АКЦИОНЕРНОЕ ОБЩЕСТВО «ФИНФОРТ МП»
(АО «ФИНФОРТ МП»)

Утверждены
приказом генерального директора
АО «Финфорт МП»
№ МП21/22ОД от 20» июня 2022 г.

Правила защиты и раскрытия информации

(версия – 1.0)

Москва
2022

ОГЛАВЛЕНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Правила защиты и раскрытия информации АО «Финфорт МП» (далее – Правила) определяют способы хранения, защиты, а также раскрытия информации при осуществлении АО «Финфорт МП» (далее – Организация) деятельности оператора финансовой платформы.

1.2. Настоящие Правила разработаны в соответствии с законодательством Российской Федерации и нормативными актами Банка России, в том числе:

- Федеральным законом № 211-ФЗ от 20.07.2020 «О совершении финансовых сделок с использованием финансовой платформы»;
- Положением Банка России № 757-П от 20.04.2021 «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций»;
- Уставом АО «Финфорт МП»;
- Правилами финансовой платформы АО «Финфорт МП».

1.3. К информации, которая подлежит защите в соответствии с настоящими Правилами, относятся сведения, которые составляют конфиденциальную информацию, в том числе (но не исключительно):

- информация, содержащаяся в документах, сформированных в электронном виде оператором финансовой платформы, потребителем финансовых услуг, финансовой организацией (эмитентом), регистратором финансовых транзакций при совершении финансовых сделок;
- информация обо всех совершенных финансовых сделках, а также о расчетах по финансовым сделкам, предоставленная оператором финансовой платформы в адрес регистратора финансовых транзакций;
- информация, отраженная в документах, сформированных в электронном виде работниками или клиентами оператора финансовой платформы при осуществлении финансовых операций (сделок);
- информация, необходимая оператору финансовой платформы для авторизации пользователей финансовой платформы в целях осуществления финансовых операций (сделок), а также в целях удостоверения права пользователей (участников) распоряжаться денежными средствами и иным имуществом;
- информация об осуществленных оператором финансовой платформы и пользователями финансовой платформы финансовых операциях (сделках);
- ключевая информация средств криптографической защиты информации, используемая при осуществлении финансовых операций (сделок).

1.4. Организация осуществляет хранение и защиту информации, связанной со своей деятельностью, в том числе путем создания резервной копии (дублированного хранения информации) и наличия процедур, направленных на предотвращение технических сбоев и ошибок в части хранения и защиты информации, содержащейся в финансовой платформе.

2. ОРГАНИЗАЦИЯ ДЕЯТЕЛЬНОСТИ СЛУЖБЫ БЕЗОПАСНОСТИ

2.1. Ответственность за разработку и осуществление мер, направленных на предотвращение неправомерного использования защищаемой информации, возлагается на службу безопасности Организации.

2.2. Права, обязанности и ответственность работников службы безопасности определены «Положением о службе безопасности АО «Финфорт МП» и должностными инструкциями.

2.3. Принципы, задачи и методы обеспечения информационной безопасности в условиях наличия угроз, характерных и существенных для систем и информационных технологий Организации, регламентированы «Политикой информационной безопасности АО «Финфорт МП».

2.4. Основной целью деятельности службы безопасности по обеспечению информационной безопасности является достижение защищенности бизнес-процессов Организации и минимизация рисков информационной безопасности.

3. РЕГЛАМЕНТАЦИЯ И ДОКУМЕНТИРОВАНИЕ ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ

3.1. Порядок обеспечения безопасности информации, реализуемые меры защиты и иная деятельность по информационной безопасности регламентируется внутренними документами Организации.

3.2. В процессе функционирования системы управления информационной безопасностью должны создаваться записи с целью определения соответствия требованиям по обеспечению информационной безопасности, а также анализа ее эффективности.

3.3. Записи – это любые документы или иные зафиксированные свидетельства о выполнении требований внутренних документов Организации и об исполнении действий в процессе управления информационной безопасностью. Записями могут служить, в том числе журналы аудита событий информационных систем, иные записи в электронном виде или на бумажном носителе.

3.4. Записи должны сохраняться, защищаться и быть доступными в течение всего срока их хранения в соответствии с требованиями законодательства Российской Федерации и номенклатурой хранения документов и информации Организации.

