ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке 513322
способом Тендер путем проведения конкурентных переговоров

Лот № (256 У, 1814067) Услуги консультационные по обеспечению безопасности

Заказчик: Товарищество с ограниченной ответственностью "KAP Technology"
Организатор: Товарищество с ограниченной ответственностью "KAP Technology"

1. Краткое описание ТРУ

Наименование	Значение
Номер строки	256 У
Наименование и краткая характеристика	Услуги консультационные по обеспечению безопасности, Услуги консультационные по обеспечению безопасности
Дополнительная характеристика	Оказание консультационных услуг по построению системы управления информационной безопасностью (СУИБ) в соответствии с требованиями стандарта ISO/IEC 27001:2013
Количество	1.000
Единица измерения	-
Место поставки	КАЗАХСТАН, г.Нур-Султан, ул. Е-10, здание 17/12, 6 этаж
Условия поставки	-
Срок поставки	С даты подписания договора по 12.2020
Условия оплаты	Предоплата - 0%, Промежуточный платеж - 0%, Окончательный платеж - 100%

2. Описание и требуемые функциональные, технические, качественные и эксплуатационные характеристики

Техническое задание на оказание консультационных услуг по построению системы управления информационной безопасностью (СУИБ) в соответствии с требованиями стандарта
ISO/IEC 27001-2013

Аннотация
В данном документе приведено техническое задание на выполнение проектных работ по построению системы управления информационной безопасностью в ТОО “KAP Technology" (далее - СУИБ).
Целями построения СУИБ ТОО «KAP Technology» в соответствии со стандартом ISO/IEC 27001-2013 являются:
• Повышение общего уровня информационной безопасности компании;
• Повышение прозрачности процесса управления информационной безопасностью (ИБ);
■ Процедуры по обеспечению ИБ;
■ Критерии оценки эффективности выполняемых мероприятий по обеспечению ИБ;
■ Четкое разделение полномочий и ответственности за обеспечение ИБ;
■ Построение методики оценки рисков ИБ;
■ Интеграция процедуры проведения внутренних аудитов ИБ с существующей в компании методикой проведения внутренних аудитов ИСУ;
■ Приведение документов компании в соответствие с Приложением А стандарта ISO/IEC 27001:2013;
■ Обоснование затрат на ИБ.
• Снижение рисков информационной безопасности, связанных с возможными ущербами для активов Заказчика от реализации угроз информационной безопасности;
• Задачи проекта, направленные на приближение к целям проекта, включают:
• Обследование, обнаружение и анализ несоответствий требованиям стандарта ISO/IEC 27001-2013, определение границ области действия СУИБ.
• Разработка процессов СУИБ для области действия, соответствующей требованиям стандарта ISO/IEC 27001-2013.
• Внедрение процессов СУИБ в области действия СУИБ.

Содержание

1. Заявление о конфиденциальности

Данный документ содержит конфиденциальную информацию, принадлежащую ТОО “KAP Technology”.
Исполнитель обязуется использовать данную информацию только для целей, указанных в настоящем задание. Исполнитель также обязуется не разглашать, не копировать, не распространять данный документ и не раскрывать его содержание среди юридических и/или физических лиц, не связанных непосредственно с процедурой оценки и обработки данного Задания, без предварительного согласования с Заказчиком.
Указанные ограничения не распространяются на информацию, которая включена в данный документ, но была известна Исполнителю для составления коммерческого предложения, на информацию, известную из общедоступных источников, или на информацию, полученную Исполнителем из сторонних источников, относительно которых Исполнитель не несет каких-либо обязательств по сохранению конфиденциальности полученной информации.

2. Общие сведения

Данный документ представляет собой техническое задание на выполнение проектных работ по созданию системы управления информационной в ТОО “KAP Technology”, соответствующей требованиям международного стандарта ISO/IEC 27001-2013
Работы должны проводится в соответствии с методиками, разработанными в соответствии с ISO/IEC 27001-2013 и соответствующими лучшим международным практикам в области построения систем управления информационной безопасностью.
2.1 Границы проведения работ
Границы проведения работ включают в себя 1 территориальную площадку в г.Нур-Султан.
Ориентировочное количество сотрудников, входящих в ОД СУИБ - не более 350 сотрудников.

