«УТВЕРЖДЕНО»
Директором
ИП ООО «SILK CAPITAL»

«14» 02 2018 года

ПОРЯДОК

ХРАНЕНИЯ, ЗАЩИТЫ И ВОСТАНОВЛЕНИЯ ИНФОРМАЦИИ ИП ООО «SILK CAPITAL»

Ташкент – 2018 год

РАЗДЕЛ I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Порядок разработан в соответствии с Законом Республики Узбекистан «О рынке ценных бумаг», Положением «О внутреннем контроле профессионального участника рынка ценных бумаг» (рег. №1899 от 6 февраля 2009 г.) и устанавливает порядок хранения, защиты и восстановления информации, в том числе перечень мер, направленных на неправомерное использование конфиденциальной информации инвестиционного консультанта, инвестиционного посредника и доверительного управляющего инвестиционными активами Иностранного предприятия общество с ограниченной ответственностью «SILK CAPITAL» (далее – Общество).

1.2. В настоящем Порядке используются следующие основные понятия:

профессиональный участник рынка ценных бумаг (далее — профессиональный участник) — Общество, которое осуществляет профессиональную деятельность на рынке ценных бумаг;

конфиденциальная информация — сведения о клиентах профессиональных участников рынка ценных бумаг, состоянии их счетов и проведенных операциях, а также содержании сделок с ценными бумагами (за исключением наименования ценных бумаг, количества, цены, даты, времени заключения, а в случаях проведения биржевых торгов — лиц, участвовавших в торгах);

клиент/контрагент – юридическое или физическое лицо, состоящее в договорных отношениях с Обществом в рамках осуществления профессиональным участником профессиональной деятельности на рынке ценных бумаг в качестве инвестиционного консультанта, доверительного управляющего инвестиционными активами и инвестиционного консультанта;

меры – действия и мероприятия, препятствующие неправомерному использованию конфиденциальной информации лицами, в частности, работниками Профессионального участника, которые имеют непосредственный доступ к Конфиденциальной информации;

работники/сотрудники - лица, выполняющие определенные функции на основании трудового или гражданско-правового договора в рамках деятельности, осуществляемой профессиональным участником.

уполномоченный государственный орган по регулированию рынка ценных бумаг — Центр по координации и развитию рынка ценных бумаг при Госкомконкуренции Республики Узбекистан.

1.2. Порядок определяет правила хранения и восстановления информации, порядок доступа сотрудников общества к информации и меры по информационной безопасности.

Цели информационной безопасности:

создание безопасного информационного пространства для осуществления профессиональным участником своей деятельности, как самостоятельно, так и в сотрудничестве с другими субъектами и системами финансово-экономической и другой деятельности;

соблюдение интересов вышестоящих организаций и предприятий, клиентов и партнеров в вопросах обеспечения информационной безопасности;

Задачи информационной безопасности:

главной задачей является создание условий для обеспечения хранения, защиты и восстановления информации, а также предупреждения и пресечения неправомерного использования конфиденциальной информации, выполнение которой предусматривается по следующим направлениям:

- определение и классификация информационных объектов, на основе которых профессиональный участник осуществляет свою деятельность, изменение и дополнение списка данных объектов с учетом меняющихся условий;

- учет программного, аппаратного и другого информационного обеспечения, позволяющего создавать, хранить, обрабатывать или уничтожать информационные объекты;

- разработка механизмов оценки состояния информационной безопасности и сокращения ущерба от результатов нарушений во всех аспектах.

1.3. Хранение, защита и восстановление документов, в том числе по делопроизводству, трудовым отношениям, бухгалтерской деятельности и финансовой отчетности по предусмотренным обстоятельствам осуществляется также в соответствии с Правилами внутреннего учета оказываемых ИП ООО «SILK CAPITAL» услуг, совершаемых им операций и сделок на рынке ценных бумаг и иными внутренним документами профессионального участника.