3.5. Защита электронных записей осуществляется в соответствии с требованиями, установленными «Положением о порядке защиты информации АО «Финфорт МП». Записи на бумажных или отчуждаемых магнитных носителях, содержащие сведения конфиденциального характера, хранятся в металлических шкафах, сейфах или специально оборудованных помещениях.

4. ЗАЩИТА ИНФОРМАЦИИ

4.1. **Обеспечение защиты информации при управлении доступом и регистрацией**

4.1.1. Предоставление доступа к информационным системам и ресурсам Организации осуществляется в соответствии с требованиями «Положения о порядке предоставления доступа к информационным системам АО «Финфорт МП».

4.1.2. Порядок предоставления прав доступа к информационным системам:

- предоставление (изменение) доступа возможно только на основе заявки с обоснованием необходимости запрашиваемого доступа и одобренной руководителем работника, запрашивающего доступ, владельца системы, специалистами информационной безопасности, специалистом экономической безопасности и другими работниками (при необходимости);
- права доступа могут быть изменены в следующих случаях:
  - выполнение работником своих должностных или договорных обязанностей;
  - увольнение работника или прекращение деятельности представителя внешней стороны;
  - перевод работника в другое подразделение внутри Организации;
  - выполнение процедуры мониторинга учетных записей и прав доступа к информационным системам;
  - расследование или предупреждение инцидента информационной безопасности;
- непосредственный доступ к информации на бумажном носителе осуществляется руководителем подразделения, которое отвечает за обеспечение работы с указанной информацией.

4.1.3. Работниками службы безопасности осуществляется регулярный контроль предоставленных прав доступа.

4.2. **Обеспечение защиты информации при назначении и распределении ролей**

4.2.1. Организация принимает все доступные меры для обеспечения защиты информации, в том числе при назначении и распределении ролей в информационной системе.

4.2.2. Защита информации при назначении и распределении ролей в информационной системе обеспечивается посредством реализации следующих мер:

- реализация принципа «знай своего клиента (контрагента)»;
- распределение прав и обязанностей работников в соответствии с принципом «запрещено все, что не разрешено явно»;
- наличие должностной инструкции для каждой штатной едициницы, определяющей должностные обязанности и полномочия;
- предоставление работнику доступа только к информации и сведениям, необходимым для выполнения своих должностных обязанностей в пределах предоставленных полномочий;
- индивидуальная идентификация пользователя, то есть установление идентификатора (учетной записи), в соответствии с которым осуществляется разграничение доступа к информации;
- наличие подписанного каждым работником соглашения о конфиденциальности, регламентирующего запрет на неправомерное использование информации и сведений, составляющих конфиденциальную информацию, а также их разглашение;
- установление перечня лиц, имеющих доступ к информации и сведениям, относящимся к деятельности финансовой платформы.

4.3. **Обеспечение защиты информации средствами антивирусной защиты**

4.3.1. Обеспечение защиты информации средствами антивирусной защиты осуществляется в соответствии с требованиями «Положения об антивирусной защите АО «Финфорт МП».

4.3.2. Защита информации средствами антивирусной защиты обеспечивается в соответствии со следующими принципами:

- внедрение и корректное функционирование системы антивирусной защиты с регулярным обновлением вирусных баз на всех рабочих станциях и серверах;
- работа в информационной инфраструктуре (в том числе удаленно) без корректно функционирующих средств антивирусной защиты, а также с устаревшими обновлениями антивирусных баз запрещена;
- самостоятельное удаление или отключение средств антивирусной защиты запрещено;
- обязательный контроль на отсутствие вредоносного программного обеспечения любой информации (текстовые файлы любых форматов, файлы данных, исполняемые файлы, файлы архивов и т.п.), хранение которой осуществляется на рабочих станциях и серверах, информации, получаемой и передаваемой по телекоммуникационным каналам, а также информации на съемных носителях (USB-накопителях, магнитных дисках т.п.);
- проверка на отсутствие вредоносного программного обеспечения установочных файлов любого устанавливаемого на рабочие станции или серверы программного обеспечения;
- проверка на отсутствие вредоносного программного обеспечения почтовых сообщений, WEB-трафика, а также файлов;
- проверка, в том числе сканирование всех файлов на жестком диске на предмет заражения проводится в режиме реального времени и по расписанию;
- централизованное управление и регулярное обновление всех средств антивирусной защиты с применением механизма автоматического обновления.