3. Состав, содержание и основные этапы работ по созданию СУИБ

Работы по созданию СУИБ для Заказчика проводятся в 5 основных этапов.
Этап 1. Обследование, обнаружение и анализ несоответствий требованиям стандарта ISO/IEC 27001-2013, определение границ области действия (далее - ОД) СУИБ.
Этап 2. Разработка процессов СУИБ для области действия, соответствующей требованиям стандарта ISO/IEC 27001-2013.
Этап 3. Внедрение процессов СУИБ в области действия СУИБ.
В течении 3 (трех) рабочих дней после заключения Договора Исполнитель должен предоставить Заказчику на согласование детализированный План выполнения работ с указанием мероприятий по этапам и сроков исполнения.
Все разработанные/актуализированные нормативные документы должны содержать блок схемы и соответствовать лучшим мировым практикам, требованиям международного стандарта ISO/IEC 27001:2013 и внутренним процессам системы управления информационной безопасности Компании.
3.1 Этап 1. Обследование, обнаружение и анализ несоответствий требованиям стандарта ISO/IEC 27001-2013, определение границ ОД СУИБ
Основной целью данного этапа работ является определение границ области действия1 СУИБ, а также формирование перечня необходимых работ, выполнение которых позволит создать СУИБ, отвечающую требованиям стандарта ISO/IEC 27001-2013.
На данном этапе осуществляются следующие работы:
• Определение границ области действия СУИБ. На данном подэтапе анализируются бизнес-процессы Компании, включая бизнес-процессы, на которые предполагается установить действие СУИБ, определяются подразделения и сотрудники Заказчика, задействованные в данных бизнес-процессах. Согласованные границы ОД СУИБ фиксируются в документе «Область действия СУИБ»
• Проведение обследования в рамках ОД СУИБ с целью выявления несоответствий существующих организационных процедур и программно-¬технических средств защиты информации требованиям стандарта ISO/IEC 27001-2013 (GAP-анализ). На данном подэтапе осуществляется сбор и анализ информации о существующих регламентах, процедурах и средствах обеспечения информационной безопасности, используемых в рамках выбранной области деятельности, делается заключение о степени их соответствия стандарту ISO/IEC 27001-2013. Обследование проводится посредством интервьюирования и анкетирования.
Работы выполняются специалистами Исполнителя при активном участии ответственного персонала со стороны Заказчика.
Обследование проводится посредством анкетирования и проведения интервью.
Результатом данного этапа являются следующие данные:
• «Отчет по результатам обследования», включающий заключение о степени соответствия рассмотренной области требованиям стандарта ISO/IEC 27001-2013,
• Документ «Область действия СУИБ»

1 Область действия СУИБ (ОД) - представляет собой выделенную область Компании, в которой внедряются процессы управления информационной безопасностью, подаваемые на сертификацию в соответствии с требованиями стандарта ISO/IEC 27001-2013. Область деятельности должна покрывать те бизнес-процессы компании, в которых присутствует критичная для деятельности компании, ее клиентов и контрагентов информация.

3.2 Этап 2. Разработка процессов СУИБ для области действия, соответствующей требованиям стандарта ISO/IEC 27001-2013
На данном этапе в соответствии с требованиями международного стандарта ISO/IEC 27001 осуществляются следующие работы:
• Проведение анализа и оценки рисков информационной безопасности.
• Разработка/корректировка процессов СУИБ для области действия.
3.2.1 Проведение анализа рисков информационной безопасности Заказчика
Целью подэтапа является идентификация активов Заказчика в рамках ОД СУИБ, оценка критичности данных активов и определение уровней рисков, связанных с реализацией угроз ИБ, которые могут нанести ощутимый ущерб в отношении идентифицированных активов. Данный подэтап подразумевает проведение следующих работ:
• Корректировка методики анализа рисков ИБ;
• Проведение инвентаризации и оценки критичности активов в рамках ОД СУИБ;
• Идентификация угроз и уязвимостей выявленных активов;
• Анализ и оценка рисков ИБ;
• Выбор мер противодействия рискам ИБ, разработка «Плана обработки рисков ИБ»;
• Разработка документа «Положение о применимости механизмов контролей СУИБ».
Результатом подэтапа являются:
• Документ «Методика анализа рисков ИБ»;
• Документ «Отчет об инвентаризации активов»;
• Документ «Отчет об анализе рисков ИБ»;
• Документ «План обработки рисков ИБ»;
• Документ «Положение о применимости механизмов контролей СУИБ»;
• Каталог рисков ИБ
3.2.2 Разработка процессов СУИБ и комплекта необходимой документации
На данном этапе производится определение ролевой структуры СУИБ, ответственных сотрудников, распределение обязанностей и ролей в части СУИБ, разработка документации СУИБ.
Разработка документации СУИБ производится специалистами Исполнителя с привлечением в оговоренном объеме специалистов Заказчика.
Этап разработки документации включает 2 вида работ:
• Разработка/корректировка основного комплекта документации СУИБ, требуемого основной частью стандарта ISO/IEC 27001.
• Политика информационной безопасности.
• Руководство по СУИБ
• Документ управления документацией и записями СУИБ.
• Документ внутренних аудитов ИБ.
• Документ управления корректирующими и предупреждающими действиями.
• Документ анализа СУИБ со стороны руководства.
• Документ оценки эффективности мер обеспечения ИБ.
• Документ управления инцидентами ИБ.
• Документ обучение и повышение осведомленности
• Документ обеспечения сетевой безопасности
• Документ обеспечения непрерывностью бизнеса
• Разработка/корректировка документов, требуемых Приложением А стандарта ISO/IEC 27001:2013.
• Документ управления уязвимостями.
• Документ управления доступом к ресурсам компании.
• Документ антивирусной защиты.
• Документ резервного копирования.
• Документ использования корпоративной электронной почты и сети Интернет.
• Стандарт классификации информационных активов и категорирования информации.
• Стандарт обеспечения физической защиты.
• Стандарт разработки, эксплуатации и сопровождения ПО.
• Стандарт эксплуатации и сопровождения оборудования.
• Перечень требовании по ИБ для поставщиков
• Политика использования криптографического контроля информации
• Управление ЭЦП
• Документ по обработке персональных данных
• Документ по сохранности служебной и коммерческой тайне
Результатом работ на данном подэтапе являются проекты документов, в соответствии с приведенным выше перечнем необходимых документов.
3.3 Этап 3. Внедрение процессов СУИБ на области действия СУИБ
Внедрение процессов СУИБ на области действия СУИБ производится за счет реализации следующих работ специалистами Исполнителя при активном содействии сотрудников Заказчика:
• Консультации по выполнению персоналом Заказчика, вовлеченным в процесс функционирования СУИБ, своих ролевых обязанностей, в соответствии с изданной организационно-распорядительной и нормативной документацией;
• Контроль и первичный запуск всех процессов СУИБ.
• Помощь в документировании записей СУИБ в соответствии с подготовленными процедурами;

