«УТВЕРЖДЕНО»

Председатель Конкурсной комиссии
АКБ «ASIA ALLIANCE BANK»

_____ Норкулов О.О.

КОНКУРСНАЯ ДОКУМЕНТАЦИЯ

по выбору исполнителя на проведение работ
по приведению в соответствие и сертификационному аудиту соответствия требованиям стандарта PCI DSS в АКБ «ASIA ALLIANCE BANK»

Заказчик: Акционерно-коммерческий банк «ASIA ALLIANCE BANK»

Ташкент 2022г.

1. Общие сведения

1. **Область действия конкурса:** настоящая Конкурсная документация разработана в соответствии с требованиями "Положения Акционерного коммерческого банка «ASIA ALLIANCE BANK» о порядке организации установления рыночной стоимости имущества и собственных ценных бумаг, а также определения поставщика товаров, работ и услуг" и регулирует порядок проведения и участия участников конкурса в конкурсе.

2. **Наименование Заказчика:** АКБ «ASIA ALLIANCE BANK», 100047, г.Ташкент, Яшнабадский район, ул. Махтумкули дом №2а Телефон: (+998 71) 231-60-00, факс: (+998 71) 289-55-33

3. **Предмет конкурса:** Проведение работ по приведению в соответствие и сертификационному аудиту соответствия требованиям Стандарта PCI DSS в АКБ «ASIA ALLIANCE BANK»

4. **Вид конкурса**: открытый.

5. **Источник финансирования:** финансируется за счет собственных средств АКБ «ASIA ALLIANCE BANK»

6. **Условия платежа:** предоплата в размере 50% от размера вознаграждения перечисляется на расчетный счет Исполнителя в течении 10 банковских дней с даты подписания контракта. Оставшиеся 50% от размера вознаграждения выплачиваются по факту оказания услуг.

7. **Валюта платежа:** предложения могут быть представлены в национальной валюте Республики Узбекистан, долларах США или ЕВРО

2. Правила и требования для участников

1. Участники, представляющие предложения, должны нести все расходы, связанные с подготовкой и подачей конкурсной документации. АКБ «ASIA ALLIANCE BANK» не несет никакой материальной ответственности за расходы, понесенные участником конкурсных торгов по подготовке и предоставлению конкурсного предложения.

2. В конкурсе могут принять участие как иностранные фирмы и организации, так и отечественные Исполнители (далее по тексту **«Участник конкурса»**), выполнившие условия, предъявляемые настоящим документом, имеющие необходимый опыт по оказанию подобных услуг.

3. К участию в конкурсе ***не допускаются*** фирмы и организации:

- находящиеся в стадии реорганизации, ликвидации и банкротства;
- не предоставившие в установленный срок необходимые документы для участия в конкурсе;
- не надлежаще исполнявшие принятые обязательства по ранее заключенным контрактам с Покупателем;
- учрежденные менее чем за 12 месяцев до объявления конкурса;
- не имеющие соответствующего статуса в регионе CEMEA - Qualified Security Assessor (QSA), сроком не менее 3-х лет, позволяющего проводить работы в регионе;
- находящиеся в состоянии судебного или арбитражного разбирательства;
- не отвечающие требованиям Конкурсной документации по коммерческим, финансовым и иным показателям.

4. Конкурсное предложение должно быть представлено в одном опечатанном конверте. Визирование уполномоченным представителем Участника конкурса, а также опечатывание конверта производится в местах склейки. Конверт должен быть опечатан штампом или печатью Участника (при наличии). В случае осуществления деятельности без печати и штампа, необходимо указать об этом на конверте следующей надписью: «деятельность организации осуществляется без печати/штампа». В конверте должны содержаться вместе с конкурсным предложением следующие материалы для проведения квалификационного отбора:

4.1. Копии документов о государственной регистрации претендента;

4.2. Общая информация о компании;

4.3. Срок действия статуса в регионе CEMEA - Qualified Security Assessor (QSA) не менее 3 лет должен быть подтвержден письмом от регулирующей организации или в виде договора с МПС;

4.4. Подтверждением статусов должно быть нахождение компании (и ее аудиторов) в актуальных списках сертифицированных аудиторов: Payment Card Industry Security Standards Council (ссылка: https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf) – необходимо предоставить копию списка;

4.5. Информация о не менее 10-ти завершенных работ по оценке соответствия требованиям стандарта PCI DSS за последние 2 (два) года (результаты приняты МПС и выданы сертификаты соответствия) и не менее 3-х завершенных проектов по оценке соответствия требованиям стандарта PCI DSS (результаты приняты МПС и выданы сертификаты соответствия), проведенного на территории Республики Узбекистан;

4.6. Среди членов команды должны быть представлены специалисты, обладающие подтверждёнными компетенциями в области информационной безопасности:

- наличие в штате сертифицированных специалистов, обладающих статусом Qualified Security Assessor (QSA) – не менее 5 (Копия сертификатов специалистов, резюме специалистов);

- наличие в штате сертифицированных специалистов, обладающих статусом Certified Information Systems Security Professional (CISSP) или Certified Information Systems Auditor (CISA) – не менее 1 (Копия сертификатов специалистов, резюме специалистов);

- наличие в штате специалистов, обладающих статусом BSI ISO/IEC 27001 Lead Auditor – не менее 1 (Копия сертификатов специалистов)

- наличие в штате специалистов, обладающих статусом ISO/IEC 27001 Lead Implementer – не менее 1 (Копия сертификатов специалистов)

- наличие в штате специалистов, обладающих статусом Certified Ethical Hacker (CEH) – не менее 1 (Копия сертификатов специалистов)

- наличие в штате специалистов, обладающих статусом PCI Secure SLC Assessor или PCI Secure Software Assessor – не менее 1 (Копия сертификатов специалистов)

4.9. На конверте указываются наименование и адрес Заказчика, контактные телефоны, а также:

- название (предмет) конкурса;
- наименование Участника конкурса, контактные данные, ИНН участника;
- пометка - «Не вскрывать до установленного времени проведения конкурса».

Конверты не опечатанные и не помеченные в соответствии с вышеуказанными требованиями не принимаются и не рассматриваются.

5. При необходимости Конкурсная комиссия может дополнительно потребовать от Участников конкурса предоставления дополнительной информации касательно представленных ими конкурсных предложений или других дополнительных документов, необходимых для выполнения данного заказа.

6. Никакие вставки между строками, подтирки или приписки в документах конкурсного предложения не допускаются, а при наличии их в документах, заявка не подлежит рассмотрению и отклоняется.

7. Участники конкурса должны представить конкурсное предложение строго в соответствии с формами, предлагаемыми в Конкурсной документации. В случае предоставления конкурсного предложения не по формам настоящей конкурсной документации, Конкурсная комиссия вправе отклонить данное предложение.

8. Предложения должны подаваться цельно и в количествах, указанных в конкурсной документации.

9. Полномочия представителя участника должны быть подтверждены доверенностью/приказом, которые должны быть представлены конкурсной комиссии. Доверенность должна быть оформлена по форме Приложения № 4.

10. Все документы, предоставляемые в рамках конкурсного предложения, должны быть выполнены на русском языке, подписаны уполномоченным представителем Участника конкурса, прошнурованы, пронумерованы и скреплены подписью представителя и/или печатью Участника конкурса. Участник конкурса несет ответственность за достоверность предоставляемой информации в рамках настоящего конкурса.

11. Конкурсное предложение должно быть действительно в течение не менее 3 (трех) месяцев со дня окончания приема конкурсных предложений.

12. Конкурсные предложения принимаются в Головном офисе банка по адресу: г.Ташкент, Яшнабадский район, ул. Махтумкули, дом №2А до срока, указанного в объявлении о проведении конкурса. Предложения, полученные после указанного срока, не рассматриваются и возвращаются участникам конкурса без вскрытия конвертов. Электронные предложения не принимаются. Финансирование данной закупки будет осуществлено за счет собственных средств АКБ «ASIA ALLIANCE BANK».

13. Перенос даты и времени окончания приема предложений на участие в конкурсе производится только решением Конкурсной комиссии.

14. Время вскрытия конкурсных предложений определяется Конкурсной комиссией после окончания срока приема конкурсных предложений.

15. Если наружный конверт с конкурсным предложением не опечатан должным образом, имеет нарушения печати или разрывы, то Конкурсная комиссия вправе не принимать их к рассмотрению.

16. Конкурсная комиссия вправе не рассматривать предложения, представленные не по форме, не полностью оформленными или не соответствующие оговоренным условиями.

17. Вскрытие конвертов с предложениями Участников конкурса производится на заседании конкурсной комиссии. Копии протокола вскрытия предложений Участникам конкурса не предоставляется.

18. Рассмотренные конкурсные предложения, а также другая документация, представленная для участия в конкурсе, возврату участникам не подлежат.

19. Оценка конкурсных предложений и определение победителя конкурса будет производиться на основании:

- анализа и сравнения предложений согласно раздела «3.Техническая часть»;
- соответствия предложенных цен среднемировым и сложившейся конъюнктуре рынка;
- иным параметрам, предусмотренным настоящей Конкурсной документацией.

20. Во внимание также могут приниматься дополнительные технические, организационные и коммерческие преимущества предоставленных конкурсных предложений, а также репутация Участника конкурса.

21. Срок рассмотрения конкурсных предложений определяется Конкурсной комиссией с момента вскрытия конвертов, но не может превышать более 15-ти дней.

22. Предложения могут быть представлены в национальной валюте Республики Узбекистан, долларах США или ЕВРО. При анализе предложений суммы будут учитываться в национальной валюте - сум по курсу Центрального банка Республики Узбекистан на день вскрытия конвертов.

23. При необходимости Конкурсная комиссия может дополнительно потребовать от Участников конкурса предоставления дополнительной информации касательно представленных ими конкурсных предложений или других дополнительных документов, необходимых для выполнения данного заказа.

24. Конкурсная комиссия гарантирует конфиденциальность предоставляемых предложений.

