақылау тәсілдерін, құралдары мен тетіктерін таңдауды, енгізуді жүзеге асырады;

5) ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты жинауды, шоғырландыруды, сақтауды және өңдеуді жүзеге асырады;

6) ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты талдауды жүзеге асырады;

7) ақпараттық қауіпсіздік комитеті ақпараттық қауіпсіздік мәселелері бойынша шешім қабылдауы үшін ұсыныстар әзірлейді;

8) Банктің ақпараттық қауіпсіздігін қамтамасыз ету процесін автоматтандыратын бағдарламалық-техникалық құраларды енгізуді, олардың тиісті түрде қызмет етуін, сонымен қатар оларға қолжеткізуді қамтамасыз етеді;

9) артықшылықты есептік жазбаларды пайдалану бойынша шектеулерді анықтайды;

10) Банк жұмыскерлерінің ақпараттық қауіпсіздік саласындағы хабардарлығын арттыру процесін ұйымдастыруға қатысады;

11) Банктің ақпараттық қауіпсіздігін басқару жүйесінің жай-күйіне мониторинг жүргізеді;

12) Банк басшылығына Банктің ақпараттық қауіпсіздігін басқару жүйесінің жай-күйі туралы ақпарат береді;

13) ақпараттық қауіпсіздік тәуекелдеріне бағалау жүргізеді;

14) ақпараттық қауіпсіздік тәуекелдерін өңдеу бойынша шаралар әзірлейді және Операциялық тәуекелдер дирекциясына оларды іске асыру бойынша есептілік ұсынады;

15) елеулі ақпараттық қауіпсіздік тәуекелдерін іске асыру туралы, сонымен қатар олардың салдарын жою туралы есептілікті әзірлейді және оларды Операциялық тәуекелдер дирекциясына ұсынады;

16) ақпараттық қауіпсіздікті қамтамасыз етуге қатысты Банктің стратегиясын іске асыру бойынша іс-шаралар жоспарын әзірлейді, олар келесі көрсетілгендерді ашып көрсетеді, бірақ олармен шектелмейді:

1) ресурстегі қажеттіліктерді анықтау, соның ішінде ақпараттық қауіпсіздік тәуекелдерін басқаруға бағытталған шараларды іске асыруға байланысты бюджетті анықтау;

2) мерзімі мен оларды іске асыру үшін жауапты орындаушыларды көрсетіп, ақпараттық қауіпсіздік саласында талап етілетін іс-шараларды сипаттау.

28. IT блогы келесі функцияларды жүзеге асырады:

1) Банктің ақпараттық инфрақұрылымының сұлбасын әзірлейді;

2) IT блогына қатысты болмайтын ақпараттық жүйелердің IT менеджерлері кіруге рұқсат беретін арнайы ақпараттық активтерді есепке алмағанда, пайдаланушылардың Банктің ақпараттық активтеріне кіру рұқсатын беруді қамтамасыз етеді;

3) Банктің жүйелік және қолданбалы бағдарламалық қамсыздандыруын конфигурациясын қамтамасыз етеді;

4) Банктің ішкі құжаттарына сәйкес ақпараттық инфрақұрылымның қызмет етуінің үздіксіздігі, Банктің аталған ақпараттық жүйелерінің конфиденциалдылығы, түгендігі мен қолжетімділігі бойынша белгіленген талаптарын орындалуын (ақпаратты резервтеу және (немесе) архивтеу және резервтік көшірмесін жасау) қамтамасыз етеді;

5) ақпараттық жүйелерді таңдаған, енгізген, әзірлеген және тестілеген кезде ақпараттық қауіпсіздіктің талаптарын сақтауды қамтамасыз етеді.

29. Қауіпсіздікті қамтамасыз ету блогы келесі функцияларды жүзеге асырады:

1) Банкте жеке және техникалық қауіпсіздік шараларын іске асырады, оған қаса кіруге рұқсат беруді және объекті ішіндегі режимді ұйымдастырады;

2) Банкте жұмыскерлерді жұмысқа қабылдаған және жұмыстан босатқан кезде ақпараттық қауіпсіздіктің қауіп-қатерінің пайда болу тәуекелін азайтуға бағытталған алдын ала іс-шараларды жүргізеді.