• Проведение вводного тренинга для ключевых сотрудников Заказчика, ответственных за разработку и внедрение СУИБ, с учетом разработки курса обучения, программы обучения;
• Внесение корректировок в разработанные документы, с учетом изменений процессов и взаимосвязей;
• Оказание консультаций по функционированию и взаимосвязям всех вновь разработанных процессов СУИБ.

Результатом данного этапа являются:
• Работающие процессы СУИБ;
• Обученный персонал вопросам СУИБ в рамках ОД;
• Материалы для обучения персонала в части ИБ.

4. Продолжительность и стоимость работ
Работы по созданию системы управления информационной безопасностью ТОО «KAP Technology» предлагается проводить в несколько этапов (при этом отдельные работы на каждом из этапов могут проводиться параллельно). Ориентировочные длительность и стоимость каждого из этапов работ представлена в Табл. 1.

5. Квалификационные требования
1. Не менее двух специалистов, обладающих международными сертификатами ведущий аудитор ISO 27001:2013 Lead Auditor - подлинность сертификата проверяется по запросу у тренинг-центра, выдавшего сертификат;
2. Не менее одного специалиста, обладающего действующим сертификатом Cisco CCNP Security – подлинность сертификата проверяется онлайн на сайте https://www.cisco.com;
3. Не менее двух специалистов, обладающих действующим сертификатом Cisco CCNP Routing and Switching – подлинность сертификата проверяется онлайн на сайте https://www.cisco.com;
4. Не менее одного специалиста, обладающего действующим сертификатом Cisco CCNA Wireless – подлинность сертификата проверяется онлайн на сайте https://www.cisco.com;
5. Не менее одного специалиста, обладающего действующим сертификатом IPMA не ниже уровня C или сертификатом PMI не ниже уровня PMP, выданного обладателем прав на методику и систему сертификации или его авторизованным партнёром по обучению и сертификации Подлинность сертификата проверяется по запросу у тренинг-центра, выдавшего сертификат;
6. Не менее одного специалиста, обладающего действующим сертификатом CISM (международный сертификат по управлению информационной безопасностью) – подлинность сертификата проверяется онлайн на сайте https://www.isaca.org;
7. Не менее 1 эксперта аудитора по системе менеджмента ИБ зарегистрированного в Казахстаном реестре экспертов аудиторов по подтверждению соответствия систем менеджмента информационной безопасностью.

3. Технические стандарты

№ п/п	Зарегистрирован в РК	Обозначение	Номер документа	Категория	Наименование	Область применения	Разработчик	Страницы	МКС	Статус	Приказ	Дата введения с	Дата по
1	Да				ISO/IEC 27001:2013								

Приложение

Таблица №1.docx
Таблица №1.docx

Подписал Нысанов Нурлан Серикович
Дата подписания 08.12.2020