4.4. **Обеспечение защиты информации при использовании ресурсов сети Интернет**

4.4.1. Обеспечение защиты информации при использовании ресурсов информационно-телекоммуникационной сети Интернет осуществляется в соответствии с «Положением о порядке защиты информации АО «Финфорт МП».

4.4.2. Защита информации при использовании ресурсов информационно-телекоммуникационной сети Интернет обеспечивается посредством реализации следующих мер:

- использование работниками сети Интернет только в служебных целях;
- для доступа к сети Интернет используется только разрешенное программное обеспечение;
- технические меры, предотвращающие доступ работникам к небезопасным ресурсам и сервисам сети Интернет;
- применение технических средств защиты от сетевых атак.

4.5. **Обеспечение защиты информации на этапах жизненного цикла финансовой платформы**

4.5.1. Процесс обеспечения информационной безопасности и защиты информации осуществляется в следующем порядке

1) разработка технического задания – определение функциональных требований и требований по информационной безопасности;
2) проектирование – определение структуры и характеристик разрабатываемой системы, состава технических и программных средств, в том числе средств защиты информации, требований к настройке и эксплуатации этих средств, параметры их взаимодействия; проверка программного обеспечения на наличие уязвимостей;
3) разработка и тестирование – на данном этапе применяются следующие меры безопасности процесса:
   - разработка осуществляется в специально выделенных сегментах корпоративной сети Организации;
   - применяются только лицензированные средства разработки и отладки программного кода;
   - разработка осуществляется на основании планов и методов, определенных в техническом задании и проектной документации;
   - тестирование осуществляется, в том числе посредством проверки логики работы программного кода, входных и выходных данных, целостности информации, а также контроль внутренней обработки данных;
   - в тестовой среде не должны использоваться данные, которые могут содержать конфиденциальную информацию;
   - разработчикам запрещается проводить приемочное тестирование собственных разработок, а работник, проводящий тестирование не имеет прав на ввод в действие новых версий систем без согласования;
4) приемка – включает в себя следуюшие виды проверок:
   - правильности функционирования финансовой платформы при выполнении каждой функци;
   - качества реализации защитных мер;
   - совместимости финансовой платформы с уже используемыми техническими средствами и отсутствия конфликтов между ними;
   - полноты и качества документации;
5) ввод в экслуатацию – осуществляется после настройки средств и механизмов обеспечения информационной безопасности;
6) сопровождение и модернизация – любые действия, связанные с внесением изменений в параметры работы финансовой платформы, в том числе в параметры реализованных мер, осуществляются только уполномоченными специалистами и в порядке, установленном соответствующим внутренними документами Организации.

4.6. **Организационные меры защиты информации**

4.6.1. В целях обеспечения целостности и доступности финансовой платформы, предотвращения сбоев и ошибок, а также обеспечения конфиденциальности информации реализуются следующие организационные меры защиты:

- ограничение доступа посторонних лиц в помещения Организации, в которых расположены рабочие станции работников, непосредственно осуществляющих функции, связанные с управлением финансовой платформой, а также в иные помещения Организации, предусматривающие возможность эксплуатации и получения информации, связанной с деятельностью финансовой платформы, а именно:
  - оборудование системой контроля доступа;
  - размещение рабочих мест и установка оборудования Организации в порядке, исключающем возможность бесконтрольного доступа в указанные помещения, бесконтрольного доступа к оборудованию, а также наблюдения за работой со стороны третьих лиц;
- оснащение рабочих мест работников Организации программно-аппаратными комплексами защиты от несанкционированного доступа;
- установление порядка доступа к финансовой платформе:
  - определение в должностных инструкциях работников Организации их прав, обязанностей и ответственности при работе с финансовой платформой;
  - предоставление доступа к финансовой платформе исключительно работникам финансовой платформы;
  - наделение работников правами, обеспечивающими доступ только к информации и сведениям, необходимым им для выполнения своих должностных обязанностей;
  - контроль регистрации пользователей в финансовой платформе и регистрации попыток несанкционированного доступа;
- проведение службой безопасности контроля перечня лиц, допущенных к работе с информацией и сведениями, которые содержатся в финансовой платформе.

