СТАНДАРТ
по обеспечению подрядными организациями информационной безопасности при подключении к корпоративной сети АО «Инвестиционный Дом «Астана-Инвест»

1. Общие положения

1. Настоящий Стандарт по обеспечению подрядными организациями информационной безопасности при подключении к корпоративной сети АО «Инвестиционный Дом «Астана-Инвест» (далее - Стандарт) разработан с целью обеспечения информационной безопасности АО «Инвестиционный Дом «Астана-Инвест» (далее – Компания) при подключении подрядных организаций, заключивших Договор с Компанией, к корпоративной сети Компании через защищенные каналы связи или подключение персональных компьютеров вышеуказанных подрядных организаций непосредственно в корпоративную сеть Компании.
2. Настоящий Стандарт размещается в открытом доступе на корпоративном сайте Компании по адресу https://investdom.kz/ для ознакомления любой подрядной организацией, желающей выполнять работу либо оказать услугу Компании в будущем или оказывающий/выполняющий такие услуги/работы Компании по действующим договорам.

2. Термины и определения

3. В настоящем Стандарте используются следующие понятия и сокращения:
1) **Компания** - АО «Инвестиционный Дом «Астана-Инвест».
2) **Договор** - договор или иное соглашение, подписанное между Компанией и подрядной организацией, предметом которого либо в процессе исполнения которого возможен любой контакт с корпоративной сетью Компании, либо любого контента Компании в интернете (корпоративный сайт, торговая платформа и т.п.).
3) **Подрядчик –** подрядная организация, заключившие Договор с Компанией. **Действующий подрядчик** -подрядная организация (разработка, техническая поддержка информационных систем, программного обеспечения, сайта и т.п.), которая на момент ознакомления со Стандартом находится с Компанией во взаимодействии по заключенному и действующему договору. **Потенциальный подрядчик** – подрядная организация (разработчка, техническая поддержка информационных систем, программного обеспечения, сайта и т.п.), которая на момент ознакомления со Стандартом, находится в стадии намерения на установление договорных правоотношений с Компанией.
4) **Конфиденциальная информация** - информация, имеющая коммерческую ценность, в том числе потенциальную, в отношении которой установлен режим неразглашения (непубличности).
5) **Мобильные и портативные устройства** - мобильные и/или портативные компьютеры, устройства, носители информации или системы, которые можно легко переносить, перемещать, транспортировать или передавать, используемые в связи с Договором. Примерами таких устройств могут служить ноутбуки, планшеты, внешние жесткие диски, карты памяти, карманные персональные компьютеры, мобильные телефоны и смартфоны, а также любые другие беспроводные или периферийные устройства, на которых можно хранить конфиденциальную информацию и персональные данные.
6) **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
7) **Криптостойкое шифрование** - использование технологий шифрования, длина ключа в которых составляет не менее 256 битов при симметричном шифровании и не менее 2048 битов — при ассиметричном шифровании. Такая длина дает разумно обоснованную гарантию того, что ключ защитит зашифрованную информацию от несанкционированного доступа и обеспечит надлежащую защиту ее конфиденциальности и анонимности.

8) **Технические и организационные меры безопасности** - любые мероприятия, необходимые в соответствии с настоящим Стандартом по обеспечению информационной безопасности Компании.
9) **Третье лицо** - субподрядчики, временные сотрудники Подрядчика, его субподрядчиков или дополнительных подрядчиков и/или представители, действующие от имени Подрядчика.