25. При любой попытке участника Конкурса оказать влияние на решение Конкурсной комиссии (при анализе предложений или при выборе предложения, наиболее приемлемого для заключения контракта) Конкурсная комиссия имеет право исключить его из числа участников конкурса.

26. В случае, если Победитель конкурса отказывается заключить контракт, то право на его заключение переходит к резервному участнику, имеющему наилучшие показатели после Победителя.

27. В случае если конкурс не состоялся или имел отрицательный результат, по решению Конкурсной комиссии возможно повторное проведение конкурса.

28. Конкурсная комиссия может отменить Конкурс в любое время, с письменным уведомлением Участников конкурса.

29. Победитель конкурса заключает контракт с Покупателем после принятия соответствующего решения Конкурсной комиссией и получения уведомления Рабочего органа о присуждении ему права заключения контракта.

30. Участник в представляемой заявке на участие должен указывать цену предложения с учетом НДС или без учета НДС.

31. Предложения должны подаваться цельно и в количествах, указанных в конкурсной документации.

3. Техническая часть

Общие сведения

1.1. Полное наименование предмета работ

Приведение АКБ «ASIA ALLIANCE BANK» в соответствие требованиям стандарта PCI DSS 3.2.1 (далее – Работы).

1.2. Границы проведения работ

Работы проводятся не более чем на 2-х площадках Заказчика, расположенных в г. Ташкент, Республика Узбекистан.

Внешний тест на проникновение выполняется Исполнителем не более 1-го (одного) раза.

Внутренний тест на проникновение выполняется Исполнителем не более 1-го (одного) раза.

Внешнее сканирование уязвимостей (ASV-сканирование) выполняется Исполнителем как минимум ежеквартально в течение 1 года с даты проведения первого из ASV-сканирования для не более чем 5 IP-адресов.

Расширение границ работ закрепляется дополнительным соглашением сторон к Договору, подписываемым Сторонами и скрепляемым печатями Сторон.

1.3. Состав работ

Для приведения Заказчика в соответствие требованиям Стандарта PCI DSS - Исполнитель обеспечивает выполнение следующих работ:

a) Предварительный аудит и консультирование на этапе приведения в соответствие, включая:
   - Предварительный аудит на площадке Заказчика;
   - Консультирование по выбору возможных средств защиты и способам снижения затрат;
   - Разработку детального плана приведения в соответствие;
   - Оказание годовой консультационной поддержки по вопросам выполнения требований Стандарта;
b) Разработку пакета необходимой нормативной документации;
c) Проведение внешних сканирований уязвимостей (ASV-сканирования);
d) Проведение внешнего тестирования на проникновение;
e) Проведение внутреннего тестирования на проникновение;
f) Тестирование механизмов сегментации
g) Проведение итогового сертификационного аудита.

2. Этапы проведения работ

2.1. Предварительный аудит по требованиям Стандарта PCI DSS 3.2.1

2.1.1. Предварительное определение области применения Стандарта

Целью данного этапа является определение области применения Стандарта PCI DSS 3.2.1 применительно к создаваемой и имеющейся ИТ-инфраструктуре АКБ «ASIA ALLIANCE BANK» а также согласование объема выполняемых работ при проведении первичной оценки процессингового центра Заказчика.

Для определения области применения Стандарта PCI DSS Заказчик предоставляет документацию о разрабатываемой (существующей) архитектуре АКБ «ASIA ALLIANCE BANK» перечне систем, участвующих в процессах обработки, хранения или передачи

данных платежных карт, а также существующих процессах обеспечения информационной безопасности.

Результатом данного этапа является перечень обследуемых физических, программных и информационных ресурсов, функциональных подсистем, включаемых в границы проведения работ.

2.1.2. Сбор организационной и технической информации о процессинговом центре

Целью данного этапа является получение актуальной и достоверной информации об архитектуре создаваемого процессингового центра, потоках данных платежных карт, текущем уровне обеспечения информационной безопасности, планов по развитию и модернизации процессинга, а также другой информации, необходимой для оценки соответствия требованиям Стандарта PCI DSS и разработки Плана мероприятий с рекомендациями по подготовке к успешному сертификационному аудиту.

При выполнении данных работ производится сбор следующих сведений:

- об организационной структуре;
- о структуре комплекса используемых программно-технических средств;
- о топологии сети и применяемых методах сегментации (в т.ч. характеристики используемых каналов и точек подключения к сетям связи и сети Интернет, беспроводные точки доступа);
- о процедурах обеспечения безопасности в локальной сети;
- о механизмах защиты данных платежных карт;
- о процедурах управления уязвимостями;
- о реализации системы управления доступом;
- о процедурах мониторинга и контроля доступа (на уровне сети и приложений);
- о политике информационной безопасности.

Сбор всех необходимых сведений производится путем изучения предоставленной Заказчиком документации, проведения интервью с персоналом Заказчика, анализа конфигурационных файлов программных и программно-технических системных компонентов, демонстрирования сотрудниками Заказчика выполняемых ими процедур.

Также, по желанию Заказчика, на данном этапе может быть проведено однократное внутреннее сканирование уязвимостей, с выдачей рекомендаций по устранению выявленных уязвимостей.

2.1.3. Оценка соответствия требованиям Стандарта PCI DSS

Целью данного этапа является определение текущего уровня соответствия платежного шлюза Заказчика требованиям Стандарта PCI DSS.

На данном этапе, на основе полученной ранее информации - выполняется анализ соответствия инфраструктуры Заказчика требованиям Стандарта PCI DSS, для чего проводятся следующие работы:

- анализ структуры сети и сегментации;
- анализ конфигураций активного сетевого оборудования и существующих правил разграничения доступа;
- анализ используемых сетевых протоколов с точки зрения безопасности;
- анализ принятых в информационной системе политик безопасности;
- анализ процессов обработки данных платежных карт;
- и другие необходимые работы.

Результатом работ на данном этапе является «Отчет об оценке соответствия создаваемой и существующей инфраструктуры Заказчика требованиям Стандарта PCI DSS». Данный отчет, включает в себя описание предлагаемой архитектуры платежного шлюза, перечень выявленных несоответствий требованиям Стандарта PCI DSS, описание

текущей области применимости требований Стандарта PCI DSS (текущей области аудита) и входящих в неё системных компонент.

2.1.4. Разработка рекомендаций по приведению в соответствие требованиям Стандарта PCI DSS

На данном этапе работ осуществляется разработка возможных вариантов реализации требований Стандарта PCI DSS, путем построения комплекса организационных мероприятий и реализации необходимых технических решений, также, на данном этапе разрабатываются возможные варианты уменьшения области аудита (области сертификации) для снижения суммарных затрат на подготовку к успешной сертификации, за счет уменьшения числа внедряемых средств защиты и объема проводимых работ.

При составлении рекомендаций по устранению выявленных несоответствий требованиям Стандарта PCI DSS учитываются следующие направления:

- уменьшение границ применимости требований Стандарта PCI DSS;
- изменение конфигураций существующих средств защиты;
- доработка существующей и разработка дополнительной документации в области обеспечения информационной безопасности;
- внедрение и настройку дополнительных средств защиты информации (как общедоступных, так и коммерческих решений);

Результатом работ на данном этапе является передаваемый Заказчику - План реализации организационных и технических мероприятий, выполнение которых позволит обеспечить выполнение всех требований Стандарта PCI DSS.

2.1.5. Обучение основам требований стандарта PCI DSS

В рамках данного этапа Исполнитель проводит разовое обучение специалистов Заказчика основам обеспечения соответствия стандарту PCI DSS.

Обучение по согласованию с Заказчиком может проводиться либо очно в г. Ташкент, в офисе Заказчика во время визита QSA-аудитора в рамках Этапа 1 либо в виде вэбинара.

Обучение проводится в течение не более чем 5 (пяти) часов.

Курсы проводятся по следующей программе:

1. Введение в стандарт PCI DSS
1.1. PCI SSC и обзор стандарта
1.2. Терминология платежной индустрии
1.3. Классификация торгово-сервисных предприятий и сервис-провайдеров
1.4. Жизненный цикл стандарта PCI DSS
1.5. Взаимоотношения участников в рамках стандарта.
2. Роли в стандарте PCI DSS и смежные сертификации
2.1. Роли платежных брендов
2.2. Программы безопасности данных от VISA и MasterCard
2.3. SAQ и ROC. В чем разница?
2.4. Обзор стандарта SSF
2.5. Обзор стандарта P2PE
2.6. Обзор стандарта PCI PIN Security Requirements
2.7. Роли и обязанности участников
3. Обнаружение данных платежных карт и область аудита
3.1. Как обнаружить данные платежных карт в своей инфраструктуре.
3.2. Сегментация сети. Как правильно выполнить.
3.3. Как определить область аудита.
4. Требования стандарта PCI DSS
5. Внедрение и поддержание соответствия PCI DSS
5.1. Особенности приведения в соответствие требованиям стандарта
5.2. Требования с периодическим контролем

5.3. Требования с постоянным контролем
5.4. Аутсорсинг требований PCI DSS. Как правильно организовать.
5.5. Как применять компенсирующие меры.
6. Вспомогательные документы PCI SSC и работа с Международными платежными системами (МПС)
6.1. Обзор вспомогательных документов от PCI SSC
6.2. Приоритетный подход в достижении соответствия PCI DSS.
6.3. ROC и AOC. Что делать с отчетными документами?
7. Подведение итогов

Программа курсов может быть скорректирована Исполнителем.

2.2. Разработка пакета нормативной документации

Целью данного этапа является разработка пакета проектов нормативной документации, необходимой для выполнения требований Стандарта PCI DSS, включая:

- Стандарты конфигурирования операционных систем и СУБД;
- Политики обеспечения безопасности данных платежных карт;
- Процедуры реагирования на инциденты информационной безопасности;
- Регламенты и инструкции;
- Другая необходимая документация.

