

ПРИЛОЖЕНИЕ №2

Регламент ролей, прав доступа и управления пользователями S-OMS

к Договору № ____ о предоставлении доступа к S-OMS

г. _____

« ____ » _____ 2026 года

ТОО «QOR.KZ», БИН 260440024350, в лице первого руководителя Левина Игоря Александровича, действующего на основании Устава, далее — «Оператор», с одной стороны, и

_____, БИН/ИИН _____, в лице _____, действующего на основании _____, далее — «Клиент», с другой стороны,

совместно именуемые «Стороны», утвердили настоящее Приложение №2 — Регламент ролей, прав доступа и управления пользователями S-OMS.

1. Общие положения

1.1. Настоящий Регламент определяет порядок создания, назначения, изменения, ограничения, блокировки и удаления ролей и прав доступа пользователей в S-OMS.

1.2. Настоящий Регламент является неотъемлемой частью Договора № ____ о предоставлении доступа к S-OMS.

1.3. S-OMS является операционным модулем управления охранными, объектными, диспетчерскими и инцидентными процессами в цифровой экосистеме QOR.

1.4. Цель настоящего Регламента — обеспечить разграничение доступа к данным, функциям, объектам, постам, сменам, персоналу, инцидентам, отчётам, настройкам и API S-OMS.

1.5. Доступ к S-OMS предоставляется по ролевой модели. Каждый пользователь получает только те права, которые необходимы для выполнения его служебных задач.

1.6. Клиент отвечает за корректное назначение ролей своим пользователям, своевременное удаление неактуальных доступов, контроль сотрудников и законность обработки данных в своей организации.

1.7. Оператор отвечает за техническую реализацию ролевой модели в пределах возможностей S-OMS и за управление платформенными доступами со стороны Оператора.

1.8. Все действия пользователей S-OMS могут фиксироваться в журнале действий.

2. Термины и определения

2.1. S-OMS — Security Operations Management System, операционный модуль управления охранными и объектными процессами.

2.2. Пользователь S-OMS — физическое лицо, которому предоставлен доступ к S-OMS.

2.3. Роль — набор прав доступа, определяющий, какие действия пользователь может выполнять в S-OMS.

2.4. Права доступа — разрешения на просмотр, создание, изменение, удаление, экспорт, назначение, подтверждение, закрытие или иное действие с данными и функциями S-OMS.

2.5. Организация — юридическое лицо, охранный агент, корпоративный клиент, служба безопасности или иная структура, подключённая к S-OMS.

2.6. Объект — адрес, территория, здание, помещение, жилой комплекс, бизнес-центр, предприятие, пост, зона или иной объект, заведённый в S-OMS.

2.7. Инцидент — тревожное обращение, событие, нарушение, заявка, происшествие, сигнал, сообщение или иное событие, зафиксированное в S-OMS.

2.8. Администратор организации — пользователь Клиента, управляющий доступами, объектами, пользователями и настройками своей организации.

2.9. Платформенная роль — роль пользователя со стороны Оператора, необходимая для управления платформой, технической поддержки, диспетчеризации, контроля качества и администрирования QOR.

2.10. Организационная роль — роль пользователя внутри организации Клиента.

2.11. API-пользователь — техническая учётная запись или интеграционный доступ, используемый для обмена данными между S-OMS и внешней системой.

2.12. Журнал действий — техническая запись действий пользователей в S-OMS.

3. Принципы управления доступами

3.1. Доступы в S-OMS предоставляются по следующим принципам:

минимально необходимый доступ;
персональная ответственность пользователя;
запрет общих учётных записей, если иное не согласовано Сторонами;
разделение административных и операционных прав;
разграничение доступа по организации;

разграничение доступа по объектам;
разграничение доступа по ролям;
разграничение доступа по действиям;
фиксация действий в журнале;
своевременное удаление неактуальных доступов;
защита персональных данных;
контроль доступа к инцидентам и тревожным обращениям.

