СОГЛАШЕНИЕ О СОБЛЮДЕНИИ ТРЕБОВАНИЙ КИБЕРБЕЗОПАСНОСТИ

(далее – «Соглашение»)

Для целей настоящего документа принимаются следующие обозначения:

Исполнитель	–	Общество с ограниченной ответственностью «Облачные технологии» ИНН: 7736279160, ОГРН: 5167746080057
Заказчик	–	сторона по договору, соглашению или оферте (далее совместно – «Договор»), предметом которого является оказание Исполнителем услуг, описания и условия предоставления которых размещены на сайте Исполнителя по электронному адресу: https://cloud.ru/ru/documents#contracts

Исполнитель и Заказчик совместно именуются в Соглашении как «Стороны», а по отдельности – «Сторона».

Данное Соглашение является неотъемлемой частью Договора, содержащего ссылку на данный документ.

1. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ, ИСПОЛЬЗУЕМЫЕ В СОГЛАШЕНИИ

Безопасность информации	–	сохранение конфиденциальности, целостности и доступности информации; кроме того, также могут охватываться другие свойства информации, такие как аутентичность, учётность, неотказуемость и надежность.
Вредоносное программное обеспечение	–	программное обеспечение, предназначенное для получения несанкционированного доступа к устройству пользователя или к информации, хранимой на нем, с целью несанкционированного использования ресурсов или причинения вреда.
Доступность	–	гарантия того, что авторизованные пользователи могут иметь доступ и работать с необходимыми информационными активами, ресурсами и системами с требуемой производительностью.
Информационный ресурс	–	отдельный документ или отдельный массив документов, документ или массив документов в Информационной системе (библиотеке, архиве, фонде, банке/базе данных и т.д.).
Информационная система	–	совокупность взаимосогласованных компонентов программного, технического, информационного, организационного, методического, правового обеспечения, используемая пользователями для реализации заданной информационной технологии.
Недопустимое событие	–	событие в результате кибератаки, делающее невозможным достижение операционных и (или) стратегических целей организации или приводящее к значительному нарушению ее основной деятельности.
Инцидент кибербезопасности	–	реализованная угроза в киберпространстве; любое непредвиденное или нежелательное событие, которое может нарушить бизнес-процесс или состояние защищенности информационного актива.
Кибербезопасность	–	состояние защищенности киберпространства (сохранение конфиденциальности, целостности, доступности), в котором функционирует бизнес, достигающееся применением набора средств, методик и принципов, направленных на противодействие угрозам в киберпространстве и минимизацию последствий их реализации.
Киберпространство	–	информационное пространство, образованное совокупностью телекоммуникационных сетей и оборудования, средств вычислительной техники и программного обеспечения, а также деятельностью человека по его информационному наполнению.
Конфиденциальность	–	характеристика, определяющая, что информация не может быть доступной и раскрытой неавторизованным индивидуумом, логическим объектом или процессом.
Уязвимость	–	недостаток в компьютерной системе, использование которого приводит к нарушению целостности системы и некорректной работе.
Фишинг	–	сетевое мошенничество.
Целостность	–	свойство сохранения правильности и полноты активов.
DDoS	–	Distributed Denial of Service (атака типа «распределенный отказ в обслуживании»)
ВПО	–	Вредоносное программное обеспечение
ИР	–	Информационный ресурс

ИС	–	Информационная система
ИТ	–	Информационные технологии
КБ	–	Кибербезопасность
ОС	–	Операционная система
ПО	–	Программное обеспечение
ЦКЗ	–	Центр киберзащиты Исполнителя

2. ПРЕДМЕТ СОГЛАШЕНИЯ

2.1. В соответствии с Соглашением Заказчик обязуется безоговорочно соблюдать требования по кибербезопасности, применять защитные меры и проводить мероприятия, перечисленные в разделах 3 и 4 Соглашения.

2.2. Стороны признают, что обязательство Заказчика по исполнению требований по кибербезопасности, применению защитных мер, проведению мероприятий и иных условий, установленных Соглашением, является обстоятельством, имеющим существенное значение для Общества для заключения, исполнения и прекращения Договора (в порядке, предусмотренном ст. 431.2 Гражданского кодекса РФ).

3. ТРЕБОВАНИЯ ПО КИБЕРБЕЗОПАСНОСТИ

3.1. Заказчик обязуется предпринимать адекватные организационные меры и использует современные технические (аппаратные и программные) средства для обеспечения кибербезопасности и защиты от актуальных угроз.

3.2. Доступ Заказчика к Услугам Исполнителя должен предоставляться только зарегистрированным пользователям и только после успешного прохождения процедур идентификации, аутентификации и авторизации

3.3. Для доступа к Услугам Исполнителя должны использоваться только персонифицированные учетные записи.

3.4. В процессе эксплуатации Заказчик при назначении прав доступа должен использоваться принцип минимальных привилегий.

3.5. Для аутентификации в зависимости от выбранного метода проверки подлинности пользователя (пароль, токен, сертификат и т.д.) должны использоваться надёжные параметры. В частности, при использовании аутентификации с помощью пароля настройки парольной политики должны удовлетворять следующим критериям:

3.5.1. Требования к паролям персональных учетных записей:

- пароли каждой персональной учетной записи должны быть уникальны;
- длина пароля должна быть не менее 12 символов;
- пароль должен содержать в себе символы как минимум трех категорий из четырех:
  - буквы нижнего регистра (от a до z);
  - буквы верхнего регистра (от A до Z);
  - цифры (от 0 до 9);
  - спецсимволы (например: $, #, %);
- в случае разглашения или компрометации пароль должен быть незамедлительно изменен;
- запрещается включать в пароль осмысленные слова, словосочетания, общепринятые аббревиатуры, а также легко идентифицируемую с его владельцем информацию:
  - имена;
  - фамилии;
  - названия учетных записей;
  - номера телефонов;
  - клички животных;
  - наименования организаций и тому подобное;
- пароль не должен совпадать с паролями, использованными ранее (глубина проверки – 10).

