

**Техническая спецификация
на Комплекс работ по восстановлению базы данных и предоставлению
доступа к архивным материалам**

1. Краткое описание и сроки выполнения работ

- 1.1. Наличие или развёртывание серверных мощностей в дата центре на территории РК
- 1.2. Проведение комплекса мероприятий для обеспечения норм информационной безопасности в том числе, но не ограничиваясь, исполнение пп.2.1-2.5.
- 1.3. Установка Платформы для разархивации и конвертации базы данных, обеспечивающую совместимость со структурной конфигурацией баз источников за 2020 год, 2021год, 2022год, 2023год, 2024год, 2025 год, и целевой базы данных платформы E-HUB
- 1.4. Перенос базы данных из архива
- 1.5. Базовая настройка SQL серверов.
- 1.6. Конфигурирование кластера SQL.
- 1.7. Базовая настройка web серверов
- 1.8. Настройка IIS.
- 1.9. Настройка кластера NLB
- 1.10. Настройка web публикации
- 1.11. Базовая настройка маршрутизаторов.
- 1.12. Настройка VPN сервера.
- 1.13. Подготовка методики тестирования и проведение тестирования на отказоустойчивость
- 1.14. Подключение пользователей Заказчика к интегрированной в сервис (без использования сторонних цифровых систем) службе технической поддержки выполняющей работы в соответствии с требованиями данного Технического регламента.
- 1.15.
- 1.16. Восстановление и структурирование изолированных архивных баз данных заказчика сформированных на портале <https://pvl.ekitaphana.kz/> за 2020 год, 2021год, 2022год, 2023год, 2024год, 2025 год, имеющих отличную друг от друга структурную конфигурацию.
- 1.17. Бесшовная интеграция данных в платформу E-HUB
- 1.18. Пункты 1.1-1.18 должны быть выполнены (в течении 3 календарных дней с момента подписания договора)
- 1.19. Предоставление персонифицированного WEB доступа к восстановленным данным сотрудникам заказчика, согласно ранее произведённым регистрационным данным (через 3 календарных дня с момента подписания договора и до 31.12.2025)

2. Требования к Исполнителю.

- 2.1. Исполнитель, для обеспечения информационной безопасности при работе с персональными данными находящимися в архивах, обязан на основании подпункта 11-1) статьи 7-1 Закона Республики Казахстан «Об информатизации» иметь в наличии полученный в Комитете по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан Акт по результатам проведения испытаний на соответствие требованиям информационной безопасности платформы для восстановления и работы с архивными базами данных сформированными на портале <https://pvl.ekitaphana.kz/> за 2021год, 2022год, 2023год, 2024год, 2025 год.
 - 2.2. Наличие собственного верифицированного Call-центр не менее 150 входящих линий связи. Постоянно действующий на протяжении периода не менее 2 лет.
 - 2.3. Потенциальный Исполнитель должен иметь или арендовать сертифицированный Data-центр соответствующий характеристикам согласно п.4.1 активно действующий на протяжении не менее 2 лет.
 - 2.4. Наличие собственных или арендных серверных мощностей хранения и обработки данных для бесперебойного обеспечения работы сервиса, не менее чем в трёх ЦОДах расположенных в трёх распределённых регионах РК по уровню безопасности не ниже TIERIII из расчёта одна активная и две резервные, обеспечивающие полное зеркалирование данных и готовых к подключению в активную работу. При использовании арендных серверных мощностей, для обеспечения верификации, Исполнитель должен предоставить информацию о резервировании и полной предоплате услуг ЦОДа на период 6 месяцев вперёд, с даты заключения договора согласно данного Технического регламента.
 - 2.5. В рамках Работы с целью успешной интеграции Системы Исполнитель должен организовать и провести работы по бесшовной интеграции с информационными системами Заказчика.
3. Требования к программному обеспечению для организации работы Системы в рамках выполнения Работы.
- 3.1. Применяемое в процессе внедрения Системы прикладное программное обеспечение должно быть зарегистрировано в органах юстиции РК
 - 3.2. В части прикладного программного обеспечения и выполняемых работ должно быть обеспечено 100% Казахстанского содержания.
 - 3.3. Пул технологий Системы должен состоять из следующих компонентов: свободная объектно-реляционная система управления базами данных PostgreSQL, программное обеспечение WEB сервера - Nginx, который должен обеспечивать работу с пользователями посредством web браузера программная платформа веб-приложений – Python3 Django, программное обеспечение операционных систем: Ubuntu – программное

обеспечение, необходимое для развертывания всех остальных приложений, платформа веб-приложений – Python3 Node.JS, в состав которой должны входить веб-сервисы, программная инфраструктура, модель программирования

3.4. Исполнитель в рамках оказания Услуг должен обеспечить взаимодействие с внешними системами при помощи Web-сервисов и использовании стандартов REST и форматов JSON, протоколы Интернет – HTTP, HTTPS, сетевой протокол TCP/IP. Для реализации различного рода протоколов взаимодействия должны использоваться открытые стандарты, на основе языка разметки JSON, как языка описания информации.

