УТВЕРЖДЕНО
Решением Правления АО «SQIF Capital»
Протокол заседания № 18/11-1 от 18 ноября 2024 года

ПРАВИЛА
по обеспечению беспрерывности предоставления услуг клиентам в АО «SQIF Capital»

г. Алматы, 2024

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила по обеспечению беспрерывности предоставления услуг клиентам в АО «SQIF Capital» (далее – «**Правила**» и «**Компания**», соответственно) разработаны в соответствии с уставом Компании; законодательством РК о требованиях к безопасности и беспрерывности работы информационных систем организаций, осуществляющих отдельные виды банковских операций; иными нормативными правовыми актами РК.

1.2. Правила определяют требования к безопасности и беспрерывности работы информационных систем Компании, посредством которых Компания обеспечивает оказание брокерских услуг и обменные операции с иностранной валютой, за исключением обменных операций с наличной иностранной валютой (далее – «услуги»).

2. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ

В настоящих Правилах используются следующие основные понятия и определения:

1) **объект информационной системы** – отдельный компонент информационной системы, предназначенный для передачи, обработки и хранения информации для выполнения отдельной функции при оказании услуг;
2) **основной центр информационной системы** (далее – основной центр) – совокупность программно-технических средств, обеспечивающих оказание услуг в штатном (повседневном) режиме;
3) **резервный центр информационной системы** (далее – резервный центр) – совокупность программно-технических средств, обеспечивающих оказание услуг при возникновении нестандартных ситуаций или проведении плановых технических работ в основном центре;
4) **информационная система для оказания услуг** (далее – информационная система) – совокупность информационных систем и сервисов (АИС «InvestManager», личный кабинет, система 1С), предназначенная для хранения, обработки, поиска, распространения, передачи и предоставления информации с применением программно-аппаратного комплекса, посредством которой обеспечивается оказание услуг;
5) **ответственный работник** – работник Компании, ответственный за работу в информационной системе в соответствии с должностными обязанностями. К таким работникам относятся работники Департамента информационных технологий (ДИТ), Департамента информационной безопасности (ДИБ), Главный бухгалтер, Департамент по работе с клиентами (ДРК) и Департамента операционной деятельности (Бэк офиса);
6) **рабочее место** – персональный компьютер (сервер), на котором установлен программно-пользовательский интерфейс для управления информационной системой либо объектами информационной системы;
7) **команда восстановления** – работники Компании и/или организаций, оказывающих Компании услуги по обеспечению доступности и полноценного функционирования информационной системы или объектов информационной системы, которые обеспечивают полное восстановление либо перевод работы информационной системы в резервный центр;
8) **пользователь** – клиент Компании, обращающийся к информационной системе за получением услуг, либо ответственный работник;
9) **идентификация** – подтверждение подлинности субъекта или объекта доступа к информационной системе путем определения соответствия предъявленных реквизитов доступа;
10) **программно-аппаратный комплекс** – совокупность программного обеспечения и технических средств, совместно применяемых для решения задач определенного типа.

3. ТРЕБОВАНИЯ К РАБОЧИМ МЕСТАМ

3.1. На рабочих местах Компания обеспечивает:

1) установку и функционирование программно-аппаратного комплекса защиты от несанкционированного доступа, включающего в себя средства идентификации и аутентификации ответственного работника;
2) установку и функционирование технических средств бесперебойного электропитания, позволяющих осуществлять работу рабочего места при отсутствии напряжения в электросети в течение времени, необходимого для корректного завершения работы в информационной системе, но не менее десяти минут. Допускается использование общего источника бесперебойного питания, установленного в здании, где находится офис Компании;
3) установку и функционирование средств обнаружения вредоносного программного кода и/или программы. В случае выявления факта заражения данная информация доводится до сведения работника Департамента информационной безопасности, для принятия соответствующих мер;
4) программную либо программно-аппаратную защиту передаваемой информации и каналов связи. Допускается централизованная защита передаваемой информации путем установки соответствующих программно-аппаратных средств на специально выделенных рабочих местах.

3.2. Для обеспечения защиты данных от несанкционированного доступа внутренними документами Компании устанавливается порядок хранения и использования технических средств, паролей или другой информации, предоставляющих доступ к рабочему месту.

3.3. Внутренними документами Компании также утверждается порядок доступа к ресурсам (дисковое пространство, директории, сетевые ресурсы, базы данных), выделенным для накопления в них информации для передачи в информационную систему, получения информации из информационной системы, хранения, архивирования либо другой обработки информации.