4.7. **Мониторинг анализ обеспечения защиты информации**

4.7.1. Организация на постоянной основе проводит мониторинг и анализ эффективности информационной безопасности финансовой платформы.

4.7.2. Цели мониторинга эффективности информационной безопасности финансовой платформы:
- выявление ошибок в результате обработки информации;
- выявление попыток нарушений и инцидентов информационной безопасности
- выявление мошеннических действий.

4.7.3. Мониторинг и анализ обеспечения защиты информации может проводиться как с применением специальных технических и программных средств контроля, так и без их применения.

4.7.4. Деятельность по анализу эффективности процессов управления информационной безопасностью осуществляется службой безопасности на основании результатов аудита процессов информационной безопасности, а также статистики инцидентов информационной безопасности.

4.8. **Выявление инцидентов информационной безопасности и реагирование на них**

4.8.1. Управление инцидентами информационной безопасности, связанными с деятельностью финансовой платформы, осуществляется в соответствии с «Положением по работе с инцидентами информационной безопасности АО «Финфорт

МП», в котором устанавливаются требования к порядку обнаружения и регистрации инцидентов информационной безопасности, сбора информации об инцидентах и выявлению предпосылок их возникновения для минимизации негативных последствий, а также их расследования и недопущения повторного возникновения.

4.9. **Своевременное совершенствование обеспечения защиты информации**

4.9.1. Процесс обеспечения защиты информации должен постоянно совершенствоваться посредством применения предупреждающих мер, определенных после проведения анализа системы управления информационной безопасностью.

4.9.2. Меры по совершенствованию обеспечения информационной безопасности Организации отражены в «Политике информационной безопасности АО «Финфорт МП».

4.9.3. Реализация мер по совершенствованию обеспечения информационной безопасности:

- распределение функций и ответственности работников Организации в сфере обеспечения информационной безопасности;
- управление документацией системы управления информационной безопасностью;
- управление рисками информационной безопасности;
- мониторинг, анализ эффективности и совершенствование процессов системы управления информационной безопасностью;
- обеспечение информационной безопасности при работе с персоналом;
- повышение уровня знаний и контроль знаний персонала Организации в области информационной безопасности;
- организация работы со сторонними организациями;
- обеспечение физической безопасности и защита оборудования;
- технические и организационные меры обеспечения информационной безопасности;
- управление инцидентами информационной безопасности;
- управление непрерывностью бизнеса;
- соблюдение требования законодательства Российской Федерации;
- использование лицензионного программного обеспечения;
- внутренние аудиты информационной безопасности.

5. ПОВЫШЕНИЕ ОСВЕДОМЛЕННОСТИ РАБОТНИКОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

5.1. Повышение осведомленности работников в сфере информационной безопасности осуществляется в соответствии с «Положением о проведении мероприятий по повышению осведомленности и проверки знаний по вопросам информационной безопасности персонала АО «Финфорт МП» и включает в себя следующее:

- документы и памятки по обеспечению информационной безопасности, непосредственно связанные с функциональной деятельностью работников размещаются на внутреннем ресурсе Организации и доступны для ознакомления всеми работниками;
- первичный инструктаж по соблюдению требований информационной безопасности проводится со всеми работниками Организации при приеме на работу под подпись;

- повышение уровня знаний в области информационной безопасности работников Организации проводится на регулярной основе;
- работники, ответственные за мониторинг и контроль требований информационной безопасности постоянно поддерживают уровень своей компетенции;
- контроль знаний работников в области информационной безопасности проводится на регулярной основе.

6. УПРАВЛЕНИЕ РИСКАМИ НАРУШЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

6.1. В целях создания эффективной системы управления рисками информационной безопасности и достижения полной защищенности финансовой платформы Организация осуществляет деятельность по управлению рисками информационной безопасности, которая является неотъемлемой частью деятельности в области информационной безопасности в целом. Деятельность по управлению рисками информационной безопасности представляет собой непрерывный процесс, который включает в себя совокупность следующих функций:
- определение контекста управления рисками;
- оценка риска;
- обработка риска;
- мониторинг риска;
- контроль риска;
- расчет риска;
- минимизация риска.