4. Требования к Подрядчикам

5. Порядок ознакомления и согласия Подрядчика (действующего и потенциального) со Стандартом осуществляется следующим образом:
1) Действующий Подрядчик знакомится со Стандартом на корпоративном сайте Компании и подписывает с Компанией дополнительное соглашение к Договору, предметом которого является выражение согласия со Стандартом и исполнении его требований.
2) Потенциальный Подрядчик знакомится со Стандартом на корпоративном сайте Компании и выражает свое согласие с требованиями Стандарта путем заключения Договора с Компанией, содержащего выражение согласия со Стандартом и исполнении его требований.
6. Подрядчик (действующий и потенциальный), подписывая дополнительное соглашение к Договору либо Договор с условием о согласии со Стандартом, гарантирует и подтверждает, что Подрядчик и третьи лица, привлекаемые им в рамках предоставления продуктов и услуг Компании, обязуются соблюдать технические и организационные меры безопасности, указанные в настоящем Стандарте, в той степени, в какой они применимы к предоставлению услуг и выполнению работ, предусмотренных Договором.
7. Для обеспечения информационной безопасности Компании Подрядчик обязан:
1) Использовать только лицензионные операционные системы и программное обеспечение.
2) Установить и использовать современное антивирусное программное обеспечение, предназначенное для сканирования и быстрого удаления или перемещения в карантин вирусов и других вредоносных программ из любых систем или устройств.
3) Установить и использовать межсетевой экран, ограничивающий взаимодействие устройств Подрядчика и внешних сетей только разрешенными потоками информации.
4) Использовать при работе стойкие пароли или многофакторную аутентификацию.
5) Регулярно производить обновление операционных систем и средств защиты.
6) Использовать криптостойкое шифрование или другие надежные методы для защиты конфиденциальной информации и персональных данных по месту хранения.
7) Не хранить конфиденциальную информацию и персональные данные в электронном виде за пределами сетевой среды Подрядчика (или собственной защищенной компьютерной сети Компании), если устройство хранения данных (например, ленточный накопитель, ноутбук, карта памяти, компьютерный диск и т. д.) не защищено криптостойким шифрованием или другим надежным методом защиты.
8) Не хранить конфиденциальную информацию и персональные данные на съемных носителях (например, флеш-накопителях, картах памяти, ленточных накопителях, компакт-дисках или внешних жестких дисках), за исключением случаев резервного копирования, обеспечения непрерывности деятельности, послеаварийного восстановления и обмена данными, как допускается и требуется в соответствии с Договором.
9) В случае наличия или предоставления Подрядчику в связи с Договором возможности подключения к ресурсам конфиденциальной информации и персональных данных:
   - использовать для подключения ресурсов конфиденциальной информации и персональных данных к ресурсам Подрядчика только взаимно согласованные материально-технические средства и методики.
   - не подключаться к ресурсам конфиденциальной информации и персональных данных без предварительного согласия с Компанией.

- обеспечить Компании доступ к любым задействованным материально-техническим средствам подрядчика в течение рабочего дня с целью выполнения технического обслуживания и поддержки любого оборудования, предоставленного Компанией в соответствии с Договором для подключения к ресурсам конфиденциальной информации и персональных данных.
- использовать любое оборудование, предоставленное Компанией в соответствии с Договором для подключения к ресурсам конфиденциальной информации и персональных данных, исключительно для предоставления услуг или функций, прямо разрешенных в Договоре.

10) Обеспечивать соблюдение принципа наименьших привилегий, согласно которому доступ ограничивается только командами, информацией, системами и другими ресурсами, необходимыми для выполнения задач по Договору.

11) Настроить системы на выполнение автоматического тайм-аута по истечении максимального периода бездействия (15 минут).

12) В случае наличия или предоставления Подрядчику в связи с Договором возможности подключения к ресурсам конфиденциальной информации и персональных данных в дополнение к прочим правам, предусмотренным настоящим Стандартом, разрешать Компании следующее:

- собирать информацию, связанную с доступом, в том числе доступом Подрядчика, к ресурсам конфиденциальной информации и персональных данных. Компания имеет право без дополнительного уведомления собирать, сохранять и анализировать такую информацию с целью выявления потенциальных угроз безопасности. Такая информация может включать данные файлов трассировки, статистические данные, сетевые адреса, а также просмотренные или переданные фактические данные или страницы.
- незамедлительно приостанавливать или прерывать подключение к ресурсам конфиденциальной информации и персональных данных, если Компания по своему единоличному усмотрению считает, что имело место нарушение безопасности, несанкционированный доступ или неправомерное использование информационных объектов Компании или какой-либо информации, систем или других ресурсов Компании.