3.4. Доступ к рабочему месту ответственным работником осуществляется в соответствии с его должностными обязанностями.

3.5. Одному системному имени пользователя, по которому идентифицируется пользователь на входе в информационные системы, соответствует один ответственный работник, за исключением работников, выполняющих функции администратора. Для работника, выполняющего функции администратора, допускается создание нескольких системных имен пользователя.

3.6. Порядок доступа к рабочему месту посредством сети и иных технических каналов передачи данных минимизирует возможность несанкционированного доступа.

3.7. Во внутренних документах Компании, предусматривающих порядок работы ответственных работников, имеющих доступ в информационную систему, определяются:

1) порядок назначения ответственных работников;
2) режим работы ответственных работников;
3) права и обязанности ответственных работников, включая должностные инструкции;
4) список команды восстановления.

4. ТРЕБОВАНИЯ К ВНУТРЕННИМ ДОКУМЕНТАМ ПО СТРУКТУРЕ И ФУНКЦИОНИРОВАНИЮ ИНФОРМАЦИОННОЙ СИСТЕМЫ

4.1. Внутренними документами Компании по структуре и функционированию информационных систем утверждается:
   1) перечень информационных систем и их объектов, их назначение и основные характеристики, требования к числу уровней иерархии и степени централизации систем, в том числе, перечень функций, задач по каждому объекту информационной системы;
   2) требования к способам и средствам связи для информационного обмена между компонентами информационных систем;
   3) планы восстановления работы информационных систем (далее - план восстановления);
   4) требования к режимам функционирования информационных систем;
   5) требования к мониторингу функционирования информационных систем;
   6) требования к классификации, количеству и режиму работы ответственных работников команды восстановления.

4.2. Внутренние документы Компании по структуре и функционированию информационных систем подлежат пересмотру на предмет актуализации на периодической основе, определенной Компанией, но не реже одного раза в год.

5. ТРЕБОВАНИЯ К БЕЗОПАСНОСТИ РАБОТЫ ИНФОРМАЦИОННЫХ СИСТЕМ

5.1. При обращении пользователя к информационной системе для получения услуг Компания обеспечивает:
   1) регистрацию действий по получению клиентами услуг в электронных журналах без возможности изменения внесенных в них данных, в том числе, как успешных, так и неудачных, начиная от попытки установления связи, с указанием времени совершения операций. Период хранения сведений электронных журналов составляет не менее 2 (двух) месяцев;
   2) функционирование программного обеспечения, предназначенного для автоматического мониторинга, выявления и блокирования в информационной системе несанкционированных операций или действий, направленных на создание условий для проведения несанкционированных операций;
   3) архитектуру «клиент-сервер», позволяющую при выводе из строя рабочего места пользователя или получении злоумышленником несанкционированного доступа к нему не влиять на работу серверной части системы, а при сбое сервера приложений не влиять на состояние данных системы;
   4) резервное копирование и архивацию данных с возможностью их последующего восстановления;
   5) выполнение действий, предусмотренных подпунктом 4 пункта 3.1. настоящих Правил.

5.2. При оказании услуг осуществляется шифрование передаваемых данных и (или) информационно-коммуникационной сети для их передачи от персональных компьютеров, телефонов, электронных терминалов и иных устройств до конечной системы обработки передаваемых данных.

6. ТРЕБОВАНИЯ К ОБЕСПЕЧЕНИЮ БЕСПРЕРЫВНОСТИ РАБОТЫ ИНФОРМАЦИОННЫХ СИСТЕМ

6.1. В целях обеспечения беспрерывности предоставления услуг Компания определяет во внутренних документах план восстановления, порядок его пересмотра и тестирования.

6.2. Разработка плана восстановления осуществляется ДИТ с учетом следующих факторов:

1) виды и характер нестандартных ситуаций, их степень воздействия на деятельность Компании;
2) перечень информационных систем и их объектов, обеспечивающих оказание услуг, с указанием приоритетности их восстановления;
3) ущерб, возникающий при остановке работы информационных систем, и затраты для восстановления их работы.

6.3. При указании перечня информационных систем определяются допускаемые сроки их восстановления. Сроки устанавливаются Компанией в зависимости от критичности простоя в работе информационной системы.

6.4. Компания обеспечивает наличие не менее одного резервного центра, находящегося в том же населенном пункте, что и основной центр, гарантирующего возобновление предоставления Компанией услуг в течение не более четырех часов с момента возникновения сбоя (простоя).

Основной и резервный центры Компании размещаются на территории Республики Казахстан.

