Государственная Транспортная Лизинговая Компания	**ДИРЕКЦИЯ ПО БЕЗОПАСНОСТИ**

ОБОСНОВАНИЕ
невозможности соблюдения запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей поставки программного обеспечения Vaultize (виртуальная комната данных)

2017

Предмет закупки: Лицензионное программное обеспечение Vaultize (виртуальная комната данных)

Обстоятельство, обусловливающее невозможность соблюдения запрета:

Подпункт «а» пункта 5.1.4 а именно: в реестре ПО (https://reestr.minsvyaz.ru/reestr/) отсутствуют сведения о программном обеспечении, соответствующем тому же классу программного обеспечения, что и программное обеспечение, планируемое к закупке.

Класс (классы) программного обеспечения: Средства обеспечения информационной безопасности, Прикладное программное обеспечение общего назначения, Офисные приложения, Системы управления процессами организации

Лицензионное программное обеспечение Vaultize Technologies

Неисключительные права на продукт Vaultize VZG-PVTC-LIC-FILE-SHARING-ADVANCED-DRM на 50 пользователей.

Предоставляемые неисключительные права (лицензия) включают в себя право на воспроизведение, ограниченное правом инсталляции, копирования и запуска программного обеспечения, предоставляемое с единственной целью передачи этого права конечным пользователям.

Производитель (разработчик) – Vaultize Technologies.

Вид поставки – неисключительная лицензия на 50 пользователей (с возможностью дальнейшего увеличения количества лицензий).

Срок действия лицензии: на все время действия исключительных прав

Пользовательский интерфейс – русский (английский - на выбор).

Требования к функциональным, техническим и эксплуатационным характеристикам:

1. Поддержка операционных систем семейства Windows, Linux и Mac OS, мобильных операционных систем Android и iOS

2. Возможность использования двухфакторной аутентификации пользователей

3. Авторизация пользователей на основе функциональных ролей для предоставления гранулярного доступа к ресурсам и защищенным конфиденциальным документам.

4. Хранение конфиденциальных документов в зашифрованных DRM (DRM-Digital rights management) -контейнерах.

5. Отправка по электронной почте ссылки на ресурс хранения, на котором требуется авторизация получателя, вместо самого документа.

6. Контроль операций в соответствии с предопределенными политиками безопасности, ведение журнала регистрации событий информационной безопасности (ИБ).

7. Передача конфиденциальных документов по зашифрованным каналам в виде DRM-контейнеров.

8. Маркирования документов с атрибутами, указывающими на различный уровень конфиденциальности, несколькими альтернативными способами (водяной знак, содержащий информацию об уровне конфиденциальности, либо соответствующие колонтитулы или метаданные в виде расширенных свойств документа)

Ограничения по использованию защищенного документа:

- Запрет на редактирование;

- Запрет на извлечение документа из DRM-контейнера;

- Запрет на открытие документа без авторизации на сервере заказчика;

- Запрет на открытие документа после истечения срока действия прав доступа;

- Запрет/разрешение на открытие защищенного документа на основе черных и белых списков IP-адресов;

- Блокировка доступа при достижении максимального кол-ва открытий DRM-контейнера, установленных владельцем документа;

- Запрет вывода документа на печать;

- Запрет на выполнение скриншотов экрана на мобильном устройстве и рабочей станции ;

- Запрет на копирование и вставку содержимого документа или его частей в буфер обмена;

- Ограничение прав доступа к документу по времени и дням недели.

Исходя из указанного, вышеизложенные функциональные, технические и (или) эксплуатационные характеристики (в том числе их параметры) программного обеспечения не представлены в сведениях о программном обеспечении, включенном в реестр российского ПО.