Итоговый состав разрабатываемых документов определяется аудиторами Исполнителя по результатам этапа «Разработка рекомендаций по приведению в соответствие требованиям Стандарта PCI DSS».

Результатом работ на данном этапе является переданный Заказчику пакет проектов нормативной документации, необходимой для выполнения требований Стандарта PCI DSS.

2.3. Внешнее сканирование уязвимостей (ASV-сканирование)

В ходе выполнения работ Исполнитель, используя ASV-сертифицированное решение, осуществляет поиск уязвимостей и небезопасных конфигураций сетевых служб, функционирующих на общедоступных сетевых узлах Заказчика.

Внешнее сканирование уязвимостей (ASV-сканирование) выполняется Исполнителем ежеквартально, по запросу Заказчика, в течение 1 года с даты проведения первого из сканирований, для не более чем 5 IP-адресов.

При проведении работ в соответствии с требованиями Стандарта PCI DSS (процедурами сканирования) используются профили, не включающие в себя опасные проверки, такие как атаки на «отказ в обслуживании», «перебор паролей», а выявляемые в ходе проведения работ уязвимости классифицируются по степени критичности.

По желанию Заказчика, ему могут быть предоставлены права доступа к системе сканирования, для самостоятельного проведения неограниченного числа сканирований в течение 1 года с даты проведения первого из сканирований.

Результатом работ являются отчеты, передаваемые Заказчику по результатам проведения каждого из проведенных сканирований.

2.4. Тестирование на проникновение

Работы по моделированию действий потенциального злоумышленника разделяются на два типа:

- Внешнее тестирование на проникновение. Осуществляется из сети Интернет и представляет собой выявление и анализ технических уязвимостей ИС внешнего периметра корпоративной компьютерной сети Заказчика.

- Внутреннее тестирование на проникновение. Осуществляется с мобильной рабочей станции Исполнителя, включенной в ЛВС Заказчика, и представляет собой выявление и анализ технических уязвимостей внутренних ИС.

Состав и ход работ на каждом этапе тестирования на проникновение определяются внутренними методиками Исполнителя, поддерживаемыми в актуальном состоянии путем их регулярного пересмотра и анализа с учетом постоянно накапливаемого опыта проведения работ и текущих изменений в области информационной безопасности.

Также в ходе тестирования на проникновение Исполнителем используются общепринятые мировые практики проведения подобных работ, включая такие методики, как OSSTMM v3.0 и OWASP Testing Guide v3.

Работы на каждом из этапов предварительно согласуются с ответственными представителями Заказчика. В случае высокой вероятности нарушения функционирования целевых систем или в случае успешного доступа к конфиденциальной информации Заказчика Исполнитель прекращает дальнейшее выполнение работ до получения от Заказчика формального разрешения на продолжение работ.

В ходе работ Исполнитель не проводит распределенные атаки на отказ в обслуживании (DDoS).

По результатам работ Заказчику передаются отчетные документы, содержащие описание выполненных работ, выявленных проблем (уязвимостей) и рекомендации по их устранению.

2.4.1. Сведения о моделях злоумышленника

В рамках работ по тестированию на проникновение предлагается смоделировать действия потенциальных злоумышленников, соответствующих следующим моделям:

- «Интернет-хакер» – злоумышленник, действующий из сети Интернет, не имеющий логических прав в ИС Заказчика и не обладающий сведениями о корпоративной сети и ИС Заказчика;
- «Посетитель» – злоумышленник, имеющий возможность подключения неконтролируемой рабочей станции к ЛВС Заказчика (например, внешний консультант), не имеющий логических прав в ИС Заказчика и не обладающий подробными сведениями о структуре корпоративной сети и используемых средствах защиты;

Потенциальные злоумышленники, соответствующие каждой из описанных моделей, используют общедоступное специализированное ПО и не обладают навыками самостоятельного исследования уязвимостей ИС и их компонентов, а также не обладают квалификацией, достаточной для самостоятельной разработки вредоносного ПО.

Основными целями потенциальных злоумышленников являются:

- получение доступа в корпоративную сеть Заказчика;
- получение логического доступа в ИС Заказчика;
- получение доступа к конфиденциальной информации, обрабатываемой в ИС Заказчика;
- определение возможности нарушения работоспособности ЦОД Заказчика путем нарушения целостности обрабатываемых данных или нарушения доступности функционирующих сервисов.

2.4.2. Внешнее тестирование на проникновение

Работы по анализу защищенности внешнего периметра сети заключаются в моделировании действий потенциального внешнего злоумышленника, не обладающего подробными сведениями о корпоративной сети и процессинговом центре Заказчика.

Моделирование действий потенциального злоумышленника разделяется на два основных этапа:

1) Предварительный сбор информации. На данном этапе производится сбор сведений о структуре и компонентах корпоративной сети Заказчика, таких как: доменные имена и зоны, сетевая адресация, компоненты сети, используемые средства защиты.
2) Проведение активного внешнего тестирования на проникновение. Работы на данном этапе включают в себя выявление уязвимостей «ручным» методом и с использованием специализированного ПО. Состав работ на данном этапе включает в себя:
   - Определение типов и версий устройств, ОС, сетевых сервисов и приложений по реакции на внешнее воздействие;
   - Идентификация уязвимостей серверов, сетевого оборудования и сетевых средств защиты. Идентификация уязвимостей производится для всех хостов, входящих в границы работ и доступных (или ставших доступными в ходе работ) из сети Интернет (в том числе, сервисы HTTP и DNS, VPN-сервисы, web-приложения, сервис электронной почты, системные и прикладные сервисы). Производится выявление как уязвимостей, связанных с некорректной реализацией, так и уязвимостей, связанных с некорректной конфигурацией сетевых сервисов, ОС, приложений, сетевых устройств и средств защиты.

     Экспертный анализ защищенности (проникновение). Представляет собой моделирование атак, с использованием специализированных средств и сведений об известных уязвимостях, в отношении целевых систем. Работы на данном этапе при необходимости могут итеративно повторяться с целью воздействия на связанные информационные системы, вошедшие в границы работ.

2.4.3. Внутреннее тестирование на проникновение

Работы на данном этапе заключаются в моделировании действий потенциального внутреннего злоумышленника. В состав работ входит:

1) Сбор сведений о ЛВС Заказчика изнутри сети;
2) Определение типов и версий устройств, ОС, сетевых сервисов и приложений по реакции на внешнее воздействие;
3) Моделирование атак на сетевом уровне;
4) Идентификация уязвимостей рабочих станций пользователей, компонентов информационных систем, сетевого оборудования и сетевых средств защиты;
5) Моделирование атак на уровне приложений, сетевых сервисов и ОС, с использованием специализированных средств и сведений об известных уязвимостях в отношении выявленных систем.

2.5. Тестирование механизмов сегментации

Работы на данном этапе заключаются в проверки эффективности использованных мер сегментации сети (отделении границ сертификации от остальной сети). В состав работ входит:

1) Сбор сведений о ЛВС Заказчика изнутри сети;
2) Идентификация сетевых сервисов и приложений по реакции на внешнее воздействие из-за пределов границ сертификации;
3) Выборочная проверка правил межсетевого экранирования на границе среды сертификации.

Результатом работ на данном этапе является отчет по результатам дополнительного внутреннего тестирования сегментации, содержащий информацию о выполненных работах, включая информацию обо всех выявленных недостатках и рекомендации по их устранению.

2.6. Сертификационный аудит соответствия требованиям стандарта PCI DSS

2.6.1. Определение области сертификации

На данном этапе аудиторской группой Исполнителя производится определение и согласование актуальной области аудита. Для этого, Исполнителем запрашивается имеющаяся информация о структуре информационных систем процессингового центра и процессах обеспечения информационной безопасности, а также определяются системные компоненты, каналы передачи данных и другие системы, включаемые в область аудита в соответствии с требованиями Стандарта PCI DSS.

Результатом данного этапа является перечень системных компонент, подлежащих аудиту.

2.6.2. Сбор свидетельств соответствия

На данном этапе, аудиторы Исполнителя проводят необходимое интервьюирование ответственных сотрудников Заказчика, проверяют параметры безопасности системных компонент, входящих в область аудита и документируют свидетельства аудита необходимые для формирования итоговой отчетной документации.

Сбор всех необходимых сведений производится путем изучения нормативной документации, проведения интервью, анализа конфигурационных файлов, демонстрирования сотрудниками Заказчика выполняемых ими процедур по обеспечению информационной безопасности.

2.6.3. Формирование отчетной документации

На данном этапе аудиторская группа Исполнителя на основе собранных свидетельств аудита проводит анализ выполнения требований Стандарта PCI DSS, которые определены в шести группах:

a) Построение и поддержание защищенной вычислительной сети;
b) Защита информации держателей платежных карт;
c) Реализация программы управления уязвимостями;
d) Реализация мер по строгому контролю доступа;
e) Регулярный мониторинг и тестирование вычислительных сетей;
f) Поддержание политики информационной безопасности.

и формирует необходимую отчётную документацию.

Результатом работ на данном этапе являются отчетные документы, направляемые Заказчику и в Международные Платежные Системы:

- Report on Compliance (на английском языке);
- Attestation of Compliance (на английском языке);
- Сертификат соответствия PCI DSS (на русском и английском языках).

2.7. Консультационная поддержка по вопросам выполнения требований Стандарта PCI DSS

Целью работ на данном этапе является консультирование специалистов Заказчика по возникающим вопросам, связанным с разъяснением конкретных требований Стандарта PCI DSS и способам их выполнения.

Консультационная поддержка Заказчика осуществляется в течение 1 года с момента заключения договора. Прием запросов осуществляется по электронной почте и телефону. Время ответа на каждый поступивший запрос может составлять от 1 до 5 рабочих дней с даты приема запроса, в зависимости от сложности запроса.

Предельная стоимостью по выбору исполнителя на проведение работ по приведению в соответствие и сертификационному аудиту соответствия требованиям Стандарта PCI DSS в АКБ «ASIA ALLIANCE BANK» составляет 60 000 (шестьдесят тысяч) долларов США.

