**Техническая на поиск и подбор персонала Менеджера информационной безопасности.**

Потенциальный поставщик (далее Исполнитель) должен предоставить кандидатуры необходимых Заказчику специалистов в течение 15 (пятнадцати) календарных дней со дня получения заявки на подбор персонала.

Ответственность за достоверность сведений резюме кандидата несет Исполнитель. После размещения Заказчиком заявки на подбор персонала, Исполнитель должен предоставить диплом и/или сертификаты, подтверждающие квалификацию кандидата.

В случае если Заказчика не удовлетворяет квалификация кандидата, Исполнитель должен в течении 5 (пяти) календарных дней со дня получения соответствующего уведомления предоставить альтернативные резюме специалистов, соответствующих квалификационным требованиям Заказчика

В случае если Заказчик удовлетворён квалификацией предложенного кандидата, оплата за услуги по подбору персонала будет осуществлена в течение 10 дней с момента начала работы кандидата в штате Заказчика.

В случае если у Заказчика будут мотивированные претензии к качеству работы нанятых специалистов, в течение 3 месяцев после заключения трудового договора, Исполнитель гарантирует в течении 7 (семи) календарных дней произвести процедуру подбора персонала для осуществления замены специалиста на безвозмездной основе.

Должностные обязанности

- Разрабатывать, управлять, соблюдать корпоративную политику, стандартов и процедур информационной безопасности. Политика должна основываться на международных стандартах (напр., ISO270001), правовых и нормативных требованиях (например, PCI DSS).
- Проводить внутренние проверки для определения рисков, недостатков и уязвимостей ИТ инфраструктуры, корпоративных приложений, бизнес-процессов и практики.
- Предлагать и внедрять меры по повышению уровня безопасности ИТ и устранению уязвимостей ИТ-инфраструктуры.
- Направлять процессы управления программными активами.
- Проводить оценку рисков информационной безопасности и всей деятельности ИТ.
- Управлять рисками, связанными с информационной безопасностью и всей деятельности ИТ.
- Направлять и следить за соблюдением практики ITIL.
- Контролировать и представлять отчет о нарушениях информационной безопасности или политики или стандартов.
- Управлять всеми инцидентами информационной безопасности и управлять внутренними и/или внешними командами для реагирования, разрешения и восстановления после инцидентов.

- Контролировать систему внутреннего контроля, чтобы обеспечить поддержание соответствующих уровней доступа, включая расследование нарушений разрешений и разрешений на удаление прав доступа по мере необходимости.

- Проводить исследования, связанные с информационной безопасностью.

- Обеспечить выполнение всех аспектов безопасности и управления рисками в соответствии с соответствующими правилами.

- Проводить тестирования на безопасность приложений и проникновения с использованием проверенных методов в области безопасности мобильных, веб-приложений.

- Реализовать возможности SAST / DAST / IAST и RASP в жизненные циклы разработки программного обеспечения.

- Внедрять методы моделирования угроз.

Управлять уязвимостью и представлять отчет

Требования к кандидату:

- Высшее образование в области компьютерных наук, вычислительной техники, информационных технологий или связанных с ними областях.

- Профессиональная сертификация в области информационной технологии/ информационной безопасности / Аудиту / Управлению корпоративными ИТ, такие как CISSP, CISA, CISM, CGEIT, OSCP.

- Профессиональная сертификация и опыт в области инфраструктуры ИТ.

- Хорошее знание и опыт работы с ISO 270001, PCI DSS и другими международными стандартами в области информационной безопасности и процессов.

- Хорошее знание законодательства, положений и международных норм по информационным ресурсам.

- Опыт в области разработки информационных технологий и политики безопасности, процедур, стандартов и руководящих принципов.

- Знания и опыт управления корпоративными и информационными рисками.

- Минимум 5 лет профессионального опыта в области безопасности приложений, тестирования на проникновение, оценки безопасности, разработки безопасного программного обеспечения итп.

- Опыт в области оценки уязвимости и оценки воздействия.

- Глубокие знания с помощью сканеров уязвимостей.

- Отличные навыки устного и письменного общения

- Знание разработки безопасного программного обеспечения.

- Опыт использования уязвимостей в Интернете, мобильных устройствах и приложениях.

- Большое чувство срочности и ответственности.

- Опыт работы на руководящей должности в области ведущих профессионалов информационной безопасности.

**Обязательное предоставление технической спецификации с предоставлением гарантийного обязательства (письмо подтверждение) об оказании услуг в соответствии с обязательными требованиями настоящей Технической спецификации.**