30. Қызметкерлерді басқару орталығы келесі функцияларды жүзеге асырады:

1) Банк жұмыскерлерінің, сонымен қатар қызмет көрсету шарты бойынша жұмысқа тартылған тұлғалардың, тәлімгерлердің, тәжірибеден өтушілердің конфиденциалды ақпаратты жария етпеу туралы міндеттемеге қол қоюын қамтамасыз етеді;

2) Банк жұмыскерлерінің ақпараттық қауіпсіздік мәселелеріне қатысты хабардарлығын қамтамасыз ету бойынша іс-шараларды ұйымдастырады және жүргізеді.

31. Заң департаменті ақпараттық қауіпсіздікті қамтамасыз ету мәселелері бойынша Банктің ішкі нормативтік құжаттарына құқықтық сараптама жүргізеді.

32. Комплаенс қызметі Заң департаментімен бірге осы Саясаттың 24-тармағында көрсетілген қорғалатын ақпараттың тізіміне қосылуы тиіс ақпарат түрлерін анықтайды.

33. Ішкі аудит қызметі Банктің ішкі аудит қызметінің жүйесін ұйымдастыруды реттейтін Банктің ішкі нормативтік құжаттарына сәйкес Банктің ақпараттық қауіпсіздігін басқару жүйесінің жай-күйіне бағалау жүргізеді.

34. Операциялық тәуекелдер дирекциясы «Екінші деңгейдегі банктерге, Қазақстан Республикасының бейрезидент-банктерінің филиалдарына арналған тәуекелдерді басқару және ішкі бақылау жүйесін қалыптастыру қағидаларын бекіту туралы» Қазақстан Республикасының Ұлттық Банкі Басқармасының 2019 жылғы 12 қарашадағы №188 қаулысымен бекітілген Екінші деңгейдегі банктерге арналған тәуекелдерді басқару және ішкі бақылау жүйесін қалыптастыру қағидаларында көзделген функцияларды жүзеге асырады.

35. Ақпараттық жүйелер мен шағын жүйелердің бизнес-иелері:

1) Қызметтер мен өнімдерді құрған, енгізген, модификациялаған, клиенттерге ұсынған кезде ақпараттық қауіпсіздікке қойылатын талаптардың сақталуы үшін жауап береді;

2) Ақпараттық жүйелерге кіруге рұқсат беретін матрицаларды құрады және олардың актуалды болуына қолдау көрсетеді.

36. Банктік құрылымдық бөлімшелерінің басшылары:

1) жұмыскерлердің ақпараттық қауіпсіздікке қойылатын талаптар қамтылатын Банктің ішкі нормативтік құжаттарымен танысуын қамтамасыз етеді;

2) олар басқаратын бөлімшелерде ақпараттық қауіпсіздікті қамтамасыз ету үшін жеке жауапкершілік көтереді.

37. Банктік құрылымдық бөлімшелерінің жұмыскерлері:

1) Банкте қабылданған ақпараттық қауіпсіздікке қойылатын талаптардың сақталуы үшін жауап береді;

2) Өзінің қызметтік міндеттемелері аясында бірлесіп әрекет ететін үшінші тұлғалардың ақпараттық қауіпсіздікке қойылатын талаптарды орындауын, соның ішінде аталған талаптарды үшінші тұлғалармен жасалатын шарттарға қосу арқылы бақылайды;

3) ақпараттық активтермен жұмыс жүргізген кездегі барлық күдікті жағдайлар мен бұзушылықтар туралы өзінің тікелей басшысына және АҚҚО-ға хабарлайды.