Объявление о проведении конкурса

АКБ «ASIA ALLIANCE BANK» объявляет конкурс и приглашает правомочные организации представить свои предложения по выбору исполнителя на проведение работ по приведению в соответствие и сертификационному аудиту соответствия требованиям стандарта PCI DSS в АКБ «ASIA ALLIANCE BANK»

№	Наименование товара/работы/услуги	Ориентировочная стоимость	Особые условия
1	Приведение АКБ «ASIA ALLIANCE BANK» в соответствие требованиям стандарта PCI DSS 3.2.1	60 000 (шестьдесят тысяч) долларов США	См. Приложение №1 к конкурсной документации п.7,8,9,10.

Заинтересованные претенденты должны подать соответствующим образом заполненную и подписанную Заявку на участие в конкурсе по адресу: г.Ташкент, Яшнабадский район, ул. Махтумкули, дом № 2А.

Конкурсные предложения, поступившие после указанного срока, не будут рассмотрены и будут отклонены. Электронные предложения не принимаются.

В конкурсных торгах могут принимать участие предприятия и организации независимо от форм собственности.

Финансирование данной закупки будет осуществлено за счет собственных средств АКБ «ASIA ALLIANCE BANK».

Имя и должность ответственного лица Заказчика и контакты:
Начальник Управления Юсупов Равшан Журабекович,
Главный специалист Филатов Владимир Олегович
Главный специалист Мирзаева Феруза Гаппарджановна
Адрес: г.Ташкент, Яшнабадский район, ул. Махтумкули, дом №2а.
Телефон: (+998 71) 231-60-00, факс: (+998 71) 289-55-33

4. Образцы форм

Приложение №1
к Конкурсной документации

ПЕРЕЧЕНЬ ДОКУМЕНТОВ, ПРЕДОСТАВЛЯЕМЫХ УЧАСТНИКАМИ КОНКУРСА.

Участник конкурса должен представить в запечатанном конверте следующие документы:

1. Заявка на участие в конкурсе по форме (Приложение № 2)
2. Документы, подтверждающие правоспособность (документы о регистрации, копия паспорта руководителя, выписки из торгового реестра)
3. Гарантийное письмо, свидетельствующее, о том, что участник не находится в стадии реорганизации, ликвидации или банкротства, в состоянии судебного или арбитражного разбирательства с Заказчиком по форме, не имеет задолженности по налогам и сборам № 2 по форме Приложения № 3.
4. Техническая часть, общие сведения.
5. Копии документов о государственной регистрации претендента;
6. Общую информацию о компании;
7. Срок действия статуса в регионе CEMEA - Qualified Security Assessor (QSA) не менее 3 лет должен быть подтвержден письмом от регулирующей организации или в виде договора с МПС;
8. Подтверждением статусов должно быть нахождение компании (и ее аудиторов) в актуальных списках сертифицированных аудиторов: Payment Card Industry Security Standards Council (ссылка: https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf) – необходимо предоставить копию списка;
9. Информация о не менее 10-ти завершенных работ по оценке соответствия требованиям стандарта PCI DSS за последние 2 (два) года (результаты приняты МПС и выданы сертификаты соответствия) и не менее 3-х завершенных проектов по оценке соответствия требованиям стандарта PCI DSS (результаты приняты МПС и выданы сертификаты соответствия), проведенного на территории Республики Узбекистан;
10. Среди членов команды должны быть представлены специалисты, обладающие подтверждёнными компетенциями в области информационной безопасности:

- наличие в штате сертифицированных специалистов, обладающих статусом Qualified Security Assessor (QSA) – не менее 5 (Копия сертификатов специалистов, резюме специалистов);
- наличие в штате сертифицированных специалистов, обладающих статусом Certified Information Systems Security Professional (CISSP) или Certified Information Systems Auditor (CISA) – не менее 1 (Копия сертификатов специалистов, резюме специалистов);
- наличие в штате специалистов, обладающих статусом BSI ISO/IEC 27001 Lead Auditor – не менее 1 (Копия сертификатов специалистов)
- наличие в штате специалистов, обладающих статусом ISO/IEC 27001 Lead Implementer – не менее 1 (Копия сертификатов специалистов)
- наличие в штате специалистов, обладающих статусом Certified Ethical Hacker (CEH) – не менее 1 (Копия сертификатов специалистов)
- наличие в штате специалистов, обладающих статусом PCI Secure SLC Assessor или PCI Secure Software Assessor – не менее 1 (Копия сертификатов специалистов)

Приложение № 2
ФОРМА КОНКУРСНОГО ПРЕДЛОЖЕНИЯ

НА ФИРМЕННОМ БЛАНКЕ УЧАСТНИКА

Председателю Конкурсной комиссии
АКБ «ASIA ALLIANCE BANK»
Норкулову О.О.

_____ имеет возможность предоставить услугу на Проведение работ по приведению в соответствие и сертификационному аудиту соответствия требованиям Стандарта PCI DSS в АКБ «ASIA ALLIANCE BANK»:

№	Наименование этапа	Кол-во дней	Стоимость
1			

Изучив данные объявления об условиях конкурса, мы, нижеподписавшиеся, уполномоченные на подписание заявки, (полное наименование Участника конкурса), намерены участвовать в конкурсных торгах (указать предмет конкурса) в соответствии с конкурсной документацией.

Мы обязуемся выполнить работы/оказать услуги/поставить товар в точном соответствии с условиями, предусмотренными договором и действующим законодательством Республики Узбекистан.

В случае если наши предложения будут приняты банком, берем на себя обязательство заключить договор с АКБ «ASIA ALLIANCE BANK» в срок не позднее 5 дней с момента направления в наш адрес извещения о принятии наших предложений.

Руководитель Участника конкурса _____

Дата _____ Место печати

Приложение № 3
к Конкурсной документации

НА ФИРМЕННОМ БЛАНКЕ УЧАСТНИКА

Кому: Конкурсной комиссии

_____

(указать предмет конкурса)

Дата: _____

ГАРАНТИЙНОЕ ПИСЬМО

Настоящим письмом подтверждаем, что компания

_____

(наименование компании)

- не находится в стадии реорганизации (разделения, слияния), ликвидации или банкротства, имущество компании не арестовано;
- не находится в состоянии судебного или арбитражного разбирательства;
- не имеет задолженности по налогам и сборам.

Подписи:

Ф.И.О. руководителя _____

Ф.И.О. главного бухгалтера _____

Ф.И.О. юриста _____

Место печати

Приложение № 4
к Конкурсной документации

НА ФИРМЕННОМ БЛАНКЕ ОРГАНИЗАЦИИ

ДОВЕРЕННОСТЬ №_____

г. _____ _____20__г.

ООО_____,
именуемое в дальнейшем «Организация», в лице _____,
действующего на основании _____, настоящей доверенностью уполномочивает представителя Организации – гражданина _____(паспорт серии__№____, выданный _____ от _____ года) на:

а) представление конкурсных документов;
б) проведение переговоров с заказчиком конкурса и рабочим органом;
в) присутствие на заседаниях конкурсной комиссии при вскрытии конвертов с конкурсным предложением;
г) предоставление разъяснений, касательно технической и ценовой части конкурсного предложения, а также других вопросов.

Настоящая доверенность вступает в силу с момента её подписания, выдана без права передоверия, сроком до _____г.

Ф.И.О. и подпись руководителя

Ф.И.О. и подпись лица, на имя которого выдана доверенность

Место печати (при наличии)

Приложение № 5
к Конкурсной документации

ПРОЕКТ ДОГОВОРА

Настоящий проект Договора является предварительным, его условия могут подлежать изменению по согласованию сторон в частях, не противоречащих действующему законодательству Республики Узбекистан.

Договор № _____

г. Ташкент «___»_____202__

_____ именуемое в дальнейшем «Исполнитель», в лице_____, действующего на основании _____, с одной стороны, и АКБ «ASIA ALLIANCE BANK», именуемый в дальнейшем «Заказчик», в лице И.о. Председателя Правления Хакимова У.А., действующего на основании Устава, с другой стороны, а вместе именуемые Стороны, заключили настоящий Договор о нижеследующем:

I. Предмет Договора

1. Заказчик поручает, а Исполнитель обязуется оказать услуги для АКБ «ASIA ALLIANCE BANK» (Далее – Заказчик) по сертификационному аудиту соответствия требованиям стандарта PCI DSS 3.2.1 (далее – Услуги) согласно Заданию на Услуги, приведенному в Приложении №1 к настоящему Договору, и Календарному плану-графику, приведенному в Приложении №2 к настоящему Договору.

2. Подготовленные Исполнителем отчётные документы передаются Заказчику в электронной форме посредством электронной почты на следующий адрес: Info@aab.uz, в виде, допускающем редактирование (Microsoft Office), для предварительного согласования. Данные материалы могут быть возвращены на доработку на основании мотивированных возражений (замечаний) Заказчика. Доработка отчетных материалов выполняется без изменения цены Услуг по настоящему Договору.

3. Все подлежащие выполнению по настоящему Договору Услуги осуществляются Исполнителем своими силами.

II. Сроки оказания Услуг

1. Исполнитель приступает к оказанию Услуг после подписания Сторонами настоящего Договора. Исполнитель обязуется оказать Услуги в сроки, указанные в Календарном плане-графике (Приложение №2 к настоящему Договору).

2. По взаимной письменной договоренности Сторон сроки оказания Услуг могут быть увеличены без изменения общей стоимости Услуг.

III. Цена Услуг, порядок расчетов и порядок сдачи-приемки Услуг по Договору

1. Оплата по настоящему Договору производится в _____ на основании счетов, выставленных Исполнителем.