3.2. Пользователь не должен получать доступ к данным, которые не относятся к его служебным задачам.

3.3. Пользователь не вправе передавать свой логин, пароль, код подтверждения, токен, API-ключ или иной идентификатор доступа третьим лицам.

3.4. Все действия, совершённые через учётную запись пользователя, считаются действиями соответствующего пользователя и организации Клиента, если не доказано иное.

3.5. Клиент обязан немедленно блокировать или инициировать блокировку доступа пользователя, который уволен, переведён, отстранён, утратил полномочия или больше не должен иметь доступ к S-OMS.

4. Категории ролей

4.1. В S-OMS могут использоваться следующие категории ролей:

платформенные роли Оператора;
административные роли Клиента;
операционные роли Клиента;
диспетчерские роли;
объектовые роли;
роли охранного персонала;
наблюдательные роли;
аудиторские роли;
технические роли;
API-роли.

4.2. Конкретный перечень ролей может отличаться в зависимости от тарифа, версии S-OMS, типа Клиента, подключённых модулей и настроек организации.

4.3. Оператор вправе изменять, добавлять, объединять или удалять роли в S-OMS, если такие изменения не нарушают оплаченный доступ Клиента в существенной части.

4.4. В отдельных проектах Стороны могут согласовать индивидуальные роли и права доступа.

5. Платформенные роли Оператора

5.1. Платформенные роли предназначены для управления S-OMS, поддержки Клиентов, обработки технических обращений, контроля качества, диспетчеризации и администрирования платформы.

5.2. К платформенным ролям могут относиться:

суперадминистратор платформы;
администратор платформы;
диспетчер платформы;
директор платформы;
специалист технической поддержки;
технический администратор;
аудитор платформы.

5.3. Суперадминистратор платформы имеет максимальный административный доступ к настройкам S-OMS, организациям, пользователям, ролям, системным параметрам, журналам и техническим функциям.

5.4. Администратор платформы управляет организациями, пользователями, настройками и доступами в пределах полномочий, предоставленных Оператором.

5.5. Диспетчер платформы может просматривать и обрабатывать инциденты, тревожные обращения, статусы, карточки событий и связанные данные в пределах служебной необходимости.

5.6. Директор платформы может иметь доступ к отчётам, аналитике, показателям качества, журналам и управленческим данным без права технического администрирования, если иное не установлено Оператором.

5.7. Специалист технической поддержки может получать ограниченный доступ к данным Клиента для решения технических обращений, восстановления доступа, проверки ошибок и сопровождения.

5.8. Технический администратор может иметь доступ к техническим настройкам, интеграциям, API, журналам ошибок, системным параметрам и инфраструктурным функциям.

5.9. Аудитор платформы может просматривать журналы, отчёты и действия пользователей без права изменения данных, если иное не установлено Оператором.

6. Организационные роли Клиента

6.1. Организационные роли предназначены для пользователей Клиента.

6.2. К организационным ролям могут относиться:

владелец организации;
администратор организации;

руководитель службы безопасности;
директор;
диспетчер организации;
оператор организации;
менеджер объекта;
начальник смены;
сотрудник охраны;
наблюдатель;
аудитор организации;
API-пользователь.

6.3. Владелец организации имеет максимальный доступ в пределах организации Клиента.

6.4. Администратор организации управляет пользователями, ролями, объектами, постами, настройками и базовыми справочниками организации.

6.5. Руководитель службы безопасности имеет доступ к объектам, инцидентам, персоналу, сменам, маршрутам, отчётам и показателям качества в пределах своей организации.

6.6. Директор имеет доступ к управленческим отчётам, аналитике, ключевым показателям и событиям организации без обязательного права операционного изменения данных.

6.7. Диспетчер организации принимает, распределяет, обновляет и закрывает инциденты в пределах своей организации, объектов и назначенных зон.

6.8. Оператор организации может создавать и обновлять инциденты, фиксировать события, назначать исполнителей и работать со статусами в пределах своих прав.