38. Жұмыскер өзіне жүктелген қызметтік міндеттемелерді орындаған кезде, ақпараттық ресурстарды пайдалану тәртібі мен ережесін және ақпараттық қауіпсіздікті қамтамасыз ету бойынша Банкте қабылданған шараларды сақтамауы Қазақстан Республикасының қолданыстағы заңнамасына және Банктің ішкі нормативтік құжаттарына сәйкес жауапкершілікке әкеледі.

## 9. Банктің еншілес компанияларында ақпараттық қауіпсіздік жүйесін қамтамасыз ету

39. Банктің еншілес компанияларында ақпараттық қауіпсіздік деңгейін қажетті және жеткілікті қамтамасыз ету бөлігінде АҚҚО мен «Банк ЦентрКредит» АҚ-тың еншілес компаниялары арасында бағттауды қамтамасыз ету және бірлесіп әрекет етуді құру мақсатында, АҚҚО ЕК-тың АҚ-ты қамтамасыз ету саласындағы қызметін үйлестіру бойынша келесі функцияларды жүзеге асырады:

1) ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі талаптарды белгілейді;
2) ақпараттық қауіпсіздік бөлігінде ішкі нормативтік құжаттарды келісімге алады;
3) ақпараттық қауіпсіздікті қамтамасыз етудің ұйымдастыру шараларын және бағдарламалық-техникалық құралдарын енгізуді ұсынады және келісімге алады;
4) Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы жыл сайынғы іс-шаралар жоспарларын және еншілес компаниялардың бюджетін келісімге алады;

5) Ақпараттық қауіпсіздікті басқару жүйесін дамыту бөлігінде, сондай-ақ ақпараттық қауіпсіздікті қамтамасыз етуге жауапты Еншілес компаниялардың қызметкерлерін оқыту және кәсіби дамыту мәселелерінде кеңес беріп, қолдау көрсетеді;
6) ақпараттық қауіпсіздікті қамтамасыз ету саласында сыртқы тексерулер мен аудиттерден өту үшін жәрдем береді;
7) ақпараттық қауіпсіздіктің жай-күйіне тексеру жүргізеді, ақпарат сұратады, анықталған ескертулерді жою бойынша іс-шаралар жоспарларын келісімге алады, олардың орындалуын талап етеді;
8) Еншілес компаниялардың бейінді комитеттеріне (болған жағдайда) қатысады.

## 10. Қорытынды қағидалар

40. Осы Саясатта реттелмеген барлық мәселелер Қазақстан Республикасының заңнамасына, ішкі нормативтік құжаттарға және Банктің уәкілетті органдарының шешімдеріне, сонымен қатар Банк қызметінің қалыптасқан тәжірибесіне сәйкес шешімін табады.

41. Саясат Банктің Директорлар кеңесі бекіткен күннен бастап күшіне енеді және Банктің Директорлар кеңесі оның күші жойылған деп таныған сәттен бастап күшін жояды.

42. Қазақстан Республикасының заңнамасына өзгерістер енгізудің нәтижесінде осы Саясаттың жеке нормалары Қазақстан Республикасының қолданыстағы заңнамасына қайшы болса, онда Саясатқа өзгерістер енгізген сәтке дейін Қазақстан Республикасының қолданыстағы заңнамасын және Саясаттың Қазақстан Республикасының заңнамасына қайшы келмейтін бөлігін басшылыққа алу қажет.

43. Осы Саясатты қайта қарауды АҚҚО кемінде жылына бір рет жүзеге асырады.

**Ақпараттық қауіпсіздікті қамтамасыз ету орталығы**

**Одобрено**
**Решением Правления**
**№ 3-1221-03 от 21.12.2021г.**

**Утверждено**
**Постановлением Совета Директоров**
**№ 3-0113-01 от 13.01.2022г.**

# Политика информационной безопасности АО «Банк ЦентрКредит»

**Содержание:**



## 1. Общие положения

1. Настоящая Политика информационной безопасности (далее – Политика) является основополагающим документом системы управления информационной безопасности АО «Банк ЦентрКредит» (далее – Банк), определяющим цели, задачи и область действия системы управления информационной безопасностью Банка (далее - СУИБ).