2. Общая стоимость всех оказываемых Услуг по настоящему Договору составляет _____ (_____) с учётом НДС (или без учета НДС)

3. Заказчик оплачивает оказание Услуг следующим образом:

3.1. Предоплата в размере 50 % или _____ (_____) с учётом НДС (или без учета НДС) в течение 10 (Десяти) рабочих дней с момента получения счета Исполнителя, выставляемого после подписания настоящего Договора.

3.2 Второй платеж в размере 50 % или _____ (_____) с учётом НДС (или без учета НДС) в течение 10 (Десяти) рабочих дней с момента получения счета Исполнителя, выставляемого после подписания Сторонами акта сдачи-приемки услуг.

4. Оплата оказанных Услуг производится Заказчиком в безналичном порядке на расчетный счет Исполнителя, указанный в статье X настоящего Договора.

5. Днем оплаты считается день зачисления денежных средств на корреспондентский счет банка обслуживающего расчетный счет Исполнителя. Задержка Заказчиком оплаты Услуг Исполнителя по Договору, вызванная задержкой выставления счета на оплату или Акта сдачи-приемки Исполнителем, не является нарушением финансовых обязательств Заказчика по настоящему Договору.

6. Исполнитель в течение 3 (Трех) рабочих дней после окончания Услуг осуществляет их сдачу-приемку, и представляет Заказчику 2 (Два) экземпляра Акта сдачи-приёмки.

7. Заказчик обязан в течение 5 (Пяти) рабочих дней со дня получения отчетных документов и Акта сдачи-приёмки согласовать отчетные документы и направить Исполнителю подписанный Акт сдачи-приёмки или направить мотивированный отказ от приёмки Услуг, с указанием недостатков и сроков доработки. Акт в этом случае подписывается после устранения замечаний.

8. В случае если Заказчик по истечении 5 (Пяти) рабочих дней не согласовывает отчетные документы, не подписывает Акт сдачи-приёмки и не предъявляет Исполнителю в письменном виде мотивированный отказ от приёмки Услуг, отчетные документы считаются согласованными и Услуги считаются принятыми Заказчиком, а Исполнитель составляет односторонний Акт сдачи-приёмки, о чем Исполнитель уведомляет Заказчика в письменной форме в течение 1 (Одного) рабочего дня с момента составления такого Акта сдачи-приёмки.

IV. Обязанности Сторон

1. Исполнитель обязуется:
   1.1. Оказать Услуги в соответствии с условиями настоящего Договора и Приложения № 1 к настоящему Договору, передать Заказчику их результаты в согласованные Сторонами сроки (Приложение №2 к настоящему Договору). Оказывать Услуги своевременно и с надлежащим качеством.
   1.2. Нести ответственность за результаты выполненных по настоящему Договору Услуг и гарантировать, что все результаты оказанных Услуг полностью соответствуют Приложению №1, на момент подписания Акта сдачи-приемки оказанных Услуг.
2. Заказчик обязуется:

2.1. Принимать результаты надлежаще оказанных Услуг в соответствии с п.7 ст.III настоящего Договора.
2.2. Оплачивать надлежаще оказанные и принятые Услуги в соответствии с п.3 и п.4 ст.III настоящего Договора.
2.3. Предоставить в согласованное Сторонами время доступ специалистам Исполнителя в офис Заказчика для выполнения обязательств Исполнителя по настоящему Договору.
2.4. Предоставить специалистам Исполнителя имеющуюся информацию о перечне и составе информационных систем входящих в границы оказания услуг, необходимую для выполнения обязательств Исполнителя по настоящему Договору.
2.5. Предоставить доступ специалистам Исполнителя к системотехническим ресурсам и содействие местного персонала для выполнения обязательств Исполнителя по настоящему Договору.

V. Конфиденциальность

1. Стороны обязуются в соответствие с Соглашением о конфиденциальности сохранять в тайне и не разглашать третьим лицам конфиденциальную информацию, ставшую им известной в результате заключения и исполнения настоящего Договора.

2. Не признается конфиденциальной информация, которая была получена Стороной до подписания настоящего Договора, информация, полученная законными методами из других источников, а также информация, которая не может относиться к конфиденциальной в соответствии с действующим законодательством Республики Узбекистан

3. Передача конфиденциальной информации осуществляется в соответствии с Порядком передачи конфиденциальной информации определенном в Соглашении о конфиденциальности (Приложение №3 к настоящему Договору).

VI. Ответственность Сторон и расторжение Договора

1. За невыполнение или ненадлежащее выполнение своих обязательств по настоящему Договору Стороны несут ответственность в соответствии с действующим законодательством РУз.

2. При нарушении Исполнителем сроков по каждому из этапов оказания Услуг, указанных в Приложении № 2 настоящего Договора, Заказчик вправе предъявить требование к Исполнителю об уплате пени в размере 0,1% (Ноль целых одна десятая процента) от общей стоимости Услуг, указанных в п.2. ст.III настоящего Договора за каждый день просрочки, но не более 10% (Десяти процентов) от общей стоимости Услуг по настоящему Договору.

3. При нарушении Заказчиком сроков платежей, указанных п.3 ст.III настоящего Договора, Исполнитель вправе предъявить требование к Заказчику об уплате пени в размере 0,1% (Ноль целых одна десятая процента) от суммы, подлежащей оплате за каждый день просрочки, но не более 10% (Десяти процентов) от неоплачиваемой суммы. Исполнитель может расторгнуть настоящий Договор в случае задержки срока оплаты свыше 30 (Тридцати) календарных дней с момента истечения срока, указанного в п.3 ст.III настоящего Договора.

4. Любая из Сторон может расторгнуть Договор, в одностороннем порядке, если другая Сторона:

а) не выполняет любое обязательство по настоящему Договору и такое неисполнение не устраняется в течение 30 (Тридцать) календарных дней после получения письменного уведомления о возникновении такового;

б) осуществляет процедуру банкротства, подвергается ликвидации или в ее отношении назначается управляющий имуществом и такое назначение не аннулируется в течение 30 (Тридцать) календарных дней после его осуществления.

5. В случае расторжения настоящего Договора по основаниям, предусмотренным условиями настоящего Договора Стороны обязуются уведомить друг друга о расторжении Договора как минимум за 7 (Семь) рабочих дней до даты расторжения настоящего Договора. В случае расторжения настоящего Договора Стороны производят взаиморасчеты в течение 14 (Четырнадцать) рабочих дней от даты расторжения.

VII. Обстоятельства непреодолимой силы (форс-мажор)

1. При наступлении обстоятельств невозможности полного или частичного исполнения любой из Сторон обязательств по настоящему Договору, а именно: пожара, стихийного бедствия, метеорологических или иных условий, запрещающих полеты, войны, военных операций любого характера, блокады, запрещений экспорта или импорта, или других, не зависящих от Сторон обстоятельств, срок исполнения обязательства отодвигается соразмерно времени, в течение которого будут действовать такие обстоятельства.

2. Если оговоренные обстоятельства будут продолжаться более 3 (Трех) месяцев от даты их начала, то каждая из Сторон будет иметь право отказаться от дальнейшего исполнения обязательств по настоящему Договору. В этом случае Стороны производят взаиморасчеты.

3. Сторона, для которой создалась невозможность выполнения обязательств по настоящему Договору, должна немедленно извещать другую Сторону о наступлении и прекращении обстоятельств, препятствующих исполнению обязательств.

4. Обстоятельства, освобождающие Стороны от ответственности за полное или частичное неисполнение настоящего Договора, должны быть удостоверены компетентным органом Республики Узбекистан.

5. В случае невозможности оказания услуг на площадке Заказчика, в связи с различными объективными причинами, например эпидемии, карантина и других, а также при соответствующем допуске со стороны платежных системы – осуществляет проведение аудита в удаленном режиме, посредством теле/видеоконференций, а Заказчик предоставляет необходимые свидетельства аудита по запросам Исполнителя.

VIII. Арбитраж

1. Стороны примут все меры к разрешению всех споров и разногласий, которые могут возникнуть из настоящего Договора или в связи с ним, дружественным и справедливым путем.

2. В случае если Стороны не придут к окончательному соглашению, все споры и разногласия могут быть разрешены в Ташкентском межрайонном экономическом суде, с

соблюдением претензионного порядка на основании действующего законодательства Республики Узбекистан.

IX. Прочие условия

1. После подписания настоящего Договора все предшествующие переговоры и переписка по нему теряют силу.

2. Все Приложения, Изменения, Дополнительные Соглашения к настоящему Договору являются его неотъемлемой частью и считаются действительными только в том случае, если они выполнены в письменной форме и подписаны лицами, уполномоченными на то договаривающимися Сторонами.

3. Все сообщения, заявления, извещения и претензии, связанные с исполнением настоящего Договора или вытекающие из него, должны посылаться Сторонами непосредственно друг другу по указанным в настоящем Договоре адресам.

4. Всю переписку по исполнению настоящего Договора или в связи с ним Стороны будут вести на русском языке.

5. Ни одна из Сторон настоящего Договора не имеет права передавать свои права и обязательства по настоящему Договору или в связи с ним третьим лицам без письменного на то согласия другой Стороны.

6. Настоящий Договор в 2 (Двух) экземплярах на русском языке, по одному для каждой Стороны, причем оба имеют одинаковую юридическую силу.

7. Настоящий Договор вступает в силу с момента его заключения и действует до исполнения Сторонами своих обязательств.

X. Адреса и банковские реквизиты Сторон

«ИСПОЛНИТЕЛЬ»	«ЗАКАЗЧИК»
_____	_____
_____	_____
Тел: _____	Тел: _____
Р/с _____	Р/с _____
_____	_____
МФО _____ ИНН _____	МФО _____ ИНН _____
ОКЭД	ОКЭД
_____	_____
_____	_____
М.П	М.П

Приложение № 1
к Договору № _____
от «___»_____202_ года

ЗАДАНИЕ НА УСЛУГИ

ОКАЗАНИЕ УСЛУГ ПО СЕРТИФИКАЦИОННОМУ
АУДИТУ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ СТАНДАРТА
PAYMENT CARD INDUSTRY DATA SECURITY STANDARD 3.2.1
ДЛЯ АКБ «ASIA ALLIANCE BANK»

3. Общие сведения

3.1. Полное наименование предмета оказания услуг

Оказание услуг по сертификационному аудиту соответствия «Наименование Заказчика» требованиям стандарта Payment Card Industry Data Security Standard 3.2.1 (далее – Услуги).