6.9. Менеджер объекта управляет данными конкретного объекта, постами, сменами, персоналом, инцидентами и отчётами по объекту.

6.10. Начальник смены управляет текущей сменой, сотрудниками смены, статусами, обходами, маршрутами и инцидентами в пределах смены.

6.11. Сотрудник охраны видит назначенные ему смены, посты, маршруты, задачи и инциденты, а также может выполнять действия, предусмотренные своей ролью.

6.12. Наблюдатель имеет доступ только на просмотр данных, которые разрешены Клиентом или Оператором.

6.13. Аудитор организации имеет доступ к отчётам, журналам и истории действий в пределах организации без права изменения операционных данных.

6.14. API-пользователь используется для интеграции внешних систем и имеет только те права, которые явно указаны в API-настройках.

7. Базовая матрица прав доступа

Раздел S-OMS	Владелец организации				Администратор организации			
Руководитель СБ охраны	Диспетчер		Менеджер объекта		Начальник смены		Сотрудник	
	Наблюдатель		Аудитор					
Организация	полный доступ	изменение	просмотр	нет	нет	нет	нет	нет
просмотр	просмотр							
Пользователи	полный доступ	полный доступ	просмотр	нет				
ограниченно	нет	нет	просмотр					
Роли	полный доступ	изменение в пределах прав	просмотр	нет	нет	нет	нет	нет
нет	нет	просмотр						
Объекты	полный доступ	полный доступ	просмотр/изменение	просмотр				
изменение своих объектов	просмотр	просмотр назначенных	просмотр					
просмотр								
Посты	полный доступ	полный доступ	просмотр/изменение	просмотр				
изменение своих объектов	просмотр	просмотр назначенных	просмотр					
просмотр								
Персонал	полный доступ	полный доступ	просмотр/изменение	просмотр				
просмотр/изменение по объекту	просмотр смены	свои данные	нет					
просмотр								
Смены	полный доступ	полный доступ	просмотр/изменение	просмотр				
изменение по объекту	изменение текущей смены	просмотр своих смен						
просмотр	просмотр							
Маршруты	полный доступ	полный доступ	просмотр/изменение	просмотр				
изменение по объекту	изменение текущих маршрутов	выполнение						
назначенных	просмотр	просмотр						
Инциденты	полный доступ	полный доступ	полный доступ	обработка				
обработка по объекту	обработка по смене	обработка назначенных						
просмотр	просмотр							
Статусы инцидентов	полный доступ	полный доступ	изменение					
изменение	изменение по объекту	изменение по смене	изменение назначенных					
нет	просмотр							
Отчёты	полный доступ	полный доступ	полный доступ					
ограниченно	по объекту	по смене	свои действия	просмотр	полный			
просмотр								
Журнал действий	полный доступ	просмотр	просмотр	нет	нет	нет	нет	нет
нет	нет	просмотр						
Экспорт данных	полный доступ	по разрешению	по разрешению	нет				
нет	нет	по разрешению						
API	полный доступ	по разрешению	нет	нет	нет	нет	нет	нет
нет								
Финансовые данные	по тарифу	по тарифу	нет	нет	нет	нет	нет	нет
нет								

8. Права по работе с организациями

8.1. Создание организации в S-OMS выполняется Оператором или уполномоченным платформенным администратором.

8.2. Клиент не вправе создавать дополнительные организации без согласования с Оператором, если такая функция не предусмотрена тарифом.

8.3. Изменение наименования, БИН, реквизитов, юридических данных и основного профиля организации может выполняться Оператором либо администратором организации в пределах предоставленных прав.

8.4. Удаление организации может выполняться только Оператором.

8.5. Блокировка организации может выполняться Оператором при нарушении Договора, задолженности, угрозе безопасности, незаконной обработке данных или иных основаниях, предусмотренных Договором.