13) Использовать криптостойкое шифрование или другой надежный метод защиты для передачи конфиденциальной информации и персональных данных за пределы контролируемых Компанией или Подрядчиком сетей или при передаче конфиденциальной информации и персональных данных в любой незащищенной сети. При передаче учетных данных (учетную запись и пароль) передавать их в отдельных сообщениях.

14) По запросу Компании Подрядчик также обязуется вернуть, или, по решению Компании, уничтожить всю конфиденциальную информацию и персональные данные, в том числе все копии на электронных и бумажных носителях, как это предусмотрено в Договоре, или, если не предусмотрено в Договоре, в течение тридцати (30) календарных дней после наступления первого из следующих событий:

- окончания срока действия или прекращения действия Договора.
- получения запроса Компании о возврате конфиденциальной информации и персональных данных.
- если Подрядчику больше не требуется конфиденциальная информация и персональные данные для предоставления услуг в соответствии с Договором.

15) В случае, если Компания выберет вместо возврата конфиденциальной информации и персональных данных ее уничтожение, в письменном виде подтвердить факт полного и безвозвратного уничтожения конфиденциальной информации и персональных данных. Полностью уничтожить все копии конфиденциальной информации и персональных данных во всех местах и системах, где хранится конфиденциальная информация и персональные данные, в том числе системах ранее утвержденных третьих лиц подрядчика. Такая информация должна быть уничтожена с соблюдением процедуры полного уничтожения. До уничтожения Подрядчик обязуется соблюдать все применимые технические и организационные меры безопасности для

защиты безопасности, анонимности и конфиденциальности персональных данных и конфиденциальной информации.

16) Обеспечить реагирование на инциденты и связанные с ним процедуры, незамедлительно и ни в коем случае не позднее чем через двадцать четыре (24) часа сообщать Компании о любых предполагаемых или подтвержденных атаках, вторжениях, случаях несанкционированного доступа, потере или других инцидентах, касающихся информации, систем или других ресурсов Компании.

17) После первоначального оповещения Компании регулярно предоставлять актуальную информацию о ходе реагирования на инцидент, в том числе, помимо прочего, информировать о мерах, принятых для устранения такого инцидента, через взаимно согласованные промежутки времени на протяжении всего срока существования инцидента, и в разумно возможный кратчайший срок после устранения инцидента предоставить Компании письменный отчет, содержащий описание инцидента, меры, принятые Подрядчиком в ходе реагирования, и планы дальнейших действий Подрядчика по предотвращению подобных инцидентов.

18) Не разглашать публично сведения о любых подобных нарушениях неприкосновенности информации, систем или других ресурсов Компании без получения предварительного согласования Компании.

4. Ответственность

8. Ответственность за соблюдение настоящего Стандарта, в том числе за действия привлеченных к исполнению Договора третьих лиц, несет Подрядчик.

9. В случае нарушения Подрядчиком либо привлеченным им третьим лицом требований настоящего Стандарта, Компания оставляет за собой право приостановить доступ к корпоративной сети Компании до момента устранения Подрядчиком нарушений. При повторном нарушении Подрядчиком требований Стандарта, Компания вправе расторгнуть Договор с Подрядчиком и/или применить санкции, предусмотренные Договором.

10. Подрядчик самостоятельно отслеживает изменения в Стандарте, информирование Заказчиком Подрядчика осуществляется в рабочем порядке установленными контактными лицами Заказчика и Подрядчика.

5. Иные условия

11. Настоящий Стандарт обновляется и пересматривается по мере необходимости.