2. Банк обеспечивает создание и функционирование СУИБ, являющейся частью общей системы управления Банка, предназначенной для управления процессом обеспечения информационной безопасности.

3. СУИБ обеспечивает защиту информационных активов Банка, допускающую минимальный уровень потенциального ущерба для бизнес-процессов Банка.

4. Политика разработана в соответствии с законодательством Республики Казахстан, в том числе нормативными правовыми актами, регулирующими требования к обеспечению информационной безопасности банков второго уровня, а также требованиями международных стандартов в области информационной безопасности.

5. Требования, предъявляемые к процессам системы управления информационной безопасности Банка и описанные в настоящей Политике, детально описаны во внутренних нормативных документах Банка, разработанных в соответствии с Главой 11 «Требования к процессам системы управления информационной безопасностью» постановления Правления Национального Банка Республики Казахстан от 27 марта 2018 года № 48 «Об утверждении Требований к обеспечению информационной безопасности банков, филиалов банков-нерезидентов Республики Казахстан и организаций, осуществляющих отдельные виды банковских операций, Правил и сроков предоставления информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах».

## 2. Цели, задачи и основные принципы построения системы управления информационной безопасностью

6. Целью СУИБ является повышение эффективности процессов обеспечения информационной безопасности, обеспечение требуемого уровня конфиденциальности, целостности и доступности критичных информационных активов, и как следствие, снижение рисков информационной безопасности и связанного с ними ущерба.

7. К задачам СУИБ относятся:

1) категорирование информационных активов;

2) организация доступа к информационным активам;

3) обеспечение безопасности информационной инфраструктуры;

4) осуществление мониторинга деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз и уязвимостей, противодействию атакам и расследованию инцидентов информационной безопасности;

5) проведение анализа информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах;

6) определение порядка управления средствами криптографической защиты информации;

7) обеспечение информационной безопасности при доступе третьих лиц к информационным активам;

8) проведение внутренних проверок состояния информационной безопасности.

8. Построение СУИБ и ее функционирование осуществляются в соответствии со следующими основными принципами:

1) законность – любые действия, предпринимаемые для обеспечения информационной безопасности, осуществляются на основе действующего законодательства, с применением всех дозволенных законодательством методов обнаружения, предупреждения, локализации и пресечения негативных воздействий на информационные активы Банка;

2) ориентированность на бизнес – информационная безопасность рассматривается как процесс поддержки основной деятельности, любые меры по обеспечению информационной безопасности не должны повлечь за собой серьезных препятствий для ведения бизнеса;

3) комплексность – обеспечение безопасности информационных активов в течение всего их жизненного цикла, на всех технологических этапах их использования и во всех режимах функционирования;

4) обоснованность и экономическая целесообразность – используемые возможности и средства защиты должны быть реализованы на соответствующем уровне развития науки и техники, обоснованы с точки зрения заданного уровня безопасности и должны соответствовать предъявляемым требованиям и нормам. Во всех случаях стоимость мер и технологических решений по обеспечению информационной безопасности не должна превышать стоимость защищаемых информационных активов;

5) адаптивность – определение и применение методов и средств защиты информационных активов в соответствии с их критичностью;

6) необходимое знание и наименьший уровень привилегий – пользователь получает минимальный уровень привилегий и доступ только к тем информационным активам, которые являются необходимыми для выполнения им деятельности в рамках своих полномочий;

7) специализация – реализация мер и эксплуатация технологических решений по обеспечению информационной безопасности должны осуществляться профессионально подготовленными специалистами;

8) информированность и персональная ответственность – руководители всех уровней и исполнители должны быть осведомлены обо всех требованиях информационной безопасности и несут персональную ответственность за выполнение этих требований и соблюдение установленных мер информационной безопасности;

9) взаимодействие и координация – меры информационной безопасности осуществляются на основе взаимосвязи соответствующих структурных подразделений Банка, координации их усилий для достижения поставленных целей, а также установления необходимых связей с внешними организациями, профессиональными ассоциациями и сообществами, государственными органами, юридическими и физическими лицами;

10) подтверждаемость – свидетельства, подтверждающие исполнение требований по информационной безопасности и эффективности СУИБ должны создаваться и храниться с возможностью оперативного доступа и восстановления.