6.2. Оценка рисков включает в себя следующие последовательные процедуры:
- идентификация угроз информационной безопасности в отношении оцениваемого информационного актива и их источников;
- идентификация уязвимостей, присущих оцениваемому информационному активу, в следствии которых реализация угроз информационной безопасности в отношении указанного актива становится возможной;
- оценка степени тяжести последствий от реализации угроз информационной безопасности в отношении оцениваемого информационного актива;
- расчет уровня риска.

6.3. По итогам оценки рисков информационной безопасности формируется перечень недопустимых рисков, подлежащий дальнейшей обработке в соответствии с требованиями внутренних документов Организации в области информационной безопасности.

7. ПРАВИЛА РАСКРЫТИЯ ИНФОРМАЦИИ

7.1. Организация в соответствии с Федеральным законом № 211-ФЗ от 20.07.2020 «О совершении финансовых сделок с использованием финансовой платформы» раскрывает на официальном сайте в информационно-телекоммуникационной сети Интернет следующую информацию:
- фирменное наименование оператора финансовой платформы, сведения о государственной регистрации юридического лица, сведения о регистрации оператора финансовой платформы в реестре операторов финансовых платформ;

- место нахождения оператора финансовой платформы;
- устав оператора финансовой платформы;
- правила финансовой платформы, сведения об их регистрации в Банке России;
- размер вознаграждения оператора финансовой платформы или порядок его определения, порядок уплаты такого вознаграждения;
- реквизиты специального счета или счетов оператора финансовой платформы (при наличии);
- перечень лиц, осуществляющих учет прав на ценные бумаги, передача прав на которые потребителям финансовых услуг осуществляется в результате совершения финансовых сделок, заключенных с использованием финансовой платформы;
- перечень лиц, привлекаемых оператором финансовой платформы на основании соглашения для обеспечения размещения в соответствии с правилами финансовой платформы информации о финансовых сделках, совершаемых с использованием финансовой платформы;
- перечень банков, которым оператором финансовой платформы поручено проведение идентификации клиентов – потребителей финансовых услуг при их личном присутствии, представителей клиентов, выгодоприобретателей, бенефициарных владельцев в целях заключения с такими клиентами договора об оказании услуг оператора финансовой платформы;
- сведения о выявленных конфликтах интересов и принятых мерах по минимизации риска их негативных последствий;
- информация о технических сбоях в функционировании программно-аппаратных средств, необходимых для оказания услуг оператора финансовой платформы, в том числе вследствие обстоятельств непреодолимой силы, которые повлекли за собой прекращение или ограничение работоспособности таких средств, что привело к отсутствию возможности осуществления оператором финансовой платформы своей деятельности в отношении всех участников финансовой платформы, с указанием даты, времени и причин прекращения работоспособности таких средств, а также информация о сроках восстановления функционирования программно-аппаратных средств;
- фирменные наименования и места нахождения финансовых организаций и эмитентов, являющихся участниками финансовой платформы. Раскрытие указанной информации может осуществляться в том числе с использованием указателей страниц сайтов таких финансовых организаций и таких эмитентов в информационно-телекоммуникационной сети Интернет или сетевых адресов, позволяющих идентифицировать их сайты в информационно-телекоммуникационной сети Интернет;
- информация о расторжении договора об оказании услуг оператора финансовой платформы между оператором финансовой платформы и финансовой организацией или эмитентом и о последствиях расторжения такого договора;
- иная информация в случае, если требование о ее раскрытии установлено Банком России.

7.2. Правила финансовой платформы и вносимые в них изменения (новая редакция правил финансовой платформы) подлежат раскрытию на сайте оператора финансовой платформы после их регистрации в Банке России.

7.3. Организация направляет в Банк России информацию обо всех случаях и/или попытках осуществления операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участников финансовой платформы в порядке, установленном Банком России.

8. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

8.1. Настоящие Правила утверждаются генеральным директором и вводятся в действие приказом генерального директора Организации.

8.2. Если в результате изменения законодательных и нормативных актов Российской Федерации отдельные разделы/пункты настоящего Положения вступают в противоречие с ними, эти разделы/пункты утрачивают силу и до момента внесения изменений в настоящее Положение участники бизнес-процесса руководствуются действующим законодательством Российской Федерации.