9. Права по работе с пользователями

9.1. Пользователи S-OMS создаются Оператором, администратором организации или иным уполномоченным лицом.

9.2. При создании пользователя указываются:

ФИО;
номер телефона;
email;
роль;
организация;
объект, если применимо;
подразделение, если применимо;
статус доступа;
иные данные, необходимые для работы S-OMS.

9.3. Администратор организации вправе создавать пользователей только в пределах своей организации.

9.4. Администратор организации не вправе создавать платформенных пользователей Оператора.

9.5. Пользователь может иметь одну или несколько ролей, если это предусмотрено S-OMS.

9.6. При назначении нескольких ролей применяется совокупность прав, если система не устанавливает приоритет ограничений.

9.7. Оператор вправе ограничить возможность назначения отдельных ролей Клиентом.

9.8. Удаление или деактивация пользователя не удаляет автоматически историю его действий, если такая история необходима для аудита, отчётности, расследования инцидентов или исполнения закона.

10. Права по работе с объектами

10.1. Объекты создаются Оператором, администратором организации, менеджером объекта или иным уполномоченным пользователем.

10.2. Права на создание, изменение и удаление объектов зависят от тарифа и роли пользователя.

10.3. Менеджер объекта может управлять только теми объектами, которые ему назначены.

10.4. Сотрудник охраны может видеть только назначенные ему объекты, посты, маршруты, смены и инциденты, если иное не предусмотрено настройками.

10.5. Наблюдатель может просматривать объекты только в пределах предоставленного доступа.

10.6. Удаление объекта может быть ограничено, если по объекту есть активные инциденты, смены, посты, маршруты, отчёты или история событий.

10.7. Оператор вправе архивировать объект вместо удаления, если это необходимо для сохранения истории.

11. Права по работе с постами

11.1. Посты создаются внутри объектов.

11.2. Права на создание и изменение постов могут иметь:

владелец организации;
администратор организации;
руководитель службы безопасности;
менеджер объекта;
иные роли по настройке Оператора.

11.3. Начальник смены может видеть посты, связанные с его сменой.

11.4. Сотрудник охраны может видеть назначенный пост и связанные с ним инструкции, смены, маршруты и инциденты.

11.5. Удаление поста может быть ограничено, если по нему есть история смен, маршрутов или инцидентов.

12. Права по работе с персоналом

12.1. Модуль персонала используется для управления сотрудниками, охранниками, диспетчерами, руководителями и иными лицами Клиента.

12.2. Права на создание и изменение персонала могут иметь:

владелец организации;
администратор организации;
руководитель службы безопасности;
менеджер объекта в пределах объекта;
иные роли по настройке Оператора.

12.3. Доступ к персональным данным персонала должен быть ограничен служебной необходимостью.

12.4. Сотрудник охраны может видеть свои данные, свои смены, свои маршруты и назначенные задачи, если это предусмотрено настройками.

12.5. Директор, руководитель службы безопасности и аудитор могут просматривать данные персонала в объёме, необходимом для управленческой, контрольной или отчётной функции.

12.6. Клиент несёт ответственность за законность внесения данных персонала в S-OMS.

13. Права по работе со сменами

13.1. Смены могут создаваться и изменяться уполномоченными пользователями.

13.2. Права на управление сменами могут иметь:

владелец организации;
администратор организации;
руководитель службы безопасности;
менеджер объекта;
начальник смены в пределах своих полномочий.

13.3. Сотрудник охраны может видеть свои смены и отмечать действия, если это предусмотрено настройками.

13.4. Изменение завершённых смен может быть ограничено.

13.5. Корректировка завершённой смены может требовать прав администратора, руководителя службы безопасности или владельца организации.

13.6. История изменений смен может сохраняться в журнале действий.

14. Права по работе с маршрутами

14.1. Маршруты создаются для обходов, патрулирования, проверки, реагирования или иных операционных задач.

14.2. Права на создание и изменение маршрутов могут иметь:

владелец организации;
администратор организации;
руководитель службы безопасности;
менеджер объекта;
начальник смены в пределах смены.