II. ОСНОВНЫЕ ПРАВИЛА И ПРОЦЕДУРЫ.

2.1. Профессиональный участник осуществляет хранение следующих основных документов и информации:

договора, заключенные с клиентами, дополнения, изменения и приложения к ним, отчеты по исполнению договоров;

договора купли-продажи ценных бумаг, договора поручений, договора на оказание депозитарных услуг;

выписки по счетам депо;

входящая и исходящая письменная документация;

внутренняя документация (решение учредителей о создании общества, протоколы общих собраний, штатное расписание, приказы, распоряжения, инструкции, положения и другие в соответствии с номенклатурой дел);

финансовая отчетность, документы бухгалтерского учета;

учредительные документы (учредительный договор, устав, внесенные в них изменения и дополнения, свидетельство о государственной регистрации Общества, перерегистрации, регистрации изменений и дополнений в устав);

документальная информация о юридических лицах и их деятельности, инвестиционные активы которых переданы в доверительное управление (учредительный договор, устав общества, внесенные в них изменение и дополнения; документы, утверждаемые общим собраниями и иными органами управления обществ; документы финансовой отчетности, протоколы общих собраний, заседаний наблюдательного совета, ревизионной комиссии, аудитора и другие сведения и информация);

иные документы в соответствии с внутренними регламентами, порядками и правилами, а также законодательством.

2.2. Вышеуказанная документальная информация содержится в учетных папках-регистрах, скоросшивателях, папках, делах с подписанными на них наименованиями о виде содержащейся информации, а также в электронной форме.

2.3. Основные направления действий общества, по выполнению процедур информационной безопасности:

регулярные работы (процедуры), для поддержания средств информационно-коммуникационных технологий в защищенном состоянии;

защита от несанкционированного доступа;

выбор наименования пользователя и пароля;

меры безопасности при выполнении специальных работ на ИКТ (удаление, перемещение и архивирование файлов и др).

2.4. Регулярные процедуры.

Для успешного выполнения процедур информационной безопасности, пользователи должны обладать необходимыми знаниями и навыками. Порядок и способы выполнения основных процедур информационной безопасности излагаются ниже.

2.5. Профилактические работы.

2.6. Процедуру проверки диска в сокращенном виде рекомендуется производить каждый день при загрузке (первом включении) компьютера.

2.7. Процедуру проверки диска в полной форме рекомендуется выполнять раз в неделю по окончании рабочего дня.

2.8. Процедуру оптимизации (сжатия) диска (defrag) рекомендуется выполнять после массового удаления больших объемов данных, а также после стирания конфиденциальной информации для воспрепятствования ее восстановлению.

2.9. Для пользователя компьютера с операционной системой Windows выполнение вышеописанных процедур перекладывается на саму систему или на системного администратора.

2.10. Установка режима ожидания (screen saver).

2.11. Антивирусная работа.

Последствия заражения ИКТ вирусом могут быть самыми разнообразными – от замедления работы до полной потери данных. Поэтому основной задачей пользователя является не допущение проникновения вируса на его ИКТ или скорейшее уничтожение вируса, если проникновение уже произошло.

2.12. Предварительные меры.

Любые данные, направляемые в ИКТ должны проходить процедуру проверки на вирусы. Особенно это касается перенесения электронной информации с внешнего магнитного носителя. Кроме того, вирусы могут попадать по электронной почте, модему, через открытые каталоги и пр.

2.13. Уничтожение вирусов.

Каждый сотрудник должен следить за тем, чтобы на ИКТ был установлен набор антивирусного программного обеспечение, снабженный возможность запуска пользователем данного ИКТ. Сотрудник должен регулярно обращаться к соответствующим специалистам для обновления указанного программного обеспечения.

В случае подозрения на заражение вирусом, поступлении данных извне, пользователь должен запустить антивирусное программное обеспечение для обнаружения и уничтожения вирусов.

2.14. Защита от несанкционированного доступа к данным.

Пароль на включение компьютера. Там где это возможно, ИКТ следует защищать паролями на включение (на вход).

Не следует сообщать пароль для ввода другим лицам – в этом случае секретность пароля теряет смысл. Способ использования пароля в работе и уровень его конфиденциальности определяются выполняемыми на данном устройстве задачами.

Следует помнить, что если пароль забыт или утерян, то приведение компьютера в рабочее состояние возможно только после длительной процедуры, связанной в частности с физическим вскрытием процессорного блока.

Во избежание неприятностей, связанных с выполнением этой процедуры, следует хранить дубликат пароля в сейфе Директора профессионального участника.