## 3. Область действия системы управления информационной безопасностью

9. Областью действия СУИБ являются основные бизнес-процессы Банка, непосредственно ориентированные на предоставление услуг клиентам, представляющие ценность для клиентов и обеспечивающих получение прибыли, определённых с процедурой, определяющей классификацию бизнес-процессов.

10. Объектами защиты являются критичные информационные активы, необходимые для функционирования основных бизнес-процессов, к которым могут быть отнесены:

1) Индивидуальные устройства обработки информации;
2) Носители информации;
3) Периферийное компьютерное оборудование;
4) Серверы;
5) Сетевое оборудование;
6) Аппаратура телефонии;
7) Физические канал связи;
8) Базы данных;
9) Виртуальные каналы связи;
10) Системы виртуализации;
11) Операционные системы;
12) Программное обеспечение аппаратных средств;
13) Прикладное программное обеспечение;
14) Программное обеспечение телефонии.

## 4. Требования к доступу к создаваемой, хранимой и обрабатываемой информации в информационных системах Банка и мониторинг информации и доступа к ней

11. Доступ к информации и информационным системам Банка предоставляется работникам в объеме, необходимом для исполнения их функциональных обязанностей.

12. В информационных системах Банка используются только персонализированные пользовательские учетные записи пользователей.

13. Предоставление доступа к критичным информационным системам Банка производится путем формирования и внедрения ролей для обеспечения соответствия прав доступа пользователей информационных систем их функциональным обязанностям.

14. Доступ лицам, не являющимся работниками Банка (далее - третьи лица) к информационным активам Банка предоставляется на период и в объеме, необходимых для проведения работ на основании соответствующего соглашения о соблюдении требований к информационной безопасности, за исключением случаев, предусмотренных законодательством Республики Казахстан. В соглашениях о соблюдении требований к информационной безопасности, заключаемых с третьими лицами, содержатся положения о конфиденциальности, условия о возмещении ущерба, возникшего вследствие нарушения информационной безопасности, а также сбоев в работе информационных систем и нарушения их безопасности, вызванных вмешательством третьих лиц.

15. Доступ к информационным системам Банка осуществляется путем идентификации и аутентификации пользователей информационных систем. Идентификация и аутентификация пользователей информационных систем Банка производится посредством ввода пары «учетная запись (идентификатор) – пароль» или с применением способов многофакторной аутентификации.

16. Использование технологических учетных записей допускается в соответствии с перечнем таких учетных записей для каждой информационной системы с указанием лиц, персонально ответственных за их использование и актуальность.

17. Банк применяет все необходимые организационные и технические меры, обеспечивающие эффективность процесса управления доступом к информационным активам.

## 5. Требования к осуществлению мониторинга деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности

18. Банк обеспечивает создание структурного подразделения по реагированию на инциденты информационной безопасности – службу реагирования на инциденты информационной безопасности.

19. В целях обеспечения надлежащего мониторинга деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности Банк обеспечивает:

1) внедрение, надлежащее функционирование программно-технических средств, автоматизирующих процесс реагирования на инциденты информационной безопасности;

2) определение перечня событий информационной безопасности, подлежащих мониторингу, источников таких событий, периодичности, порядка и методов мониторинга событий информационной безопасности;

3) определение порядка отнесения событий информационной безопасности к инцидентам информационной безопасности, их классификации и приоритетности;

4) разработку, поддержание в актуальном состоянии стандартных процедур реагирования и обучение работников службы реагирования на инциденты информационной безопасности по вопросам применения стандартных процедур реагирования;

5) определение ответственных работников и (или) подразделений Банка, вовлеченных в процесс реагирования на инциденты информационной безопасности;

6) определение порядка принятия неотложных мер по устранению инцидентов информационной безопасности, установления причин возникновения инцидентов информационной безопасности и их последствий;