6.5. Компания обеспечивает каждый центр (основной и резервный) двумя выделенными каналами связи от разных поставщиков (провайдеров) услуг связи.

6.6. План восстановления содержит следующие условия:

1) наличие и место нахождения резервного центра;
2) перечень бизнес-процессов, объектов информационной системы, технических, программных или других средств, обеспечивающих работу информационной системы, восстановление которых требуется в резервном центре;
3) порядок проведения, периодичность и сценарии тестирования функционирования резервного центра информационной системы;
4) порядок восстановления нарушенных информационных систем после ликвидации последствий нестандартных ситуаций, критерии, позволяющие принять решение о завершении работы в нестандартном режиме, и порядок принятия такого решения, а также порядок возврата в штатный режим функционирования.

6.7. В целях проверки готовности работы резервного центра и резервных каналов связи для восстановления деятельности информационной системы ДИТ не менее одного раза в год проводит тестирование функционирования резервного центра и резервных каналов связи в соответствии с планом восстановления (далее – тестирование Плана).

6.8. Тестирование Плана проводится по разработанной и утвержденной Компанией программе, предусматривающей описание сценария возникновения нестандартной ситуации, восстанавливаемых рабочих процессов и объектов информационной системы, действий команды восстановления, требований по срокам и месту проведения работ.

6.9. По итогам тестирования Плана ДИБ подготавливается протокол о результатах тестирования с указанием:

1) перечня информационных систем и их объектов, по которым проведено тестирование, а также места нахождения основного и резервного центров;
2) времени, затраченного на восстановление работы информационных систем и их объектов;
3) выявленных уязвимостей и предложений по их устранению.

Сведения о результатах тестирования представляются ДИБ в Национальный Банк Республики Казахстан (далее – Национальный Банк) в течение 15 (пятнадцати) рабочих дней после утверждения документа о результатах тестирования уполномоченным органом Компании.

6.10. При возникновении сбоя (простоя) в работе информационной системы ДИТ обеспечивает восстановление работы основного центра.

При отсутствии возможности восстановления работы основного центра в период минимально допустимого срока восстановления осуществляется перевод информационной системы на работу резервного центра.

Стандартный норматив времени по переводу информационной системы на резервный центр должен составлять не более четырех часов с момента возникновения сбоя (простоя).

При возникновении сбоя (простоя) в работе информационной системы Компании, повлекшего прерывание доступа клиентов к услугам посредством систем удаленного доступа, продолжительностью более трех часов ДИБ незамедлительно уведомляет Национальный Банк путем направления электронного сообщения. В случае возникновения сбоя (простоя) в нерабочее время, ДИБ уведомляет Национальный Банк не позднее 10.00 часов времени города Астаны рабочего дня, следующего за днем возникновения сбоя (простоя).

6.11. ДИТ в направляемых клиентам уведомлениях о планируемом введении в действие изменений (обновлений), вносимых в технические, программные и другие средства, обеспечивающие работу информационной системы, и влияющих на доступность клиенту услуг, указывает вид услуг, на доступность которых повлияют планируемые изменения, а также время их предполагаемой недоступности. Минимальные требования по доведению до сведения клиентов уведомления о планируемых изменениях включают размещение оповещений на интернет-ресурсе Компании.

6.12. ДИБ ежегодно, не позднее 10 января года, следующего за отчетным годом, направляет в Национальный Банк информацию в произвольной форме о произошедших в течение отчетного периода плановых и внеплановых простоях (сбоях) в работе информационной системы.

Сведения включают информацию о виде услуги, доступ к которой был приостановлен клиентам, дате, времени начала и завершения простоя (сбоя), предпринятых действиях и результатах работ по устранению простоя (сбоя).

6.13. В случае отсутствия простоев (сбоев) в работе информационной системы, ДИБ уведомляет Национальный Банк об отсутствии простоев (сбоев) в работе информационной системы за отчетный квартал.

7. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

7.1. Правила вступают в силу с даты их утверждения решением Правления Компании и действуют до их отмены соответствующим решением Правления или принятия в новой редакции.

7.2. Правила должны быть доведены до сведения всех работников путем проставления подписи в листе ознакомления с Правилами либо подписания в системе электронного документооборота.

7.3. В остальном, что не урегулировано Правилами, необходимо руководствоваться законодательством РК.

7.4. Руководители структурных подразделений и работники Компании несут ответственность за несвоевременное и/или ненадлежащее соблюдение и/или несоблюдение положений настоящих Правил.