14.3. Сотрудник охраны может видеть и выполнять назначенный маршрут.

14.4. Изменение маршрута после начала выполнения может быть ограничено.

14.5. Отчёт по маршруту может быть доступен руководителю службы безопасности, менеджеру объекта, администратору организации и аудитору.

15. Права по работе с инцидентами

15.1. Инциденты являются одним из ключевых разделов S-OMS.

15.2. Права на просмотр, создание, принятие, назначение, изменение статуса, закрытие и экспорт инцидентов зависят от роли пользователя.

15.3. Владелец организации и администратор организации имеют полный доступ к инцидентам своей организации, если иное не ограничено настройками.

15.4. Руководитель службы безопасности имеет полный операционный доступ к инцидентам своей организации или назначенных объектов.

15.5. Диспетчер организации может принимать, распределять, обновлять и закрывать инциденты в пределах своих прав.

15.6. Менеджер объекта может работать с инцидентами по назначенному объекту.

15.7. Начальник смены может работать с инцидентами, относящимися к его смене.

15.8. Сотрудник охраны может работать только с назначенными ему инцидентами, если иное не предусмотрено настройками.

15.9. Наблюдатель может только просматривать инциденты в пределах разрешённого доступа.

15.10. Аудитор может просматривать инциденты, историю статусов и отчёты без права изменения.

16. Права по статусам инцидентов

16.1. Изменение статусов инцидента доступно только ролям, которым такое право предоставлено.

16.2. Статусы могут включать:

создано;
принято;
назначено;
в пути;
на месте;
в обработке;
решено;
закрыто;
отменено;
ложная тревога;
ошибка обработки.

16.3. Оператор вправе изменять перечень статусов, если это необходимо для развития S-OMS или исполнения договоров.

16.4. Закрытие инцидента может требовать комментария, вложения, результата или подтверждения.

16.5. Для инцидентов высокого приоритета закрытие без комментария может быть запрещено.

16.6. Изменение статуса может фиксироваться в журнале действий с указанием пользователя, времени и комментария.

17. Права по отчётам и аналитике

17.1. Доступ к отчётам предоставляется в пределах роли и тарифа.

17.2. Отчёты могут включать:

инциденты;
объекты;
посты;
смены;
персонал;
маршруты;
время реакции;
статусы;
качество обработки;
ложные тревоги;
журнал действий;

нагрузку;
иные показатели.

17.3. Владелец организации, администратор организации, руководитель службы безопасности и директор могут иметь расширенный доступ к отчётам.

17.4. Менеджер объекта может видеть отчёты по своему объекту.

17.5. Начальник смены может видеть отчёты по своей смене.

17.6. Сотрудник охраны может видеть только свои действия, смены, маршруты и задачи, если это предусмотрено настройками.

17.7. Экспорт отчётов может быть ограничен отдельным правом.

18. Права на экспорт данных

18.1. Экспорт данных является повышенным правом доступа.

18.2. Экспорт может включать:

списки пользователей;
объекты;
посты;
персонал;
смены;
инциденты;
отчёты;
журналы;
аналитику;
иные данные.

18.3. Право экспорта может быть предоставлено:

владельцу организации;
администратору организации;
руководителю службы безопасности;
аудитору;
иной роли по согласованию с Оператором.

18.4. Оператор вправе ограничить экспорт персональных данных, геолокации, журналов, инцидентов и иных чувствительных данных.

18.5. Все выгрузки данных должны использоваться Клиентом только в законных целях.

18.6. Клиент несёт ответственность за сохранность выгруженных данных после их получения.

19. API-доступ

19.1. API-доступ предоставляется только при наличии соответствующего тарифа или отдельного соглашения.

19.2. API-пользователь получает только те права, которые необходимы для конкретной интеграции.

19.3. API-доступ может быть ограничен:

- организацией;
- объектом;
- типом данных;
- методами API;
- частотой запросов;
- IP-адресами;
- сроком действия ключа;
- лимитами тарифа.