3.2. Перечень документов, на основании которых оказываются услуги

Все услуги выполняются в полном соответствии со следующей нормативной документацией:

- PCI DSS Requirements and Security Assessment Procedures v3.2.1;
- Navigating PCI DSS. Understanding the Intent of the Requirements Version 2.0;
- PCI DSS Validation Requirements for Qualified Security Assessors (QSAs);
- PCI DSS Validation Requirements for Approved Scanning Vendors (ASVs);
- Technical & Operational Requirements for ASVs;
- Information Supplements. Requirement 6.6 Application Reviews and Web Application Firewalls Clarified;
- Prioritized Approach for PCI DSS Version 3.0;
- Overview of the PCI DSS Wireless Guideline;
- PCI DSS Virtualization Guidelines v2.0.
- а также дополнительными инструкциями, получаемыми от VISA.

3.3. Границы оказания услуг

Работы проводятся не более чем на 2-х площадках Заказчика, расположенных в г. Ташкент, Республика Узбекистан.

Внешний тест на проникновение выполняется Исполнителем не более 1-го (одного) раза.

Внутренний тест на проникновение выполняется Исполнителем не более 1-го (одного) раза.

Внешнее сканирование уязвимостей (ASV-сканирование) выполняется Исполнителем как минимум ежеквартально в течение 1 года с даты проведения первого из ASV-сканирования для не более чем 5 IP-адресов.

Расширение границ работ закрепляется дополнительным соглашением сторон к Договору, подписываемым Сторонами и скрепляемым печатями Сторон.

3.4. Решаемые задачи

Для приведения Заказчика в соответствие требованиям Стандарта PCI DSS - Исполнитель обеспечивает выполнение следующих работ:

g) Предварительный аудит и консультирование на этапе приведения в соответствие, включая:
   - Предварительный аудит на площадке Заказчика;
   - Консультирование по выбору возможных средств защиты и способам снижения затрат;
   - Разработку детального плана приведения в соответствие;

- Оказание годовой консультационной поддержки по вопросам выполнения требований Стандарта;

h) Разработку пакета необходимой нормативной документации;
i) Проведение внешних сканирований уязвимостей (ASV-сканирования);
j) Проведение внешнего тестирования на проникновение;
k) Проведение внутреннего тестирования на проникновение;
l) Тестирование механизмов сегментации
m) Проведение итогового сертификационного аудита.

Этапы оказания услуг

3.5. Предварительный аудит по требованиям Стандарта PCI DSS 3.2.1

3.5.1. Предварительное определение области применения Стандарта

Целью данного этапа является определение области применения Стандарта PCI DSS 3.2.1 применительно к создаваемой и имеющейся ИТ-инфраструктуре АКБ «ASIA ALLIANCE BANK», а также согласование объема выполняемых работ при проведении первичной оценки процессингового центра Заказчика.

Для определения области применения Стандарта PCI DSS Заказчик предоставляет документацию о разрабатываемой (существующей) архитектуре АКБ «ASIA ALLIANCE BANK», перечне систем участвующих в процессах обработки, хранения или передачи данных платежных карт, а также существующих процессах обеспечения информационной безопасности.

Результатом данного этапа является перечень обследуемых физических, программных и информационных ресурсов, функциональных подсистем, включаемых в границы проведения работ.

3.5.2. Сбор организационной и технической информации о процессинговом центре

Целью данного этапа является получение актуальной и достоверной информации об архитектуре создаваемого процессингового центра, потоках данных платежных карт, текущем уровне обеспечения информационной безопасности, планов по развитию и модернизации процессинга, а также другой информации, необходимой для оценки соответствия требованиям Стандарта PCI DSS и разработки Плана мероприятий с рекомендациями по подготовке к успешному сертификационному аудиту.

При выполнении данных работ производится сбор следующих сведений:

- об организационной структуре;
- о структуре комплекса используемых программно-технических средств;
- о топологии сети и применяемых методах сегментации (в т.ч. характеристики используемых каналов и точек подключения к сетям связи и сети Интернет, беспроводные точки доступа);
- о процедурах обеспечения безопасности в локальной сети;
- о механизмах защиты данных платежных карт;
- о процедурах управления уязвимостями;
- о реализации системы управления доступом;

- о процедурах мониторинга и контроля доступа (на уровне сети и приложений);
- о политике информационной безопасности.

Сбор всех необходимых сведений производится путем изучения предоставленной Заказчиком документации, проведения интервью с персоналом Заказчика, анализа конфигурационных файлов программных и программно-технических системных компонентов, демонстрирования сотрудниками Заказчика выполняемых ими процедур.

Также, по желанию Заказчика, на данном этапе может быть проведено однократное внутреннее сканирование уязвимостей, с выдачей рекомендаций по устранению выявленных уязвимостей.

3.5.3. Оценка соответствия требованиям Стандарта PCI DSS

Целью данного этапа является определение текущего уровня соответствия платежного шлюза Заказчика требованиям Стандарта PCI DSS.

На данном этапе, на основе полученной ранее информации - выполняется анализ соответствия инфраструктуры Заказчика требованиям Стандарта PCI DSS, для чего проводятся следующие работы:

- анализ структуры сети и сегментации;
- анализ конфигураций активного сетевого оборудования и существующих правил разграничения доступа;
- анализ используемых сетевых протоколов с точки зрения безопасности;
- анализ принятых в информационной системе политик безопасности;
- анализ процессов обработки данных платежных карт;
- и другие необходимые работы.

Результатом работ на данном этапе является «Отчет об оценке соответствия создаваемой и существующей инфраструктуры Заказчика требованиям Стандарта PCI DSS». Данный отчет, включает в себя описание предлагаемой архитектуры платежного шлюза, перечень выявленных несоответствий требованиям Стандарта PCI DSS, описание текущей области применимости требований Стандарта PCI DSS (текущей области аудита) и входящих в неё системных компонент.

3.5.4. Разработка рекомендаций по приведению в соответствие требованиям Стандарта PCI DSS

На данном этапе работ осуществляется разработка возможных вариантов реализации требований Стандарта PCI DSS, путем построения комплекса организационных мероприятий и реализации необходимых технических решений, также, на данном этапе разрабатываются возможные варианты уменьшения области аудита (области сертификации) для снижения суммарных затрат на подготовку к успешной сертификации, за счет уменьшения числа внедряемых средств защиты и объема проводимых работ.

При составлении рекомендаций по устранению выявленных несоответствий требованиям Стандарта PCI DSS учитываются следующие направления:

- уменьшение границ применимости требований Стандарта PCI DSS;
- изменение конфигураций существующих средств защиты;
- доработка существующей и разработка дополнительной документации в области обеспечения информационной безопасности;

- внедрение и настройку дополнительных средств защиты информации (как общедоступных, так и коммерческих решений);

Результатом работ на данном этапе является передаваемый Заказчику - План реализации организационных и технических мероприятий, выполнение которых позволит обеспечить выполнение всех требований Стандарта PCI DSS.

3.5.5. Обучение основам требований стандарта PCI DSS

В рамках данного этапа Исполнитель проводит разовое обучение специалистов Заказчика основам обеспечения соответствия стандарту PCI DSS.

Обучение по согласованию с Заказчиком может проводиться либо очно в г. Ташкент, в офисе Заказчика во время визита QSA-аудитора в рамках Этапа 1 либо в виде вэбинара.

Обучение проводится в течение не более чем 5 (пяти) часов.

Курсы проводятся по следующей программе:

1. Введение в стандарт PCI DSS
1.1. PCI SSC и обзор стандарта
1.2. Терминология платежной индустрии
1.3. Классификация торгово-сервисных предприятий и сервис-провайдеров
1.4. Жизненный цикл стандарта PCI DSS
1.5. Взаимоотношения участников в рамках стандарта.
2. Роли в стандарте PCI DSS и смежные сертификации
2.1. Роли платежных брендов
2.2. Программы безопасности данных от VISA и MasterCard
2.3. SAQ и ROC. В чем разница?
2.4. Обзор стандарта SSF
2.5. Обзор стандарта P2PE
2.6. Обзор стандарта PCI PIN Security Requirements
2.7. Роли и обязанности участников
3. Обнаружение данных платежных карт и область аудита
3.1. Как обнаружить данные платежных карт в своей инфраструктуре.
3.2. Сегментация сети. Как правильно выполнить.
3.3. Как определить область аудита.
4. Требования стандарта PCI DSS
5. Внедрение и поддержание соответствия PCI DSS
5.1. Особенности приведения в соответствие требованиям стандарта
5.2. Требования с периодическим контролем
5.3. Требования с постоянным контролем
5.4. Аутсорсинг требований PCI DSS. Как правильно организовать.
5.5. Как применять компенсирующие меры.
6. Вспомогательные документы PCI SSC и работа с Международными платежными системами (МПС)
6.1. Обзор вспомогательных документов от PCI SSC
6.2. Приоритетный подход в достижении соответствия PCI DSS.
6.3. ROC и AOC. Что делать с отчетными документами?
7. Подведение итогов

Программа курсов может быть скорректирована Исполнителем.

3.6. Разработка пакета нормативной документации

Целью данного этапа является разработка пакета проектов нормативной документации, необходимой для выполнения требований Стандарта PCI DSS, включая:

- Стандарты конфигурирования операционных систем и СУБД;
- Политики обеспечения безопасности данных платежных карт;
- Процедуры реагирования на инциденты информационной безопасности;
- Регламенты и инструкции;
- Другая необходимая документация.