3.5. Исполнитель в рамках выполнения Работы должен обеспечить ключевые механизмы информационной безопасности: идентификация и аутентификация, управление доступом, протоколирование и аудит, криптография, экранирование (межсетевые экраны – Firewall). Экранирование как сервис безопасности должно обеспечивать: разграничение межсетевого доступа путем фильтрации передаваемых данных, преобразование передаваемых данных. При входе в закрытую часть Система должна производить аутентификацию пользователя по средствам протокола авторизации OAuth, который позволяет предоставить права на использование ресурса. Наличие прав должно определяться токеном (уникальным идентификатором), который может быть одним и тем же для разных пользователей, или же у одного пользователя в разное время могут быть разные токены, либо по идентификатору сессии браузера. Предоставление прав должно происходить в обмен на предоставление токена либо идентификатора сессии браузера. В общем случае должно быть нельзя определить, кому принадлежит токен, и кто в настоящий момент пользуется правами. Открытие Системы должно быть возможно только при наличии токена либо идентификатора сессии браузера. Пользователь должен указывать логин и пароль для авторизации, и Система должна осуществлять его проверку и предоставлять при верных данных токен. Если логин и пароль, либо существующий токен не проходит предусмотренных проверок, то вход в систему должен быть невозможен. Также токен должен иметь ограниченное количество времени жизни, при истечении времени жизни токена пользователю необходимо проходить авторизацию повторно.

4. Требования к обеспечению аппаратной инфраструктуры комплекса работ.

4.1. В рамках договора Исполнитель должен провести работы и обеспечить Систему серверным пространством со следующими характеристиками и условиями работы на период действия Договора и на гарантийный период по 31 декабря 2024 года: RAM не менее 256 GB, CPU, количество

ядер - не менее 48, HDD не менее 150 TB, симметричный интернет-канал со скоростью не менее 1000 мбит/с для серверов с публичными статическими IP адресами. Для предоставления качественной и стабильной Работы Исполнитель должен выделить вышеуказанные вычислительные ресурсы в собственном или арендуемом Центре Обработки Данных расположенном в РК по уровню безопасности не ниже TIERIII а также в резервном синхронизированном с основным, Центре Обработки Данных с аналогичными характеристиками, расположенном в РК, не ближе 500км от основного, с предоставлением подтверждающих документов (далее - ЦОД).

4.2. Исполнитель должен организовать технологическое администрирование серверного пространства на период действия Договора.

4.3. Исполнитель должен обеспечить бесперебойную работу серверного пространства на период действия договора с уровнем доступности – не менее 97 %.

4.4. Исполнитель должен организовать круглосуточную службу технической поддержки в режиме 24/7

4.5. Модели серверного оборудования должны быть современными и быть на официальной поддержке производителей до конца срока Работы.

4.6. Класс оборудования должен быть не ниже уровня enterprise с дублированием блоков питания, системы охлаждения, процессорной мощности, сетевых карт – выход из строя компонента не должен влиять на работоспособность Работы.

4.7. Программное обеспечение для виртуализации должно быть основано на технологиях, которые находится прямо на аппаратных средствах (Bare Metal), представлено ведущими производителями (VMware/Microsoft Hyper-V/Citrix XenServer, Сeph и т.д.

5. Требования к обеспечению каналам коммуникаций.

5.1. В рамках договора и с целью обеспечения пользователей заказчика доступом к информационным ресурсам, Исполнитель должен использовать существующие интернет-каналы

5.2. В рамках Услуг и с целью обеспечения ответственных сотрудников организаций образования оперативным доступом к службе технической поддержки Исполнитель обязан организовать закрытый информационный канал взаимодействия (помимо телефонных звонков, мессенджеров и т.д.) пользователей с операторами службы технической поддержки.

6. Техническая и консалтинговая поддержка пользователей Системы.

6.1. С целью обеспечения качественной Работы и повышения результата работы Системы Исполнитель должен в рамках Работы СП внешних пользователей организовать и предоставить единую электронную почту, и интегрированный в Систему модуль обмена сообщениями для приема

внутренних обращений. Время работы СП должно быть в режиме 24/7, за исключением праздничных дней. Все внешние обращения должны поступать на электронный адрес СП, зарегистрированный посредством модуля «Почтовый сервис». Поступающие внешние и внутренние обращения должны обрабатываться СП. Специалисты СП, получив первичное обращение, должны рассмотреть его, сформулировать ответ и направить его заявителю. Ответ должен представляться пользователю на языке обращения. СП в ходе рассмотрения обращений, при необходимости должна отправлять запрос (уточнение) на дополнительную информацию отправителю обращения или ответственным сотрудникам вовлечённых в процесс организаций. После получения необходимой дополнительной информации, СП в рамках рабочего времени, должна рассмотреть его, сформировать ответ и направить его заявителю. Если в ходе рассмотрения обращения СП определяет, что оно не относится к ее компетенции, заявителю должен быть направлен отказ в рассмотрении обращения с указанием причины. В случае если обращение относится к смежной информационной системе, заявителю дополнительно должна предоставлена информация о службе поддержки той информационной системы, в которую ему необходимо обратиться. В случае если уровень сложности обращения не дает возможности дать ответ на Заявку, снимающий возникшее затруднение, СП должно направить заявителю сообщение с указанием крайнего срока решения обращения. В случае выявления особо критичной проблемы, ответственным лицом Заказчика производится выбор приоритета рассмотрения данной проблемы, руководствуясь срочностью, важностью проблемы, а также степенью влияния проблемы на Систему и интеграционные сервисы. Исполнитель, руководствуясь установленным приоритетом, обязан реагировать на обращение и предпринимать необходимые действия. Если в процессе рассмотрения будет выявлено, что причины Ошибки связаны с проблемами, находящимися вне компетенции Исполнителя, то после соответствующего уведомления, рассмотрение данного обращения прекращается.