При необходимости зашифровать и защитить паролем отдельный файл, используется простой способ их шифрации, подготовленный в редакторах Word или Excel. В этом случае следует при сохранении файла выбрать режим Save as, далее щелкнуть по кнопке Option и выбрать режим Save (выбирается по умолчанию). В нижней части, в окошке Protection Password следует набрать пароль, после нажатия Enter, набрать пароль повторно и снова нажать Enter. После этого файл сохранить. Теперь при попытке открыть данный файл будет запрашиваться пароль.

Следует помнить, что в случае, если пароль забыт, данные файла являются потерянными.

2.16. Специальные работы.

Значительный ущерб работе информационных систем и схемам безопасности технологий, наносятся пользователями неосознанно при удалении электронных файлов или при перенастройке ИКТ.

2.17. Работа с файлами.

При удалении, перемещении, архивировании файлов следует соблюдать осторожность. Работать следует только с теми файлами, которые созданы самим пользователем. Запрещается удалять, перемещать, архивировать системные файлы или любые файлы, в назначении которых пользователь неуверен.

2.18. План восстановления деятельности в случае катастрофы.

План восстановления является составной частью общего пакета документов, определяющих регламент информационной безопасности и предназначенные для определения действий, которые необходимо выполнять для того, чтобы правильно следовать Процедурам Информационной Безопасности. Документ разделяется на следующие части:

2.19. Классификация аварий и катастроф.

По результатам своего воздействия, аварии и катастрофы разделяются на следующие категории:

Глобальная (разрушающая здание);

Локальная (частичные разрушения внутри здания):

- разрыв связи;
- сбой компьютеров;
- ошибки операторов;
- отключение электропитания;
- прочие.

2.21. Мероприятия по восстановлению критически важных процессов.

В случае если произошла авария или катастрофа, приведшая к остановке бизнес деятельности, необходимо проведение определенных восстановительных мероприятий.

Предварительные процедуры.

- Резервное копирование.

Основой восстановления данных после аварий является резервное копирование. Для каждого критического объекта информационной среды общества необходимо сохранять оперативный срез состояния объекта.

- Источники бесперебойного питания (ИБП).

Для обеспечения безопасного перехода с основного на резервное электропитание, предусматриваются комплекты источников бесперебойного питания.

- Резерв персональных компьютеров.

Для обеспечения быстрого восстановления информационной компьютерной среды в случае массового выхода из строя аппаратного обеспечения (региональная катастрофа), предусматривается резервный компьютер.

Процедуры после устранения аварии.

Сразу после устранения основных последствий аварии или катастрофы пользователи (сотрудники) обязаны провести анализ причин, полную оценку последствий и план полного их устранения, а также выяснить и, по возможности, устранить причины ошибок и сбоев, возникавших при восстановительных работах.

Процедуры пользователей информационной сети.

Аппаратно-технические меры безопасности.

Для обеспечения информационной безопасности, на вверенной ему единице средства вычислительной техники, пользователь должен в первую очередь обеспечить надежную работу устройства доступными ему способами. Это необходимо для того, чтобы избежать сбоев аппаратного и программного обеспечения в результате механических воздействий на устройства, неправильного включения в сеть и по другим причинам.

Перед включением компьютера и началом работы необходимо произвести внешний осмотр места его установки. Категорически запрещается загораживать специальные вентиляционные отверстия на панелях системного блока и монитора. Необходимо убедиться, что устройство включено в сеть гарантированного электропитания (если таковая имеется).

Запрещается производить включение кондиционеров, обогревателей и другие посторонние электротехнические устройства в электрическую сеть гарантийного питания, предназначенную для компьютеров, а также размещать их поблизости от ИКТ.

Нельзя изгибать или ломать кабель локальной вычислительной сети (ЛВС) проходящий в каждом помещении и другие кабели, соединяющие различные части ИКТ. Нельзя отключать кабель, соединяющий устройство и розетку ЛВС. Нельзя допускать повреждения розеток ЛВС и любых кабелей ИКТ, например, при перемещении стульев и другой мебели.

Запрещается ставить посторонние предметы (скрепки, чашки, сумки и т.п.) на корпус компьютера, монитор, клавиатуру и другие периферийные устройства.

