«УТВЕРЖДАЮ»
Первый заместитель председателя правления – главный инженер АО «Алмалыкский ГМК»
_____ А. Абдукадыров
«28» 06 2022 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на приобретение

Услуг по разработке и внедрению системы управления информационной безопасностью (СУИБ) в соответствии с международным стандартом ISO 27001:2013 АО «Алмалыкский ГМК»

на 7 листах

действует с 28.06.2022

«СОГЛАСОВАНО»
Заместитель председателя правления по безопасности
АО «Алмалыкский ГМК»
_____ Р. Саттаров
«27» 06 2022 г.

Заместитель председателя правления по цифровизации
АО «Алмалыкский ГМК»
_____ А. Азизов
«24» 06 2022 г.

Начальник Департамента ИТ
АО «Алмалыкский ГМК»
_____ Р. Максумов
«23» 06 2022 г.

И. о. начальника УАП
АО «Алмалыкский ГМК»
_____ В. Ирисметов
«20» 06 2022 г.

Главный инженер СТСБ
АО «Алмалыкский ГМК»
_____ И. Дятлов
«20» 06 2022 г.

«РАЗРАБОТАНО»
Инженер по информационной безопасности Отдела безопасности СТСБ
АО «Алмалыкский ГМК»
_____ Д. Мунтин
«20» 06 2022 г.

г. Алмалык
2022 г.

ОГЛАВЛЕНИЕ

1. Общие сведения 3
1.1 Термины, определения и сокращения 3
1.2 Наименование заказчика (пользователя) и поставщика Решения 3
1.3 Основание для приобретения 3
1.4 Плановые сроки начала и окончания предоставления услуг 3
1.5 Порядок оформления и предъявления заказчику результатов предоставления услуг . 3
1.6 Источник финансирования 4
2. Наименование и цели приобретения услуг 4
3. Требования к поставщику 4
4. Требования к услугам 5
4.1 Состав услуг 5
4.2 Требования к результатам услуг 6
5. Порядок контроля и приёмки системы 6
5.1 Порядок сдачи и приёмки результатов работ и услуг 6
6. Требования по передаче технических и иных документов по завершению и сдаче результатов услуг 7
7. Требования по обучению поставщиком персонала заказчика по результатам оказанных услуг 7
8. Авторские права с указанием условий о передаче неисключительных прав на объекты интеллектуальной собственности, возникших в связи с исполнением обязательств поставщика по выполнению оказанию услуг 7

1. ОБЩИЕ СВЕДЕНИЯ

1.1 Термины, определения и сокращения

ИБ	Информационная безопасность
ИТ	Информационные технологии
СУИБ	Система Управления Информационной Безопасностью
ТЗ	Техническое задание
СДО	Система дистанционного обучения

1.2 Наименование заказчика (пользователя) и поставщика Решения

Заказчик – АО «Алмалыкский ГМК», Республика Узбекистан Ташкентская область инд.110100 г. Алмалык, ул. Амира Темура, 53, e-mail: info@agmk.uz, тел: (998 71) 141-90-09, факс: (998 71) 141-90-33.

Поставщик – Организация (компания), берущая на себя ответственность по предоставлению услуг, являющимися предметом приобретения. Поставщик будет определён по результатам конкурса на отбор наилучшего предложения.

1.3 Основание для приобретения

- Мероприятия по устранению выявленных недостатков информационной безопасности утвержденные Председателем Правления АО «Алмалыкский ГМК» А.Х. Хурсановым от 10.09.2021г. на основании АКТА №13/10712 от 27.07.2021г. по результатам проверки состояния обеспечения информационной и кибербезопасности информационной инфраструктуры АО «Алмалыкский ГМК» от СГБ.

1.4 Плановые сроки начала и окончания предоставления услуг

Начало – Июль 2022 г.
Окончание – Декабрь 2022 г.

1.5 Порядок оформления и предъявления заказчику результатов предоставления услуг

Оформление и предъявление Заказчику результатов услуг по разработке и внедрению системы управления информационной безопасностью (СУИБ) в соответствии с международным стандартом ISO 27001: 2013 осуществляется Поставщиком согласно:

- сетевому графику по реализации проекта;
- требованиям государственных стандартов Республики Узбекистан по оформлению документации;
- требованиям данного Технического задания (ТЗ) с учётом требований, приведённых в подразделах по функциональной части.