19.4. API-ключи и токены являются конфиденциальной информацией.

19.5. Клиент обязан обеспечить хранение API-ключей и токенов в защищённой среде.

19.6. Оператор вправе отозвать API-ключ при нарушении правил, компрометации, подозрении на несанкционированный доступ, чрезмерной нагрузке или прекращении Договора.

20. Журнал действий

20.1. S-OMS может фиксировать действия пользователей в журнале действий.

20.2. В журнале могут фиксироваться:

- вход пользователя;
- создание пользователя;
- изменение роли;
- создание объекта;
- изменение объекта;
- создание поста;
- создание смены;
- изменение смены;
- создание инцидента;
- изменение статуса инцидента;
- закрытие инцидента;
- экспорт данных;
- API-запросы;
- изменение настроек;
- ошибки доступа;

иные действия.

20.3. Журнал действий используется для безопасности, расследования инцидентов, разрешения споров, контроля качества и защиты прав Сторон.

20.4. Доступ к журналу действий предоставляется ограниченному кругу ролей.

20.5. Удаление или изменение журнала действий пользователями Клиента не допускается, если такая функция не предусмотрена Оператором.

21. Порядок предоставления доступа

21.1. Доступ пользователю S-OMS предоставляется после создания учётной записи и назначения роли.

21.2. Доступ может быть создан:

Оператором;
администратором организации;
владельцем организации;
иным уполномоченным пользователем.

21.3. При предоставлении доступа должны быть указаны:

ФИО пользователя;
контактный номер;
email;
организация;
роль;
объекты доступа;
срок доступа, если он ограничен;
основание предоставления доступа.

21.4. Оператор вправе потребовать подтверждение полномочий пользователя.

21.5. Оператор вправе отказать в создании доступа, если данные неполные, недостоверные, нарушают требования безопасности или противоречат Договору.

22. Порядок изменения доступа

22.1. Изменение доступа выполняется при изменении должности, функций, объекта, смены, полномочий или организационной структуры.

22.2. Изменение доступа может включать:

смену роли;
добавление объекта;
удаление объекта;

добавление права;
ограничение права;
блокировку доступа;
изменение статуса пользователя;
отзыв API-ключа.

22.3. Клиент обязан своевременно изменять доступы пользователей при изменении их функций.

22.4. Если пользователь получил избыточный доступ, Клиент обязан немедленно ограничить его.

22.5. Оператор вправе самостоятельно ограничить доступ, если выявлен риск безопасности или нарушение Договора.

23. Порядок блокировки доступа

23.1. Доступ пользователя может быть заблокирован в следующих случаях:

увольнение;
отстранение;
изменение должности;
утрата полномочий;
компрометация аккаунта;
подозрение на нарушение;
передача доступа третьим лицам;
неправомерная выгрузка данных;
попытка доступа к чужим данным;
нарушение информационной безопасности;
неактивность;
требование Клиента;
требование Оператора;
требование компетентного органа;
прекращение Договора.

23.2. Клиент обязан немедленно блокировать доступ уволенных и отстранённых сотрудников.

23.3. Оператор вправе экстренно заблокировать доступ без предварительного уведомления, если доступ создаёт риск для платформы, данных, Пользователей, Клиента, Оператора или третьих лиц.

23.4. После блокировки пользователь не может выполнять действия в S-OMS.

23.5. История действий заблокированного пользователя сохраняется.

24. Порядок удаления пользователя

24.1. Удаление пользователя может быть технически заменено деактивацией, если сохранение истории действий необходимо для аудита, безопасности, отчётности или исполнения закона.

24.2. Пользователь может быть удалён или деактивирован:

администратором организации;
владельцем организации;
Оператором;
иным уполномоченным лицом.

24.3. Удаление пользователя не должно нарушать целостность истории инцидентов, смен, маршрутов и отчётов.