Нельзя самовольно подключать или отключать ИКТ, его блоки или узлы к источникам питания и тем более производить самостоятельный ремонт устройств.

Запрещается самостоятельно перемещать компьютер и отдельные его блоки. При необходимости перемещения техники, вызывать специалиста.

Нельзя размещать рядом с компьютером любое другое электронное оборудование, кроме того, которое было установлено специалистами.

Категорически запрещается курить в помещениях, где находятся компьютеры. При долговременном оставлении рабочего места необходимо выключать монитор.

III. УГРОЗЫ ОБЪЕКТАМ

3.1. Объект информационной среды может быть подвержен следующим угрозам:

- уничтожение, без возможности восстановления;
- повреждение, без возможности восстановления;
- прекращение доступа к объекту;
- замедление доступа к объекту;
- отказ субъекта от использования объекта по субъективным причинам;
- изъятие объекта вместе с носителем;
- копирование объекта на месте хранения;
- копирование объекта при передаче по линии связи;
- копирование объекта при обработке;
- овладение системной информацией для получения доступа к объекту;
- замена одного объекта другим;
- создание ложного объекта, похожего на настоящий;
- изменение объекта на месте хранения;
- изменение объекта при передаче;
- изменение объекта при обработке;
- изменение системной среды для получения доступа к объекту.

Вышеперечисленные угрозы могут быть реализованы для конкретного объекта, как по отдельности, так и в различных комбинациях.

Как видно, все указанные угрозы укладываются в три раздела: доступность, конфиденциальность, целостность.

3.2. В соответствии с описанными угрозами объектам, система информационной безопасности должна решать задачи по достижению следующих целей:

- запрет или значительное ограничение несанкционированного доступа к объектам;
- разграничение санкционированного доступа к объектам;
- защита объектов от несанкционированного копирования и модификации;

- учет и регистрация санкционированного копирования, модификации и других действий с объектами;
- создание и хранение резервных копий объектов;
- защита системной среды от изменений.

Описанные цели касаются всех этапов существования объекта: хранения, передачи и обработки.

IV. МЕРЫ, НАПРАВЛЕННЫЕ НА НЕПРАВОМЕРНОЕ ИСПОЛЬЗОВАНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

4.1. Защита конфиденциальной информации профессиональными участниками осуществляется в целях предотвращения утечки, хищения, утраты, искажения, блокировки, подделки конфиденциальной информации и иного несанкционированного доступа к ним, а также предотвращения несанкционированных действий по уничтожению, блокированию, копированию, искажению конфиденциальной информации и других форм вмешательства в информационные ресурсы и информационные системы профессиональных участников.

4.2. Целью применения Мер является:

- исключение возможности неправомерного использования Конфиденциальной информации Работниками Профессионального участника и третьими лицами в собственных интересах в ущерб интересам клиента/контрагента профессионального участника и самого Профессионального участника;
- повышение уровня доверия к профессиональному участнику со стороны клиента/контрагента;
- снижение рисков на рынке ценных бумаг.

4.2. Меры, связанные с ограничением доступа посторонних лиц в помещения подразделений Профессионального участника, предназначенные для осуществления профессиональной деятельности на рынке ценных бумаг или эксплуатации информационно-технических систем:

4.2.1. Размещение помещений подразделений Профессионального участника и оборудования способом, исключающим возможность бесконтрольного проникновения в эти помещения и к этому оборудованию посторонних лиц, включая работников других подразделений;

4.2.2. Соблюдение при размещении рабочих мест работников принципа разделения по функциональному признаку (в частности, по различным видам деятельности при их совмещении либо по выполняемым функциям);

4.2.3. Использование технических средств, специального оборудования и/или услуг специальных организаций для предотвращения доступа посторонних лиц в

помещения, занимаемые профессиональным участником, как в рабочее, так и во внерабочее время.

4.3. Меры, связанные с ограничением распространения конфиденциальной информации, полученной в процессе переговоров:

4.3.1. Проведение переговоров с клиентом/контрагентом профессиональным участником в специальном помещении, обеспечивающем режим конфиденциальности информации.