7) наделение службы реагирования на инциденты информационной безопасности полномочиями по введению дополнительных мер контроля по частичной или полной остановке бизнес-процессов в случае выявления инцидента информационной безопасности;

8) определение порядка информирования руководящих работников Банка, подразделений Банка и уполномоченного органа по регулированию, контролю и надзору финансового рынка и финансовых организаций, в том числе для принятия решения о проведении внутреннего расследования инцидента информационной безопасности;

9) сбор и анализ материалов, необходимых для проведения внутреннего расследования инцидента информационной безопасности;

10) установление причин возникновения инцидента информационной безопасности и порядка реализации инцидента информационной безопасности;

11) оценка масштаба воздействия и ущерба от реализации инцидента информационной безопасности;

12) анализ эффективности принятых мер реагирования на расследуемый инцидент информационной безопасности;

13) подготовка заключения о результатах расследования инцидента информационной безопасности, в котором отражается информация об инциденте информационной безопасности, а также рекомендации по принятию корректирующих мер в целях снижения вероятности и возможного ущерба от повторной реализации инцидента информационной безопасности.

## 6. Требования к осуществлению сбора, консолидации и хранения информации об инцидентах информационной безопасности

20. Банк обеспечивает наличие документов, сведений и фактов, подтверждающих реализацию порядка реагирования на инциденты информационной безопасности, а также консолидацию, систематизацию, целостность и сохранность информации об инцидентах информационной безопасности, результатах внутреннего расследования инцидентов информационной безопасности и материалов расследования на бумажном носителе и (или) в электронном виде.

21. Срок хранения информации об инцидентах информационной безопасности, результатах

внутреннего расследования инцидентов информационной безопасности и материалов расследования составляет не менее 5 (пяти) лет.

## 7. Требования к проведению анализа информации об инцидентах информационной безопасности

22. В целях повышения эффективности процесса мониторинга деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности, не реже одного раза в год Банк обеспечивает:

1) проведение анализа выявленных инцидентов информационной безопасности и нанесенного ими ущерба для рассмотрения коллегиальным органом Банка, с целью оценки рисков информационной безопасности, корректировки методов и средств обеспечения информационной безопасности, изменения бизнес;

2) оценку эффективности с целью корректировки процесса реагирования на инциденты информационной безопасности с использованием метрик процесса реагирования на инциденты информационной безопасности;

3) пересмотр метрик процесса реагирования на инциденты информационной безопасности с учетом результата оценки эффективности процесса реагирования на инциденты информационной безопасности;

4) пересмотр перечня событий информационной безопасности, подлежащих мониторингу, источников событий, периодичности, порядка и методов мониторинга событий информационной безопасности.

## 8. Ответственность работников Банка за обеспечение информационной безопасности при исполнении возложенных на них функциональных обязанностей

23. Участниками СУИБ Банка являются:

1) Совет директоров;
2) Правление;
3) Комитет по информационной безопасности;
4) Центр обеспечения информационной безопасности (далее - ЦОИБ);
5) Блок IT;
6) Блок по обеспечению безопасности;
7) Центр управления персоналом;
8) Юридический блок;
9) Служба Комплаенс;
10) Служба внутреннего аудита;
11) Дирекция операционных рисков;
12) Бизнес-владельцы информационных систем и подсистем;
13) Руководители структурных подразделений;
14) Работники структурных подразделений.

24. Совет директоров утверждает политику информационной безопасности и перечень защищаемой информации, включающий в том числе информацию о сведениях, составляющих служебную, коммерческую или иную охраняемую законом тайну, и порядок работы с защищаемой информацией.

25. Правление утверждает внутренние нормативные документы, регламентирующие процесс управления информационной безопасностью, а также план проведения тестирования работников на знание требований внутренних нормативных документов по информационной безопасности, в целях повышения осведомленности работников в вопросах обеспечения информационной безопасности.

26. Комитет по информационной безопасности принимает решения по вопросам обеспечения информационной безопасности и действует в рамках полномочий, предоставленных Правлением.