24.4. Оператор вправе сохранить технические записи о действиях удалённого пользователя.

25. Временный доступ

25.1. Временный доступ может предоставляться подрядчикам, аудиторам, консультантам, техническим специалистам или иным лицам.

25.2. Временный доступ должен иметь:

ограниченный срок;
ограниченную роль;
ограниченный набор объектов;
основание предоставления;
ответственного со стороны Клиента.

25.3. По окончании срока временный доступ должен быть заблокирован.

25.4. Клиент несёт ответственность за действия лиц, которым предоставил временный доступ.

26. Доступ технической поддержки Оператора

26.1. Техническая поддержка Оператора может получать доступ к данным Клиента только в объёме, необходимом для решения технического обращения, сопровождения, диагностики, исправления ошибки, настройки или исполнения Договора.

26.2. Доступ технической поддержки может быть постоянным или временным в зависимости от архитектуры S-OMS и условий тарифа.

26.3. Оператор обязан ограничивать доступ технической поддержки служебной необходимостью.

26.4. Действия технической поддержки могут фиксироваться в журнале действий.

26.5. Клиент понимает, что без доступа технической поддержки к отдельным техническим данным устранение ошибок может быть невозможно.

27. Доступ к персональным данным

27.1. Доступ к персональным данным предоставляется только ролям, которым такие данные необходимы.

27.2. Персональные данные могут включать:

ФИО;
телефон;
email;
должность;
роль;
данные смен;
данные маршрутов;
данные инцидентов;
геолокацию;
историю действий;
иные сведения.

27.3. Клиент отвечает за законность обработки персональных данных своими пользователями.

27.4. Оператор вправе ограничить отображение отдельных персональных данных в зависимости от роли.

27.5. Экспорт персональных данных может быть доступен только уполномоченным ролям.

28. Доступ к геолокационным данным

28.1. Геолокационные данные относятся к чувствительным операционным данным и должны быть доступны только при служебной необходимости.

28.2. Доступ к геолокации может быть предоставлен:

диспетчеру;
руководителю службы безопасности;
менеджеру объекта;
начальнику смены;
сотруднику охраны по назначенному событию;
администратору организации;
Оператору в рамках технической или диспетчерской функции.

28.3. Доступ к истории геолокации может быть ограничен.

28.4. Использование геолокации для контроля сотрудников допускается только при наличии законного основания со стороны Клиента.

28.5. Клиент несёт ответственность за незаконное использование геолокационных данных.

29. Доступ к тревожным обращениям

29.1. Тревожные обращения могут содержать персональные данные, геолокацию, адреса, комментарии, вложения и иные конфиденциальные сведения.

29.2. Доступ к тревожным обращениям предоставляется только пользователям, участвующим в их обработке, контроле, отчётности или аудите.

29.3. Пользователь, не связанный с объектом, организацией, сменой или функцией обработки обращения, не должен иметь доступ к такому обращению.

29.4. Оператор вправе ограничить просмотр тревожных обращений, если это необходимо для защиты данных.

29.5. Закрытые тревожные обращения могут быть доступны только уполномоченным ролям.

30. Разделение данных между организациями

30.1. Данные одной организации не должны быть доступны другой организации, если иное не предусмотрено договором, настройкой платформы, функцией агрегатора, корпоративной структурой или законным основанием.

30.2. Клиент не вправе получать доступ к данным другой организации.

30.3. Охранное агентство может получать доступ к данным Клиента только в объёме, необходимом для обработки переданных ему тревожных обращений или оказания услуг.

30.4. Корпоративный клиент может получать доступ к данным своих пользователей и объектов только в пределах договора, настроек, согласий и законодательства.

30.5. Оператор вправе иметь платформенный доступ к данным организаций в пределах технической, диспетчерской, контрольной, договорной и законной необходимости.

