«УТВЕРЖДЕН»
Приказом №_____
Генеральным директором
ЗАО «Золотой Дракон Азия»
«__» _____ 2023 года

_____

Правила, регламентирующие порядок обеспечения информационной безопасности (кибербезопасности), непрерывной деятельности, зашиты прав потребителей и обработки персональных данных (далее по тексту – Правила)

Настоящие Правила разработаны Закрытым Акционерным Обществом «Золотой Дракон Азия» (далее по тексту – Общество) в соответствии с Законом Кыргызской Республики «О виртуальных активах». Законом Кыргызской Республики «О защите прав потребителей». Законом Кыргызской Республики «Об информации персонального характера». Постановлением Кабинета Министров Кыргызской Республики «О вопросах регулирования отношений, возникающих при обороте виртуальных активах». Положением «О деятельности оператора обмена виртуальных активов и ведении Реестра операторов обмена виртуальных активов» и иными нормативными правовыми актами Кыргызской Республики.

Целью настоящих Правил является регулирование отношений, возникающих между Обществом и клиентами в целях обеспечения '"информационной безопасности (кибербезопасности), непрерывной деятельности Общества, защиты прав потребителей и обработки персональных данных.

Действие настоящих Правил распространяется на всех сотрудников и клиентов Общества.

Изменения и дополнения к настоящим Правилам разрабатываются и утверждаются Обществом.

1. Общие положения.

1.1. Настоящие Правила предусматривают принятие необходимых мер в целях зашиты информационной системы Общества от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации и в целях обеспечения процесса автоматизированной обработки данных.

1.2. Защита прав клиентов Общества осуществляется в соответствии с Законом Кыргызской Республикой «О защите прав потребителей».

2. Правила пользования информационной системой.

2.1. Ответственность за соблюдение информационной безопасности несет каждый сотрудник Общества.

2.2. Пользователям информационной системы не разрешается: сообщать свои имена учетных записей и пароли друзьям и родственникам, пытаться подобрать пароли, обрабатывая файлы

, хранящие пароли, программами-подборщиками, запускать сетевые сканеры, взламывать

чужие учетные записи, прерывать работу систем, использовать системные ресурсы и электронную почту не по назначению, открывать файлы других пользователей за исключением случаев, когда владелец файла попросил об этом, скачивать файлы, копировать нелицензионное программное обеспечение или позволять другим пользователям копировать нелицензионное программное обеспечение.

2.3. В управлении информационной системой непрерывно используются такие процессы, как планирование, реализация, проверка и совершенствование.

3. 11орядок доступа к конфиденциальной информации.

3.1. В целях обеспечения защиты информации в Обществе, устанавливается следующий порядок допуска к работе с конфиденциальными источниками:

> Решение о доступе работника к определенному разделу информационной системы принимается руководством Общества.

> Специалист по информационным технологиям обеспечивает защиту отдельных файлов и программ от чтения, удаления, копирования лицами, не допущенными к этому.

> Доступ к информационное системе Общества осуществляется только с персональным паролем. Пользователь должен держать в тайне свой пароль. Сообщать свой пароль другим лицам, а также пользоваться чужими паролями запрещается. Имя пользователя и пароль на вход в систему должны быть отличны от имени пользователя и пароля в общую компьютерную сеть Общества.

> Категорически запрещается снимать несанкционированные копни с носителей информации, знакомить с содержанием электронной информации лиц. не допущенных к этому.

4. Физическая безопасность.

4.1. Все объекты критичные с точки зрения информационной безопасности находятся в отдельном помещении, доступ в которое разрешен только сотрудникам, имеющими соответствующее разрешение от руководства Общества.

4.2. Вход в помещение осуществляется через металлическую дверь, оснащенную замками (не менее двух) и переговорным устройством. Копии ключей находятся у должностных лиц Общества.

4.3. Помещение оборудовано принудительной вентиляцией и пожарной сигнализацией. Вход в помещение контролируется системой видеонаблюдения с выходом на мониторы охраны.

4.4. Ключевые дискеты, пароли и прочая конфиденциальная информация хранится в сейфах.

4.5. Доступ в помещение посторонним лицам запрещен. Технический персонал, осуществляющий уборку помещения, ремонт оборудования, обслуживание кондиционера и т.п. может находится в помещении только в присутствии работников, имеющих право находится в помещении в связи с выполнением своих должностных обязанностей.

4.6. Доступ в помещение в неурочное время или в выходные и праздничные дни осуществляется с письменного разрешения Генерального директора Общества.

5. Разграничение прав доступа к программному обеспечению и системам хранения данных.