27. ЦОИБ в целях обеспечения конфиденциальности, целостности и доступности информации Банка осуществляет следующие функции:

1) организует систему управления информационной безопасностью, осуществляет координацию и контроль деятельности подразделений Банка по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности;

2) разрабатывает политику информационной безопасности Банка;

3) обеспечивает методологическую поддержку процесса обеспечения информационной безопасности Банка;

4) осуществляет выбор, внедрение и применение методов, средств и механизмов управления, обеспечения и контроля информационной безопасности Банка, в рамках своих полномочий;

5) осуществляет сбор, консолидацию, хранение и обработку информации об инцидентах информационной безопасности;

6) осуществляет анализ информации об инцидентах информационной безопасности;

7) подготавливает предложения для принятия Комитетом по информационной безопасности решения по вопросам информационной безопасности;

8) обеспечивает внедрение, надлежащее функционирование программно-технических средств, автоматизирующих процесс обеспечения информационной безопасности Банка, а также предоставление доступа к ним;

9) определяет ограничения по использованию привилегированных учетных записей;

10) участвует в организации процесса повышения осведомленности работников Банка в области информационной безопасности;

11) осуществляет мониторинг состояния системы управления информационной безопасностью Банка;

12) осуществляет информирование руководства Банка о состоянии системы управления информационной безопасностью Банка;

13) проводит оценку рисков информационной безопасности;

14) разрабатывает меры по обработке рисков информационной безопасности и предоставляет отчетности по их реализации в Дирекцию операционных рисков;

15) подготавливает и предоставляет отчетности о реализации существенных рисков информационной безопасности в Дирекцию операционных рисков, а также об устранении их последствий;

16) разрабатывает план мероприятий по реализации стратегии Банка в части обеспечения информационной безопасности, который раскрывает, но, не ограничиваясь, следующее:

1) определение потребностей в ресурсах, в том числе определение бюджета, связанного с реализацией мер, направленных на управление рисками информационной безопасности;

2) описание требуемых мероприятий в области информационной безопасности с указанием сроков и ответственных исполнителей за их реализацию.

28. Блок IT осуществляет следующие функции:

1) разрабатывает схемы информационной инфраструктуры Банка;

2) обеспечивает предоставление доступа пользователям к информационным активам Банка, за исключением специализированных информационных активов, доступ к которым предоставляется ИТ-менеджерами информационных систем, не относящимися к Блоку IT;

3) обеспечивает конфигурирование системного и прикладного программного обеспечения Банка;

4) обеспечивает исполнение установленных требований по непрерывности функционирования информационной инфраструктуры, конфиденциальности, целостности и доступности данных информационных систем Банка (включая резервирование и (или) архивирование и резервное копирование информации) в соответствии с внутренними документами Банка;

5) обеспечивает соблюдение требований информационной безопасности при выборе, внедрении, разработке и тестировании информационных систем.

29. Блок по обеспечению безопасности осуществляет следующие функции:

1) реализует меры физической и технической безопасности в Банке, в том числе организует пропускной и внутриобъектовый режим;

2) проводит профилактические мероприятия, направленные на минимизацию рисков возникновения угроз информационной безопасности при приеме на работу и увольнении

работников Банка.

30. Центр управления персоналом осуществляет следующие функции:

1) обеспечивает подписание работниками Банка, а также лицами, привлеченными к работе по договору об оказании услуг, стажерами, практикантами обязательств о неразглашении конфиденциальной информации;

2) организует и проводит мероприятия по обеспечению осведомленности работников Банка в вопросах информационной безопасности.

31. Юридический департамент осуществляет правовую экспертизу внутренних нормативных документов Банка по вопросам обеспечения информационной безопасности.

32. Служба комплаенс совместно с Юридическим департаментом определяет виды информации, подлежащие включению в перечень защищаемой информации, предусмотренной пунктом 24 настоящей Политики.