31. Нарушения правил доступа

31.1. Нарушениями правил доступа считаются:

передача логина или пароля;

использование чужого аккаунта;
создание общего аккаунта без согласования;
назначение избыточных прав;
несвоевременное удаление доступа;
попытка получить доступ к чужим данным;
несанкционированный экспорт данных;
копирование данных вне целей Договора;
передача данных третьим лицам;
использование API вне разрешённых целей;
обход технических ограничений;
попытка изменить журнал действий;
использование S-OMS в незаконных целях.

31.2. Нарушение правил доступа является основанием для блокировки пользователя, ограничения доступа Клиента, приостановления сервиса, расторжения Договора и предъявления требований о возмещении ущерба.

32. Ответственность Клиента

32.1. Клиент несёт ответственность за:

назначение ролей своим пользователям;
создание пользователей;
своевременное удаление доступов;
действия пользователей S-OMS;
действия администраторов организации;
действия временных пользователей;
законность обработки данных;
сохранность выгруженных данных;
соблюдение настоящего Регламента;
ущерб, причинённый Оператору, другим клиентам, пользователям или третьим лицам из-за нарушения правил доступа.

32.2. Если нарушение произошло через учётную запись пользователя Клиента, ответственность несёт Клиент, если не докажет отсутствие своей вины и принятие необходимых мер безопасности.

33. Ответственность Оператора

33.1. Оператор несёт ответственность за техническую реализацию ролевой модели в пределах возможностей S-OMS.

33.2. Оператор не отвечает за ошибочное назначение ролей Клиентом, избыточный доступ, предоставленный администратором Клиента, или несвоевременное удаление доступа сотрудника Клиента.

33.3. Оператор не отвечает за действия пользователей Клиента, если такие действия не вызваны прямой виновной ошибкой Оператора.

34. Проверка и аудит доступов

34.1. Клиент обязан регулярно проверять актуальность пользователей и ролей.

34.2. Рекомендуемая периодичность проверки доступов — не реже одного раза в квартал, если иной срок не установлен договором или внутренним регламентом Клиента.

34.3. Оператор вправе запросить у Клиента подтверждение актуальности доступов.

34.4. Оператор вправе провести технический аудит доступа при подозрении на нарушение безопасности.

34.5. По итогам аудита Оператор может потребовать:

- удалить неактуальных пользователей;
- снизить права отдельным ролям;
- отключить API-ключи;
- изменить пароль;
- включить дополнительные меры защиты;
- предоставить пояснения;
- устранить нарушение.

35. Изменение настоящего Регламента

35.1. Оператор вправе инициировать изменение настоящего Регламента при изменении S-OMS, требований безопасности, законодательства, тарифов, модулей или операционной модели QOR.

35.2. Изменения оформляются дополнительным соглашением, новой редакцией приложения или иным способом, согласованным Сторонами.

35.3. Если Клиент продолжает использовать S-OMS после вступления новой редакции Регламента в силу, он считается принявшим изменения, если такой порядок предусмотрен Договором или дополнительным соглашением.

36. Срок действия Регламента

36.1. Настоящий Регламент вступает в силу с даты его подписания Сторонами либо с даты предоставления Клиенту доступа к S-OMS.

36.2. Регламент действует в течение срока действия Договора.

36.3. Положения о конфиденциальности, персональных данных, ответственности, журналах действий, выгрузках и нарушениях доступа продолжают действовать после прекращения Договора в части ранее возникших обязательств.

37. Подписи Сторон

Оператор

ТОО «QOR.KZ»

БИН: 260440024350

Первый руководитель: Левин Игорь Александрович

Юридический адрес: M06F3A4, Карагандинская область, город Караганда, район имени Казыбек Би, пр. Бухар Жырау, ст-е 49/6

Телефон: +7 775 462 48 71

Email: _____

Сайт: _____

Подпись: _____

М.П.

Клиент

Наименование: _____

БИН/ИИН: _____

Руководитель: _____

Юридический адрес: _____

Телефон: _____

Email: _____

Подпись: _____

М.П.