Заказчик и Поставщик совместно формируют лист приёмки результатов предоставления услуг по каждому этапу.

1.6 Источник финансирования

Собственные средства АО «Алмалыкский ГМК».

2. НАИМЕНОВАНИЕ И ЦЕЛИ ПРИОБРЕТЕНИЯ УСЛУГ

Наименование проекта - услуги по разработке и внедрению системы управления информационной безопасностью (СУИБ) в соответствии с международным стандартом ISO 27001: 2013.
Целью преокта является разработка стратегии управления рисками и развития ИБ, внедрение системы управления информационной безопасностью предприятия и сопуствующих технических и организационных мероприятий ИБ.

3. ТРЕБОВАНИЯ К ПОСТАВЩИКУ

Исполнитель должен иметь репутацию, достаточный опыт реализации проектов сопоставимого уровня, а также необходимые сертификаты и ресурсы, позволяющие выполнить задание на требуемом уровне, дающем основания полагать, что качество предоставляемых услуг будет соответсвовать требованиям Заказчика.

Поставщик должен соответствовать следующим обязательным требованиям:

- иметь в команде не менее 3 аудиторов ISO 27001;
- предоставить сертификаты персонала:
  - ISO 27001 Lead Auditor – не менее одного человека;
  - ISO 27001 Internal Auditor – не менее одного человека;
  - ISC2 Certified Information Systems Security Professional (CISSP) – не менее двух человек;
  - ISACA Certified Information Systems Auditors (CISA) – не менее одного человека.
- Иметь в штате персонал с следущими знаниями и навыками:
  - Навыки работы с технической документацией;
  - Навыки проведения интервью;
  - Владение английским языком;
  - Знание методологии, практик и подходов к проектированию систем защиты от киберугроз;
  - Знание основных ИТ технологий по доменам:
    - Вычислительные сети;
    - Аппаратное и инженерное обеспечение серверных;
    - Средства виртуализации;
    - Операционные системы;
    - Системы управления базами данных;
    - Средства мониторинга и управления ИТ;
    - Средства автоматизации процессов Security Operation Center.
- иметь подтвержденный опыт выполнения не менее 3-х аналогичных проектов на протяжении последних 3-х лет.
- иметь подтвержденный опыт выполнения не менее 1-го аналогичного проекта в Узбекистане на протяжении последних 3-х лет.
- Иметь подтвержденный опыт системной интеграции и консалтинга в области информационной безопасности и информационных технологий в Узбекистане – не менее 5 проектов.

Допускается участие консорциума из компаний, которые по совокупности квалификации отвечают вышеуказанным требованиям

4. ТРЕБОВАНИЯ К УСЛУГАМ

4.1 Состав услуг

- Предварительный аудит состояния ИТ и ИБ предприятия
  - Планирование аудита текущего состояния СУИБ;
  - Обследование инфраструктуры предприятия на соответствие требованиям ISO 27001;
  - Анализ процессов на соответствие требованиям ISO 27001;
  - Анализ существующих средств защиты и процессов ИБ;
  - Разработка рекомендаций по устранению отклонений от требований стандарта и плана по их реализации
- Разработка методологии оценки рисков ИБ
  - Выбор, доработка, адаптация, согласование и утверждение методики управления рисками информационной безопасности;
  - Проведение пробной оценки рисков информационной безопасности на основе принятой методики и составление отчета по ее результатам;
- Разработка стратегии управления рисками и развития ИБ
  - Составление Плана обработки рисков;
  - Разработка стратегии информационной безопасности предприятия согласно стратегии бизнеса.
- Разработка комплекса регламентирующих документов
  - Внутренняя нормативная документация для обеспечения функционирования СУИБ на основании разработанной ранее стратегии, плана обработки рисков и рекомендаций предварительного аудита;
  - Политика информационной безопасности и политика управления ИБ;
  - Внесение изменений в существующие процессы СУИБ с целью повышения их эффективности и приведения в соответствие Стандарту;
  - Разработка контрольных процедур (Политик, Процедур, Стандартов и пр.) согласно Плана обработки рисков;
- Внедрение технических и организационных мероприятий ИБ
  - Планирование проектов по внедрению СУИБ согласно Плану обработки рисков.
  - Участие в проектах по внедрению СУИБ, согласованных на предыдущем этапе в качестве консультанта;
  - Проведение финального осмотра после завершения внедрения СУИБ и предоставление отчета по результатам анализа внедрения.