33. Служба внутреннего аудита проводит оценку состояния системы управления информационной безопасностью Банка в соответствии с внутренними нормативными документами Банка, регламентирующими организацию системы внутреннего аудита Банка.

34. Дирекция операционных рисков осуществляет функции, предусмотренные Правилами формирования системы управления рисками и внутреннего контроля для банков второго уровня, утвержденными Постановление Правления Национального Банка Республики Казахстан от 12 ноября 2019 года №188 «Об утверждении Правил формирования системы управления рисками и внутреннего контроля для банков второго уровня, филиалов банков-нерезидентов Республики Казахстан».

35. Бизнес-владельцы информационных систем или подсистем:

1) отвечают за соблюдение требований к информационной безопасности при создании, внедрении, модификации, предоставлении клиентам продуктов и услуг;

2) формируют и поддерживают актуальность матриц доступа к информационным системам.

36. Руководители структурных подразделений Банка:

1) обеспечивают ознакомление работников с внутренними нормативными документами Банка, содержащими требования к информационной безопасности;

2) несут персональную ответственность за обеспечение информационной безопасности в возглавляемых ими подразделениях.

37. Работники структурных подразделений Банка:

1) отвечают за соблюдение требований к информационной безопасности, принятых в Банке;

2) контролируют исполнение требований к информационной безопасности третьими лицами, с которыми они взаимодействуют в рамках своих функциональных обязанностей, в том числе путем включения указанных требований в договоры с третьими лицами;

3) извещают своего непосредственного руководителя и ЦОИБ обо всех подозрительных ситуациях и нарушениях при работе с информационными активами.

38. Несоблюдение порядка и правил использования информационных ресурсов и принятых в Банке мер обеспечения информационной безопасности, при исполнении работником возложенных на него функциональных обязанностей, влечет за собой ответственность в соответствии с действующим законодательством Республики Казахстан и внутренними нормативными документами Банка.

## 9. Обеспечение системы информационной безопасности в Дочерних компаниях Банка

39. В целях обеспечения кураторства и построения взаимодействия между ЦОИБ и дочерними компаниями АО «Банк ЦентрКредит» в части обеспечения необходимого и достаточного обеспечения уровня информационной безопасности в Дочерних компаниях Банка, ЦОИБ осуществляет следующие функции координации деятельности ДК в области обеспечения ИБ:

1) определяет требования по обеспечению информационной безопасности;

2) согласовывает внутренние нормативные документы в части информационной безопасности;

3) рекомендует и согласовывает внедрение организационных мер и программно-технических средств обеспечения информационной безопасности;

4) согласовывает ежегодные планы мероприятий и бюджет Дочерних компаний в области обеспечения информационной безопасности;

5) оказывает консультационную поддержку в части развития системы управления информационной безопасностью, а также в вопросах обучения и профессионального развития работников Дочерних компаний, ответственных за обеспечение информационной безопасности;

6) оказывает содействие в прохождении внешних проверок и аудитов в области обеспечения информационной безопасности;

7) проводит проверки состояния информационной безопасности, запрашивает информацию, согласовывает планы мероприятий по устранению выявленных замечаний, требует их исполнения;

8) участвует в профильных комитетах Дочерних компаний (при наличии).

## 10. Заключительные положения

40. Все вопросы, не урегулированные настоящей Политикой, решаются в соответствии с законодательством Республики Казахстан, внутренними нормативными документами и решениями уполномоченных органов Банка, а также сложившейся практикой деятельности Банка.

41. Политика вступает в силу с даты утверждения Советом Директоров Банка и прекращает свое действие с момента признания ее утратившей силу Советом Директоров Банка.

42. Если в результате изменения законодательства Республики Казахстан отдельные нормы настоящей Политики вступают в противоречие с действующим законодательством Республики Казахстан, то до момента внесения изменений в Политику, необходимо руководствоваться действующим законодательством Республики Казахстан и Политикой в части, не противоречащей законодательству Республики Казахстан.

43. Пересмотр настоящей Политики осуществляется ЦОИБ не реже одного раза в год.

**Центр обеспечения информационной безопасности**