**Техническая спецификация закупаемых услуг**

1. **Наименование: Услуги по обучению персонала/сотрудников**
2. **Технические и качественные характеристики**

Услуги по повышению квалификации по обеспечению информационной безопасности.

* 1. **Требования к потенциальному поставщику:**

1) потенциальный поставщик должен обладать опытом работы по проведению курсов по повышению квалификации по обеспечению информационной безопасности.

 (*необходимо предоставить подтверждающие документы (акты оказанных услуг) за последние 3 года предшествующие закупке*);

2) наличие у потенциального поставщика сертифицированного преподавательского состава (*необходимо предоставить диплом либо сертификат*);

* 1. Потенциальный поставщик должен оказать Заказчику услуги по проведению работникам Заказчика обучения по обеспечению информационной безопасности в соответствии с Постановлением Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 21 сентября 2020 года № 89. - «Система управления информационной безопасностью. СТ РК ISO/IEC 27001-2015. Подготовка к испытаниям ИС на соответствие требованиям ИБ» (далее – Обучение).

Обучение проводится в количестве не менее 40 (сорока) академических часов, включаемым в зачет по обязательным часам.

Обязательные часы курса повышения квалификации включают в себя следующее изучение теоретических и практических вопросов, а именно:

* Информация, виды информации, информационная безопасность, способы защиты информации
* Объекты защиты (активы) и угрозы. Понятия активов, угроз, уязвимостей. Другие основные термины и определения ИБ;
* Риски ИБ понятия, подходы, стратегии управления рисками и их обработки;
* Типовые риски при обеспечении бесперебойной работы Информационных систем. Подходы к Управлению ИБ. Стандарты ИСО. Назначение стандартов ИСО 27000, 27001, ИСО 27002, 27005 и другие;
* Механизм взаимодействия и применения стандартов. Структура. Термины. Определения;
* Поддержка при построении СУИБ со стороны руководства. Область действия СУИБ и Политика ИБ;
* Определение Области действия СУИБ (границ СУИБ), на примерах обеспечения бесперебойной работы Информационных систем, Концепция и политика ИБ, методы и примеры их формирования;
* Инвентаризация активов. Создание Реестра активов Организации, их оценка и ранжирование (На примерах обеспечения бесперебойной работы Информационных систем). Определение ценности активов;
* Типовые уязвимости защиты активов в организациях, аттестующих на ИБ ИС. Оценка угроз, возможного ущерба. Критерии оценки;
* Анализ и оценка рисков;
* Способы борьбы с рисками, снижение вероятностей из реализации, способы снижения ущерба при реализации рисков;
* Выбор стратегий и рекомендации Стандартов. Обоснование необходимости принятия документов:
	+ Положение о работе с активами. Инструкция по обеспечению сохранности коммерческой и служебной тайны. Правила работы в местах общего доступа;
	+ Правила приема, внутреннего распорядка и увольнения работников. Порядок доступа в офис. План непрерывности бизнеса;
	+ Правила проведения внутреннего аудита. Политика защиты прав интеллектуальной собственности. Правила управления несоответствиями. Правила анализа СУИБ со стороны руководства;
	+ Положение по модификации ИС и другие, их роль в построении СУИБ. Остаточные риски;
* Завершение внедрения СУИБ;
* Матрица применимости. Записи СУИБ. Механизмы анализа и пересмотра СУИБ;
* Рабочая документация СУИБ, исполнение созданных процедур. Структура документации. Проверка исполнения документации СУИБ аудиторами уполномоченной организации. Проверка на уязвимость программно-аппаратных средств защиты информации сканерами безопасности. Подготовка к Испытаниям ИС;
* Сертификация СУИБ. Этапы сертификационного процесса, сроки и ориентировочный бюджет;
* Аудит информационной безопасности, обработка инцидентов ИБ, Планы непрерывности бизнеса;
* Планирование аудита. Подготовка аудитора. Документы. Сбор свидетельств. Техника аудита. Ведение записей. Формулирование несоответствий;
* Отличия СТ РК ISO/IEC 27001-2015 от СТ РК ИСО/МЭК 27001-2008. Сравнительный анализ. «Экзамен»;
* Оценка уровня усвоения слушателями материалов курса;

Потенциальный поставщик должен предоставить программу обучения с указанием дисциплин из вышеперечисленных, входящих в обучение, количеством академических часов по каждой дисциплине, подробным расписанием по датам и времени.

Обучение по программе «Система управления информационной безопасностью. СТ РК ISO/IEC 27001-2015. Подготовка к испытаниям ИС на соответствие требованиям ИБ» проводится в режиме оффлайн либо онлайн, в формате семинара/вебинара/курса и т.д.

Во время обучения потенциальный поставщик должен предоставить методические материалы по обучению (слайды, инструкции, видеолекции, материалы на бумажном носителе или в электронном варианте и т.д.).

По завершению оказания услуг Потенциальный поставщик должен предоставить: сертификат слушателя на бумажном носителе и его электронный вариант, с указанием количества пройденных академических часов.

1. **Прочие характеристики:**

3.1.Место оказания услуги: Республика Казахстан, г. Нур-Султан.

3.2. Срок оказания услуги - до 31 декабря 2022 года с даты подписания Договора, по заявке Заказчика

3.3. Количество слушателей: 2 работника Заказчика.

3.4. Язык проведения обучения: русский.

3.5. Потенциальный поставщик после оказания услуги должен предоставить: анкеты по оценке эффективности, отчет о проведенном обучении и другие виды подтверждения..

1. **Соответствие стандартам:** СТ РК ISO/IEC 27001-2015
2. **Подлежит лицензированию:** нет
3. **Гарантийный срок на выполняемые работы:** отсутствует
4. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ прилагаются и являются неотъемлемой частью технической спецификации (если имеются, указать необходимые приложения: к примеру, дефектные акты, ведомости, чертежи и т.д.)

**Главный менеджер HR-службы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Бекишева Ж.П.**