4.4. Меры по разграничению прав доступа при вводе и обработке данных с целью защиты от несанкционированных действий работников разных подразделений профессионального участника, а также процедура ограничения доступа работников профессионального участника к конфиденциальной информации:

4.4.1. Четкое разграничение прав и обязанностей работников профессионального участника на уровне должностных инструкций и/или внутренних документов профессионального участника.

4.4.2. Обеспечение доступа работников только к сведениям, необходимым им для выполнения своих прямых служебных обязанностей в пределах предоставленных полномочий, в частности, путем применения организационных мер (издания соответствующих приказов).

4.4.3. Ограничение доступа к конфиденциальной информации путем использования возможностей программного обеспечения: наличие систем разграничения доступа к разным уровням баз данных и операционной среды на уровне локальной сети; доступ к данным только с определенных автоматизированных рабочих мест (запрет либо ограничение на использование удаленного доступа к данным); ведение автоматизированного журнала регистрации пользователей информационной системы и регистрации попыток несанкционированного доступа к данным, содержащим конфиденциальную информацию.

4.5. Меры по защите рабочих мест и мест хранения документов от беспрепятственного доступа и наблюдения, защиты конфиденциальной информации
от неправомерного использования, предусматривающие следующие мероприятия:

4.5.1. Размещение рабочих мест сотрудников таким образом, чтобы исключить возможность несанкционированного просмотра документов и информации, отраженной
на экранах мониторов.

4.5.2. Использование надежных технических систем защиты конфиденциальной информации.

4.5.3. Соблюдение процедур, регламентирующих порядок хранения и уничтожения документов, содержащих конфиденциальную информацию.

4.5.4. Соблюдение процедур, необходимых для защиты документов и информации при доставке/передаче их клиенту/контрагенту, в частности, включение в договоры с клиентом/контрагентом положений, регламентирующих порядок доставки документов/передачи информации и подтверждения их получения.

4.6. Организационные меры:

4.6.1. Четкое определение состава конфиденциальной информации, к которой имеет доступ конкретный работник, на уровне должностных инструкций, приказов, иных внутренних документов профессионального участника, которые доводятся до сведения работника.

4.6.2. Включение в трудовой договор условий/приложений к договору о неразглашении работниками охраняемой законом конфиденциальной тайны.

4.6.3. Разработка правил обмена конфиденциальной информацией.

4.6.4. Доведение до сведения работников правил обмена конфиденциальной информацией и мер ответственности за неправомерное использование конфиденциальной информации.

4.6.5. Применение дисциплинарной ответственности, в т.ч. наложение материальных взысканий на работников за несанкционированное предоставление конфиденциальной информации работникам других подразделений профессионального участника и третьим лицам.

4.7. Контроль за корректностью содержания размещаемых в СМИ сообщений и высказываний работников организации.

РАЗДЕЛ V. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

5.1. Настоящего Порядка вступает в силу со дня его утверждения Директором профессионального участника.

5.2. В случае если одно из правил настоящего Порядка утратило силу, это правило не является причиной для приостановления других правил.

5.3. Если действующими законодательными актами Республики Узбекистан либо уставом профессионального участника установлены иные положения, чем предусмотрено настоящим Порядком, то применяются правила действующих законодательных актов Республики Узбекистан и устава профессионального участника.

№ п/п	Наименование мероприятий	Срок исполнения	Ответственные лица
	Формирование системы информационной безопасности		
1.	Подготовка персонала в вопросах взаимоотношений с правоохранительными, контролирующими и надзорными органами, а также другими категориями посетителей	Постоянно	директор
2.	Обеспечение физической безопасности носителей информации (внутрифирменные и охранно-пропускной режимы)	Постоянно	директор
	Организация защиты информации на бумажных носителях		
1.	Приобретение специальных шкафов и оборудования с ограниченным доступном (сейфы и т.д.), обеспечивающих безопасное и надежное хранение информации на бумажных носителях	По мере необходимости	директор
	Организация защиты информации на электронных носителях		
1.	Контроль доступа за осуществлением политики безопасности, автоматическое обнаружение и предотвращение вирусного и иного проникновения в сеть	Постоянно	директор
2.	Защита от несанкционированного доступа - применение систем обеспечения конфиденциальности информации при её передачи по телекоммуникационным каналам и хранении	Постоянно	директор