5.1. Для входа в информационную систему Общества сотрудник должен ввести имя и пароль. Не допускается режимы беспарольного (гостевого) доступа к какой-либо информации.

5.2. В целях защиты конфиденциальной информации Общества организационно и технически разделяются должностные лица Общества, имеющие доступ и работающие с

различной информацией (в разрезе ее конфиденциальности, секретности и смысловой направленности). Данная задача решается с использованием сетевой операционной системы, где в целях обеспечения защиты данных доступ и права пользователей ограничивается персональными каталогами. Права назначаются в соответствии с производственной необходимостью, определяемой руководством.

6. Работа в глобальной сети Интернет.

6.1. К работе с ресурсами сетью Интернет допускаются сотрудники, получившие соответствующее разрешение от руководства Общества (достаточна устная форма).

6.2. Работа сотрудников Общества с электронной почтой сети Интернет допускается на основании отдельного разрешения от руководства Общества (достаточна устная форма).

6.3. При работе с сетью Интернет сотрудникам запрещено:

> Скачивать и устанавливать на компьютер программное обеспечение.

> Посещать ресурсы, не имеющие непосредственного отношения к работе и служебным обязанностям.

> Осуществлять подписку на рассылку информации непроизводственного характера.

> Сообщать адрес электронной почты в непроизводственных целях.

> Пользоваться различными Интернет-пейджерами.

> Использовать Интернет для получения материальной выгоды или непроизводственных целях, в том числе осуществляя торговлю через Интернет.

7. Дублирование, резервирование и раздельное хранение конфиденциальной информации.

7.1. В целях защиты информации от преднамеренного или же непреднамеренного ее уничтожения, фальсификации или разглашения обеспечить:

> ежедневное обязательное резервирование всей информации, имеющей конфиденциальный характер.

> дублирование информации с использованием различных физических и аппаратных носителей.

7.2, Ответственность за хранение и резервирование информации в электронном виде возложить на специалиста по информационным технологиям.

8. Управление непрерывностью.

8.1. В Обществе разрабатывается и поддерживается управляемый и документированный процесс обеспечения непрерывной деятельности Общества, учитывающий требования информационной безопасности, и служащий для того, чтобы препятствовать прерываниям хозяйственной деятельности и защищать критические важные производственные процессы от влияния крупных сбоев или аварий и обеспечивать их своевременное восстановление.

8.2. Планы обеспечения непрерывности определяют общую систему мер. ответственность, необходимые требования и условия для предотвращения прерывания критически важных производственных процессов, обеспечения требуемого уровня доступности информационных ресурсов, сервисов и инфраструктуры, а также восстановления после аварии.

8.3. Последовательность действий и способы взаимодействия персонала в критической ситуации определяются разрабатываемыми в Обществе аварийными процедурами.

9. Порядок обработки персональных данных.

9.1.Обработка персональных данных осуществляется в соответствии с Законом Кыргызской

Республики «Об информации персонального характера» и настоящими Правилами.

9.2.Общество обрабатывает персональные данные на законной и справедливой основе для выполнения своих функций, полномочий и обязанностей, осуществления прав и законных интересов Общества, сотрудников Общества и третьих лиц.

9.3.Сотрудники Общества, непосредственно осуществляющие обработку персональных данных, должны быть ознакомлены до начала работы с положениями законодательства Кыргызской Республики о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику Общества в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, с настоящими Правилами и изменениями к нему.

9.4.Общество получает персональные данные непосредственно у субъектов персональных данных.

9.5.Общество обрабатывает персональные данные автоматизированным и неавтоматизированным способами, с использованием средств вычислительной техники и без использования таких средств.

9.6.Действия по обработке персональных данных включают сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение.

9.7.Условия обработки персональных данных Обществом:

> обработка персональных данных осуществляются с согласия субъекта персональных данных на обработку его персональных данных путем оплаты услуг;

> осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с законодательством Кыргызской Республики:

> обработка персональных данных осуществляется Обществом в соответствии с требованиями законодательства Кыргызской Республики.

9.8. Обработка персональных данных физических лиц может осуществляться без согласия субъекта на обработку персональных данных исключительно в целях заключения С ними соответствующих договоров (в случае исполнения договоров (поставки, оказания услуг» при условии, не распространения и передаче третьим лицам без согласия субъекта персональных данных).

10. Заключительные положения.

10.1. Контроль за исполнением настоящих Правил осуществляется Генеральным директором Общества.

10.2. Лица, виновные в нарушении настоящих Правил, несут ответственность в соответствии с законодательством Кыргызской Республики.

Генеральный директор
ЗАО «Золотой Дракон Азия»
Васюкович Дмитрий Александрович _____