4.2 Требования к результатам услуг

№	Этап/Фаза проекта	Ожидаемый результат
1	Предварительный аудит состояния ИТ и ИБ предприятия	• Отчет по результатам аудита • План устранения несоответствий
2	Разработка методологии оценки рисков ИБ	• Методика анализа рисков ИБ • Анализ рисков ИБ • Отчет по результатам анализа рисков ИБ
3	Разработка стратегии управления рисками и развития ИБ	• Стратегия развития информационной безопасности • План обработки рисков ИБ
4	Разработка комплекса регламентирующих документов	• Политика информационной безопасности • Политики обеспечения информационной безопасности (почта, Интернет, носители) • Положение о документации системы управления информационной безопасности СУИБ (полный комплект документов для требований ISO 27001) • Положение о применимости ISO 27001
5	Внедрение технических и организационных мероприятий ИБ	• Внедрены все запланированные контрольные процедуры СУИБ • Выполняются бизнес-процессы, регламентированные СУИБ

Стратегия управления рисками и развития информационной безопасности должна включать:

- Формирование и описание процессов ИБ;
- Организация структуры службы информационной безопасности;
- Требования к участникам и ролям службы ИБ;
- Требования к системам и проектам ИБ;
- Порядок взаимодействия процессов бизнеса, ИТ и ИБ;
- Перечень мер по обеспечению требуемого уровня информационной безопасности, включая необходимые регламенты, инструкции и другую управленческую документацию.

Вся документация по проекту разрабатывается и ведется на узбекском и русском языке.

5. ПОРЯДОК КОНТРОЛЯ И ПРИЁМКИ СИСТЕМЫ

5.1 Порядок сдачи и приёмки результатов работ и услуг

Оказанные услуги Поставщик оформляет актом выполненных работ (услуг) согласно проекту, согласовывает с Заказчиком и предоставляет Заказчику счёт-фактуру на сумму

выполненных работ (услуг) и двухсторонне оформленные акты выполненных работ (услуг) по проекту.

6. ТРЕБОВАНИЯ ПО ПЕРЕДАЧЕ ТЕХНИЧЕСКИХ И ИНЫХ ДОКУМЕНТОВ ПО ЗАВЕРШЕНИЮ И СДАЧЕ РЕЗУЛЬТАТОВ УСЛУГ

По завершению предоставления услуг по каждому этапу Поставщик передаёт Заказчику документы, перечисленные в разделе 4.2 данного ТЗ.

7. ТРЕБОВАНИЯ ПО ОБУЧЕНИЮ ПОСТАВЩИКОМ ПЕРСОНАЛА ЗАКАЗЧИКА ПО РЕЗУЛЬТАТАМ ОКАЗАННЫХ УСЛУГ

Поставщик обеспечивает подготовку обслуживающего персонала Заказчика в количестве не менее 7 человек к работе по сопровождению системы управления информационной безопасностью путём проведения:

- семинаров по теоретическим основам СУИБ (требования станадртов ISO27001 и ISO27002, процессы входящие в СУИБ, методология управления рисками);
- обучающих семинаров;
- практики на рабочем месте.

Все вышеуказанные варианты подготовки персонала Заказчика могут проводится с использованием онлайн технологий системы дистанционного обучения (СДО).

8. АВТОРСКИЕ ПРАВА С УКАЗАНИЕМ УСЛОВИЙ О ПЕРЕДАЧЕ НЕИСКЛЮЧИТЕЛЬНЫХ ПРАВ НА ОБЪЕКТЫ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ, ВОЗНИКШИХ В СВЯЗИ С ИСПОЛНЕНИЕМ ОБЯЗАТЕЛЬСТВ ПОСТАВЩИКА ПО ВЫПОЛНЕНИЮ ОКАЗАНИЮ УСЛУГ

После предоставления всех услуг, Поставщик передаёт неисключительное право на ипользование полученных результатов с неограниченным сроком действия.