Итоговый состав разрабатываемых документов определяется аудиторами Исполнителя по результатам этапа «Разработка рекомендаций по приведению в соответствие требованиям Стандарта PCI DSS».

Результатом работ на данном этапе является переданный Заказчику пакет проектов нормативной документации, необходимой для выполнения требований Стандарта PCI DSS.

3.7. Внешнее сканирование уязвимостей (ASV-сканирование)

В ходе выполнения работ Исполнитель, используя ASV-сертифицированное решение, осуществляет поиск уязвимостей и небезопасных конфигураций сетевых служб, функционирующих на общедоступных сетевых узлах Заказчика.

Внешнее сканирование уязвимостей (ASV-сканирование) выполняется Исполнителем ежеквартально, по запросу Заказчика, в течение 1 года с даты проведения первого из сканирований, для не более чем 20 IP-адресов.

При проведении работ в соответствии с требованиями Стандарта PCI DSS (процедурами сканирования) используются профили, не включающие в себя опасные проверки, такие как атаки на «отказ в обслуживании», «перебор паролей», а выявляемые в ходе проведения работ уязвимости классифицируются по степени критичности.

По желанию Заказчика, ему могут быть предоставлены права доступа к системе сканирования, для самостоятельного проведения неограниченного числа сканирований в течение 1 года с даты проведения первого из сканирований.

Результатом работ являются отчеты, передаваемые Заказчику по результатам проведения каждого из проведенных сканирований.

3.8. Тестирование на проникновение

Работы по моделированию действий потенциального злоумышленника разделяются на два типа:

- Внешнее тестирование на проникновение. Осуществляется из сети Интернет и представляет собой выявление и анализ технических уязвимостей ИС внешнего периметра корпоративной компьютерной сети Заказчика.
- Внутреннее тестирование на проникновение. Осуществляется с мобильной рабочей станции Исполнителя, включенной в ЛВС Заказчика, и представляет собой выявление и анализ технических уязвимостей внутренних ИС.

Состав и ход работ на каждом этапе тестирования на проникновение определяются внутренними методиками Исполнителя, поддерживаемыми в актуальном состоянии путем их регулярного пересмотра и анализа с учетом постоянно

накапливаемого опыта проведения работ и текущих изменений в области информационной безопасности.

Также в ходе тестирования на проникновение Исполнителем используются общепринятые мировые практики проведения подобных работ, включая такие методики, как OSSTMM v3.0 и OWASP Testing Guide v3.

Работы на каждом из этапов предварительно согласуются с ответственными представителями Заказчика. В случае высокой вероятности нарушения функционирования целевых систем или в случае успешного доступа к конфиденциальной информации Заказчика Исполнитель прекращает дальнейшее выполнение работ до получения от Заказчика формального разрешения на продолжение работ.

В ходе работ Исполнитель не проводит распределенные атаки на отказ в обслуживании (DDoS).

По результатам работ Заказчику передаются отчетные документы, содержащие описание выполненных работ, выявленных проблем (уязвимостей) и рекомендации по их устранению.

3.8.1. Сведения о моделях злоумышленника

В рамках работ по тестированию на проникновение предлагается смоделировать действия потенциальных злоумышленников, соответствующих следующим моделям:

- «Интернет-хакер» – злоумышленник, действующий из сети Интернет, не имеющий логических прав в ИС Заказчика и не обладающий сведениями о корпоративной сети и ИС Заказчика;
- «Посетитель» – злоумышленник, имеющий возможность подключения неконтролируемой рабочей станции к ЛВС Заказчика (например, внешний консультант), не имеющий логических прав в ИС Заказчика и не обладающий подробными сведениями о структуре корпоративной сети и используемых средствах защиты;

Потенциальные злоумышленники, соответствующие каждой из описанных моделей, используют общедоступное специализированное ПО и не обладают навыками самостоятельного исследования уязвимостей ИС и их компонентов, а также не обладают квалификацией, достаточной для самостоятельной разработки вредоносного ПО.

Основными целями потенциальных злоумышленников являются:

- получение доступа в корпоративную сеть Заказчика;
- получение логического доступа в ИС Заказчика;
- получение доступа к конфиденциальной информации, обрабатываемой в ИС Заказчика;
- определение возможности нарушения работоспособности ЦОД Заказчика путем нарушения целостности обрабатываемых данных или нарушения доступности функционирующих сервисов.

3.8.2. Внешнее тестирование на проникновение

Работы по анализу защищенности внешнего периметра сети заключаются в моделировании действий потенциального внешнего злоумышленника, не обладающего подробными сведениями о корпоративной сети и процессинговом центре Заказчика.

Моделирование действий потенциального злоумышленника разделяется на два основных этапа:

4) Предварительный сбор информации. На данном этапе производится сбор сведений о структуре и компонентах корпоративной сети Заказчика, таких как: доменные имена и зоны, сетевая адресация, компоненты сети, используемые средства защиты.
5) Проведение активного внешнего тестирования на проникновение. Работы на данном этапе включают в себя выявление уязвимостей «ручным» методом и с использованием специализированного ПО. Состав работ на данном этапе включает в себя:
   - Определение типов и версий устройств, ОС, сетевых сервисов и приложений по реакции на внешнее воздействие;
   - Идентификация уязвимостей серверов, сетевого оборудования и сетевых средств защиты. Идентификация уязвимостей производится для всех хостов, входящих в границы работ и доступных (или ставших доступными в ходе работ) из сети Интернет (в том числе, сервисы HTTP и DNS, VPN-сервисы, web-приложения, сервис электронной почты, системные и прикладные сервисы). Производится выявление как уязвимостей, связанных с некорректной реализацией, так и уязвимостей, связанных с некорректной конфигурацией сетевых сервисов, ОС, приложений, сетевых устройств и средств защиты.
   - Экспертный анализ защищенности (проникновение). Представляет собой моделирование атак, с использованием специализированных средств и сведений об известных уязвимостях, в отношении целевых систем. Работы на данном этапе при необходимости могут итеративно повторяться с целью воздействия на связанные информационные системы, вошедшие в границы работ.

3.8.3. Внутреннее тестирование на проникновение

Работы на данном этапе заключаются в моделировании действий потенциального внутреннего злоумышленника. В состав работ входит:

6) Сбор сведений о ЛВС Заказчика изнутри сети;
7) Определение типов и версий устройств, ОС, сетевых сервисов и приложений по реакции на внешнее воздействие;
8) Моделирование атак на сетевом уровне;
9) Идентификация уязвимостей рабочих станций пользователей, компонентов информационных систем, сетевого оборудования и сетевых средств защиты;
10) Моделирование атак на уровне приложений, сетевых сервисов и ОС, с использованием специализированных средств и сведений об известных уязвимостях в отношении выявленных систем.

3.9. Тестирование механизмов сегментации

Работы на данном этапе заключаются в проверки эффективности использованных мер сегментации сети (отделении границ сертификации от остальной сети). В состав работ входит:

11) Сбор сведений о ЛВС Заказчика изнутри сети;
12) Идентификация сетевых сервисов и приложений по реакции на внешнее воздействие из-за пределов границ сертификации;

13) Выборочная проверка правил межсетевого экранирования на границе среды сертификации.

Результатом работ на данном этапе является отчет по результатам дополнительного внутреннего тестирования сегментации, содержащий информацию о выполненных работах, включая информацию обо всех выявленных недостатках и рекомендации по их устранению.

3.10. Сертификационный аудит соответствия требованиям стандарта PCI DSS

3.10.1. Определение области сертификации

На данном этапе аудиторской группой Исполнителя производится определение и согласование актуальной области аудита. Для этого, Исполнителем запрашивается имеющаяся информация о структуре информационных систем процессингового центра и процессах обеспечения информационной безопасности, а также определяются системные компоненты, каналы передачи данных и другие системы, включаемые в область аудита в соответствии с требованиями Стандарта PCI DSS.

Результатом данного этапа является перечень системных компонент, подлежащих аудиту.

3.10.2. Сбор свидетельств соответствия

На данном этапе, аудиторы Исполнителя проводят необходимое интервьюирование ответственных сотрудников Заказчика, проверяют параметры безопасности системных компонент, входящих в область аудита и документируют свидетельства аудита необходимые для формирования итоговой отчетной документации.

Сбор всех необходимых сведений производится путем изучения нормативной документации, проведения интервью, анализа конфигурационных файлов, демонстрирования сотрудниками Заказчика выполняемых ими процедур по обеспечению информационной безопасности.

3.10.3. Формирование отчетной документации

На данном этапе аудиторская группа Исполнителя на основе собранных свидетельств аудита проводит анализ выполнения требований Стандарта PCI DSS, которые определены в шести группах и формирует необходимую отчётную документацию:

n) Построение и поддержание защищенной вычислительной сети;
o) Защита информации держателей платежных карт;
p) Реализация программы управления уязвимостями;
q) Реализация мер по строгому контролю доступа;
r) Регулярный мониторинг и тестирование вычислительных сетей;
s) Поддержание политики информационной безопасности.

Результатом работ на данном этапе являются отчетные документы, направляемые Заказчику и в Международные Платежные Системы:

- Report on Compliance (на английском языке);
- Attestation of Compliance (на английском языке);
- Сертификат соответствия PCI DSS (на русском и английском языках).

3.11. Консультационная поддержка по вопросам выполнения требований Стандарта PCI DSS

Целью работ на данном этапе является консультирование специалистов Заказчика по возникающим вопросам, связанным с разъяснением конкретных требований Стандарта PCI DSS и способам их выполнения.

Консультационная поддержка Заказчика осуществляется в течение 1 года с момента заключения договора. Прием запросов осуществляется по электронной почте и телефону. Время ответа на каждый поступивший запрос может составлять от 1 до 5 рабочих дней с даты приема запроса, в зависимости от сложности запроса.

