

УТВЕРЖДЕНО:

Правлением ПАО «Томскпромстройбанк»
(протокол от 25 октября 2022)

Изменения №1

в Политику информационной безопасности ПАО «Томскпромстройбанк»

В связи с вступлением в силу Указания Банка России от 25.03.2022 №6103-У «О внесении изменений в Положение Банка России от 8 апреля 2020 года №716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе» внести в Политику информационной безопасности ПАО «Томскпромстройбанк» следующие изменения:

1. Пункт 7.9 изложить в следующей редакции:

«7.9. Требования к третьим лицам (внешним подрядчикам, контрагентам), которым могут быть переданы функции Банка по обеспечению информационной безопасности, а также определение порядка взаимодействия и распределения ответственности между Банком и привлеченными ею третьими лицами:».

2. Подпункт 11.4.2 пункта 11.4 изложить в новой редакции:

«11.4.2. В целях **управления риском** информационной безопасности:

- соблюдает процедуры управления операционным риском, установленные в п.п. 2.1.1, 2.1.2. и 2.1.7. Положения Банка России 716-П в части идентификации, сбора и регистрации информации о событиях риска информационной безопасности;
- ведет Базу событий по событиям риска информационной безопасности;
- проводит мониторинг риска информационной безопасности;
- участвует в реализации процессов в рамках комплекса мероприятий, направленных на повышение эффективности управления риском информационной безопасности и уменьшение негативного влияния риска информационной безопасности;
- осуществляет мониторинг сигнальных и контрольных значений контрольных показателей уровня риска информационной безопасности;
- разрабатывает внутренние документы по управлению риском информационной безопасности;
- информирует сотрудников Банка по вопросам, связанным с управлением риском информационной безопасности;
- осуществляет другие функции, связанные с управлением риском информационной безопасности, предусмотренные внутренними документами Банка;
- составляет отчеты по риску информационной безопасности и направление их в службу управления рисками и должностному лицу, ответственному за обеспечение информационной безопасности.

Сводные отчеты по риску информационной безопасности направляются на рассмотрение Председателю Правления и коллегиальному исполнительному органу Банка, в дополнение к отчетам, формируемым Службой управления рисками.


Сводные отчеты по риску информационной безопасности включают информацию об управлении риском информационной безопасности, включая мониторинг КИР, выполнение контрольных показателей, проведения мероприятий в секторе по информационной безопасности, направленных на повышение качества системы управления риском информационной безопасности и уменьшение негативного влияния риска информационной безопасности.

Сектор по информационной безопасности представляет сводные отчеты Правлению Банка в срок:


- для ежеквартальных отчетов - не позднее 9 рабочих дней после отчетной даты;
- для ежегодных отчетов - не позднее 18 рабочих дней после отчетной даты.»

«СОГЛАСОВАНО»


Председатель Правления

 /Н.Ю. Кайдаш/
« 25 » октября 2022г.

Заместитель Председателя Правления

 /Т.И. Рощина/
« 25 » октября 2022г.


Главный бухгалтер

 /О.В. Кох/
« 25 » октября 2022г.

Начальник управления автоматизации

 /А.Г. Назаров/
« 25 » октября 2022г.


Начальник правового управления

 /О.С. Хонявина/
« 25 » октября 2022г.

Руководитель службы управления рисками

 /Н.А. Евтехова/
« 25 » октября 2022г.

Руководитель службы внутреннего контроля

 /И.В. Аболонина/
« 25 » октября 2022г.

Начальник сектора информационной безопасности

 /Т.А. Буленко/
« 25 » октября 2022г.