- 6.2. Основным средством взаимодействия с пользователями должны являться внутренняя коммуникационная среда. Однако в исключительных ситуациях, при необходимости, сотрудники СП с согласия пользователя, могут обрабатывать заявку по телефону. Для обеспечения оперативного решения возникающих проблем, при первичном обращении пользователями должно обеспечиваться предоставление следующей информации: подробное описание возникшего затруднения, которое должно включать следующую обязательную информацию: описание последовательности действий,

приводящих к ошибке, снимки экрана (screenshot), поясняющие возникшую проблему. другая информация, которая, по мнению пользователя, может быть полезной при рассмотрении обращения. В случае отсутствия вышеуказанной информации и информации необходимой для решения возникшего затруднения, СП должна формировать запрос пользователю на уточнение, с целью получения необходимых данных. В случае, если в течение 3 (трех) рабочих дней, начиная со следующего дня, после отправки запроса СП пользователь не предоставил дополнительную информации или предоставляемая информация не соответствует запрашиваемой, рассмотрение заявки может быть прекращено, и СП должно направить отправителю сообщение о ее закрытии, с указанием причин. После закрытия заявки, последующие обращения от пользователя по данной проблеме должны определяться как новая заявка. СП должна оставлять за собой право не принимать и не обрабатывать обращения в следующих случаях: требование о предоставлении услуг, не оговоренных данным документом или противоречащих условиям, указанным в нем, обращение содержит рекламу и другую информацию, которая не была запрошена СП и не имеет отношения к Услуге, обращение передано в формате, допускающем передачу исполняемых приложений, в частности вирусов и иных вредоносных программ, в сообщении используются ненормативная лексика, фразы/слова, противоречащие общественным нормам, принципам гуманности и морали (в частности, слов непристойного содержания, призывов антигуманного характера, оскорбляющих человеческое достоинство либо религиозные убеждения), в обращении содержатся оскорбления или угрозы в адрес сотрудников СП.

- 6.3. В ходе выполнения своих задач СП должна предоставлять пользователям Системы следующие консалтинговые Работы: рассмотрение заявок и принятие решений по ним, учет заявок и принятых мер и решений по ним, консультирование пользователей по вопросам работы Системы, консультирование эксплуатационного персонала по вопросам администрирования Системы, консультирование эксплуатационного персонала по выявлению причин сбоев работы Системы, вызванных некорректным функционированием программного обеспечения. В случае поступления вопросов, находящихся вне компетенции Исполнителя, они должны перенаправляться Заказчику с соответствующим комментарием.
- 6.4. К услугам, на которые не распространяется компетенция Исполнителя и в оказании которых Исполнитель, соответственно, не обязан принимать участие, относится следующее: вопросы, ошибки или сбои в работе аппаратно-программного обеспечения пользователя, вопросы, ошибки или сбои в работе общесистемного программного обеспечения

пользователя, устранение проблем функционирования ПК или мобильного телефона пользователя, общесистемного программного обеспечения ПК или мобильного телефона пользователя, его сервисов и компонент – антивирусное ПО и т.д.

7. Контроль выполнения работ по договору

- 7.1. Все пункты данного Технического регламента подлежат полному исполнению.
- 7.2. Контроль выполнения работ Исполнителем возлагается на Ответственного сотрудника Заказчика.
- 7.3. В случае неисполнения Исполнителем данного Технического регламента Ответственный сотрудник Заказчика обязан незамедлительно проинформировать Первого руководителя Заказчика и представителя Исполнителя. Исполнитель обязан незамедлительно приложить усилия для разрешения ситуации неисполнения.
- 7.4. В случае если неисполнение Исполнителем данного Технического регламента привело к финансовым, методическим, организационным или репутационным потерям Заказчика или педагогов Заказчика либо нарушению исполнительской дисциплины Заказчика или педагогов Заказчика перед организациями методического обеспечения и вышестоящими организациями ОО или УО, Заказчик обязан незамедлительно принять решение о расторжении договора с Исполнителем, с обязательным возмещением финансовых потерь и неустоек по договору.

8. Соответствие стандартам

Исполнитель и предоставляемый комплекс работ должны соответствовать стандартам:

- 8.1. Системы менеджмента качества требованиям СТ РК ISO 9001:2016
- 8.2. Системы управления информационной безопасностью (СТ РК ISO/IEC 27001-2015)