ИСПОЛНИТЕЛЬ:	**ЗАКАЗЧИК:**
_____	_____
_____	_____
_____**ФИО**	_____ **ФИО**
М.П.	**М.П.**

Приложение №2
к Договору № _____
от «___»_____202_ года

КАЛЕНДАРНЫЙ ПЛАН-ГРАФИК ОКАЗАНИЯ УСЛУГ

№ этапа	Наименование этапа	Начало (раб. дни)	Окончание (раб. дни)
1.	**Предварительный аудит соответствия требованиям стандарта PCI DSS 3.2.1**	Д1	Д1+20
2.	**Внешнее тестирование на проникновение**	Д2	Д2+10
3.	**Внутреннее тестирование на проникновение**	Д3	Д3+13
4.	**Предоставление доступа к консоли для проведения внешнего сканирования уязвимостей (ASV-сканирование)**	Д4	Д4+2
5.	**Тестирование механизмов сегментации**	Д5	Д5+5
6.	**Сертификационный аудит соответствия требованиям стандарта PCI DSS 3.2.1**	Д6	Д6+25

Примечания:

- Д* – согласованная (по электронной почте) с Заказчиком дата начала оказания услуг по соответствующему этапу.
- Часть этапов может выполняться параллельно.

ИСПОЛНИТЕЛЬ:

_____

_____

_____**ФИО**

М.П.

ЗАКАЗЧИК:

_____

_____

_____ **ФИО**

М.П.

Приложение № 3
к Договору № _____
от «___»_____202_ года

Соглашение о конфиденциальности

г. Ташкент «___»_____202_ г.

_____, именуемое в дальнейшем «Исполнитель», в лице _____, действующего на основании _____, с одной стороны, и АКБ «ASIA ALLIANCE BANK», именуемый в дальнейшем «Заказчик», в лице И.о. Председателя Правления Хакимова У.А., действующего на основании Устава, с другой стороны, именуемые по отдельности «Сторона», а вместе - «Стороны», заключили настоящее Соглашение о конфиденциальности (далее - «Соглашение») о нижеследующем.

1. Предмет Соглашения

1.1. Настоящим Стороны определяют порядок и условия защиты Конфиденциальной Информации, которой Стороны будут обмениваться в ходе проведения переговоров, заключения договоров и исполнения обязательств по ним. При этом в целях настоящего Соглашения Сторона, передающая Конфиденциальную Информацию, будет именоваться «Передающая Сторона», а Сторона, получающая Конфиденциальную Информацию - «Получающая Сторона».

2. Термины и определения

2.1. В соответствии с настоящим Соглашением, Конфиденциальной Информацией признается любая информация, предоставляемая Передающей Стороной Получающей Стороне в устной, письменной форме и/или на электронных носителях (включая какие-либо сведения, данные, отчетные документы, разъяснения, прогнозы), при условии, что такая информация идентифицирована в качестве Конфиденциальной Информации при ее передаче.

Информация, переданная устно, будет считаться Конфиденциальной только в том случае, когда конфиденциальный характер этой информации подтверждается в письменной форме путем составления Сторонами соответствующего Протокола или иного документа в момент передачи такой Информации.

2.2. Под раскрытием, разглашением или передачей Конфиденциальной Информации понимается действие или бездействие, в результате которого Конфиденциальная Информация в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия Передающей Стороны.

3. Обязательства Сторон

3.1. В целях исполнения предмета настоящего Соглашения Стороны обязуются:

3.1.1. Не передавать друг другу Конфиденциальную Информацию по открытым каналам телефонной, телеграфной и факсимильной связи, а также с использованием сети Интернет без принятия мер, обеспечивающих ее защиту.

3.1.2. Осуществлять защиту Конфиденциальной Информации, обеспечивающую ее сохранность (неразглашение).

3.1.3. Использовать Конфиденциальную Информацию строго в целях осуществления договорной деятельности. При этом не осуществлять без предварительного письменного согласия Передающей Стороны раскрытие Конфиденциальной Информации любым способом, за исключением случаев, когда:

а) от Получающей Стороны требуется передать Конфиденциальную Информацию органам государственной власти в соответствии с действующим законодательством. При этом до непосредственной передачи Конфиденциальной Информации Получающая Сторона обязан направить Передающей Стороне соответствующее уведомление в письменной форме;

б) передача Конфиденциальной Информации своим работникам и должностным лицам вызвана неотложностью исполнения Получающей Стороной договорных обязательств, при условии, что Получающая Сторона несет ответственность за выполнение требований по защите Конфиденциальной Информации лицами, которым в соответствии с настоящим пунктом сообщается эта информация;

в) Конфиденциальная Информация является общеизвестной не по вине Получающей Стороны и была предоставлена Получающей Стороне третьей стороной.

3.1.4. Незамедлительно информировать друг друга о случаях раскрытия Конфиденциальной Информации, организовать расследование этих фактов. При проведении расследования фактов раскрытия Конфиденциальной Информации Стороны по взаимному соглашению вправе направлять друг другу специалистов в области защиты информации. Оплата расходов, связанных с командированием таких специалистов, производится Стороной, допустившей разглашение Информации.

3.2. Получающая Сторона обязана:

- Незамедлительно сообщить Передающей Стороне о допущенном Получающей Стороной либо ставшем известном Получающей Стороне факте разглашения либо угрозы разглашения, незаконном получении или незаконном использовании Конфиденциальной Информации третьими лицами.

- Не копировать и не воспроизводить другими способами Конфиденциальную Информацию, за исключением случаев, когда это необходимо для целей договоров, заключенных между Сторонами. К копиям должны применяться те же требования по соблюдению конфиденциальности, что и к оригиналам.

- Незамедлительно уведомить Передающую Сторону любым видом связи в случаях:

а) поступления в адрес Получающей Стороны требования (запроса) органов государственной власти, иных государственных органов, органов местного самоуправления, судов, органов прокуратуры, органов предварительного следствия, органов дознания о передаче Конфиденциальной Информации, полученной от Передающей Стороны;

б) изъятия (выемки, ареста) в установленном законом порядке Конфиденциальной Информации, полученной от Передающей Стороны;

в) повреждения, утраты, хищения и других случаях неправомерного выбытия из владения Конфиденциальной Информации, полученной от Передающей Стороны;

г) в других случаях, когда возникла необходимость либо целесообразность передачи Конфиденциальной Информации, полученной от Передающей Стороны, третьим лицам.

4. Распоряжение Конфиденциальной Информацией

4.1. Вся информация, раскрываемая Передающей Стороной другой Стороне в соответствии с настоящим Соглашением, независимо от формы передачи является и остается исключительной собственностью Передающей Стороны.

4.2. По письменному требованию Передающей Стороны вся Конфиденциальная Информация подлежит незамедлительному возврату или уничтожению Получающей Стороной, за исключением случаев, когда возврат или уничтожение документов противоречит действующему законодательству Республики Узбекистан. В течение 10 (десяти) дней после получения такого требования Получающая Сторона должна вернуть или уничтожить все оригиналы Конфиденциальной Информации и уничтожить все ее копии и воспроизведения в любой форме, имеющиеся в ее распоряжении, а также в распоряжении лиц, которым она передала с соблюдением условий настоящего Соглашения такую Конфиденциальную Информацию, кроме случаев, когда Получающая Сторона в соответствии с законодательством Республики Узбекистан обязана хранить одну копию Конфиденциальной Информации, полученной от Передающей Стороны для осуществления договорной деятельности.

4.3. Любая Конфиденциальная Информация, не истребованная и не возвращенная одной из Сторон, будет храниться другой Стороной в течение 5 (пяти) лет (с соблюдением в течение всего указанного срока хранения в отношении хранимой информации положений о конфиденциальности настоящего Соглашения) с даты прекращения действия настоящего Соглашения. По истечении указанного в настоящем пункте срока хранения информация подлежит уничтожению.

4.4. В течение 1 (одного) рабочего дня с даты уничтожения Конфиденциальной Информации по основаниям, предусмотренным п. 4.2., 4.3. Соглашения, Получающая Сторона обязуется в письменной форме уведомить Передающую Сторону о факте уничтожения такой Конфиденциальной Информации.

5. Ответственность Сторон

5.1. Сторона, допустившая утерю или разглашение Конфиденциальной Информации, несет ответственность за реальный документально подтвержденный ущерб, понесенный Передающей Стороной, и вытекающий из или в связи с любым разглашением Конфиденциальной Информации, в соответствии с действующим законодательством Республики Узбекистан.

6. Прочие положения

6.1. Права и обязанности Сторон по настоящему Соглашению в случае реорганизации какой-либо из Сторон переходят к соответствующему правопреемнику (правопреемникам). В случае ликвидации какой-либо Стороны, такая Сторона до завершения ликвидации обязана обеспечить возврат Передающей Стороне всех оригиналов и уничтожение всех и любых копий Конфиденциальной Информации, переданной Передающей Стороной.

6.2. Все споры и разногласия, которые могут возникнуть между Сторонами в связи с настоящим Соглашением, будут по возможности решаться путем переговоров между Сторонами. При невозможности урегулирования споров путем переговоров в разумные сроки, такие споры, по требованию любой из Сторон, передаются для окончательного разрешения в Арбитражный суд по месту нахождения ответчика.

6.3. Настоящее Соглашение толкуется и регулируется в соответствии с законодательством Республики Узбекистан.

6.4. Любые поправки, изменения и дополнения к настоящему Соглашению имеют силу только в том случае, если они составлены в письменном виде и подписаны уполномоченными представителями каждой из Сторон.

6.5. Настоящее Соглашение вступает в силу со дня его подписания Сторонами и действует до «____» _____20____ года. Конфиденциальная информация, переданная Сторонами в течение срока действия настоящего Соглашения не подлежит разглашению в течение пяти календарных лет с даты прекращения действия Соглашения.

6.6. Настоящее Соглашение составлено в двух экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.

7. Подписи Сторон:

ИСПОЛНИТЕЛЬ:	**ЗАКАЗЧИК:**
_____	_____
_____	_____
_____**ФИО**	_____ **ФИО**
М.П.	**М.П.**