3.5.2. Требования к паролям привилегированных учетных записей:

- пароли каждой привилегированной учетной записи должны быть уникальны.
- длина пароля должна составлять не менее 16 символов;
- в пароле должны присутствовать символы всех возможных категорий из числа следующих:
  - прописные буквы английского алфавита (от A до Z);
  - строчные буквы английского алфавита от (a до z);
  - десятичные цифры (от 0 до 9);
  - неалфавитные символы (например: $, #, %).

- пароль не должен содержать имя привилегированной учетной записи или какую-либо его часть.
- пароль не должен совпадать с паролями, использованными ранее (глубина проверки – 10);
- при компрометации или подозрении на компрометацию привилегированной учетной записи, пароль должен быть немедленно изменён.

3.5.3. Требования к паролям технических учетных записей:
- пароль не должен содержать имя учетной записи или его часть;
- пароль должен состоять не менее чем из 16 символов;
- в пароле должны присутствовать символы групп:
  - прописные буквы английского алфавита (от A до Z);
  - строчные буквы английского алфавита (от a до z);
  - десятичные цифры (от 0 до 9);
  - неалфавитные символы (например: $, #, %);
- пароль не должен совпадать с использованными ранее (глубина проверки – 20);
- пароль не должен содержать имя технической учетной записи или какую-либо его часть.

3.6. Учетные записи уволенных работников должны быть деактивированы (заблокированы, удалены и пр.).

3.7. Имена учетных записей пользователей должны обеспечивать возможность однозначной идентификации пользователя

3.8. Аутентификационная информация (например, пароли) должна передаваться Заказчику по защищенным каналам связи. Запрещена передача аутентификационной информации в открытом виде.

3.9. Предпочтительным способом аутентификации является двухфакторная аутентификация. Данный способ аутентификации должен применяться везде, где это возможно.

3.10. Управление доступом внутри тенанта Заказчика является зоной ответственности Заказчика. Исполнитель отвечает за регистрацию и аннулирование регистрации учетных записей Заказчика или администраторов Заказчика, а также за обеспечение защиты персональных данных администраторов и ответственных лиц Заказчика.

3.11. В целях предотвращения недопустимых событий Заказчику рекомендуется на постоянной основе, не реже одного раза в квартал, проводить внешние/внутренние аудиты кибербезопасности. К проведению аудита могут быть допущены компании, обладающие правом проведения аудитов на законном основании.

3.12. Для защиты сервисов и служб Заказчика, опубликованных в сеть Интернет, рекомендуется не реже одного раза в квартал, проводить сканирование защищенности внешнего периметра. Для проведения данного сканирования Заказчик может привлекать внешние организации, обладающие правом проведения таких работ на законном основании (наличие у такой организации лицензии ФСТЭК на деятельность по технической защите конфиденциальной информации).

3.13. Заказчику рекомендуется в максимально короткие сроки устранить выявленные на внешнем периметре уязвимости.

3.14. Заказчик предупрежден и полностью осознает, что использование предоставленных Услуг в противоправной деятельности (заражения ВПО, атаки с арендуемой инфраструктуры, вредоносное воздействие на других клиентов и т.д.) может повлечь административную, гражданско-правовую и уголовную ответственность. В случае выявления подобной деятельности Исполнитель вправе незамедлительно и без предварительного уведомления приостановить или полностью прекратить оказание Услуг Заказчику в одностороннем порядке. При этом Исполнитель не несет перед Заказчиком какой-либо ответственности в случае наступления неблагоприятных последствий в связи с приостановлением или прекращением оказания Услуг.

3.15. Заказчик обеспечивает выполнение условий для проведения расследований Инцидентов кибербезопасности. Таким условием, в частности, является выполняющийся аудит событий, прямо или косвенно влияющих на КБ, при этом журналы аудита должны храниться с условием соблюдения их доступности, целостности и конфиденциальности.

3.16. Заказчик обязан передавать Исполнителю всю необходимую информацию для выполнения им своих обязательств перед уполномоченными органами исполнительной власти, осуществляющими надзор и контроль в области защиты информации.

3.17. Заказчик самостоятельно несет ответственность за все Недопустимые события, которые могут наступить в случае невыполнения указанных в настоящем разделе Соглашения рекомендаций.

4. ОБМЕН ИНФОРМАЦИЕЙ ОБ ИНЦИДЕНТАХ КИБЕРБЕЗОПАСНОСТИ

4.1. При возникновении в инфраструктуре Заказчика значимого Инцидента кибербезопасности, последствия которого могут затронуть интересы клиентов или партнеров Исполнителя, Заказчик обязан известить об этом Исполнителя в максимально возможный короткий срок, но не позднее 3 (Трех) часов с момента обнаружения такого инцидента (подозрения на инцидент).

4.2. Для целей Соглашения значимым считается Инцидент кибербезопасности, удовлетворяющий одному из следующих критериев:
- невозможность выполнения бизнес-операций в соответствии с установленными для Исполнителя сроками или ограничение функциональности Услуг или ИС;
- разглашение аутентификационных данных или конфиденциальной информации (коммерческая тайна, персональные данные);
- воздействие ВПО, массовые блокировки учетных записей, создание несанкционированных учетных записей;
- выявлены признаки НСД или неудачных попыток получения НСД, а также злоупотребление привилегиями.

4.3. В перечень инцидентов Стороны включают, не ограничиваясь, следующие типы:
- фишинговая атака, якобы от имени Стороны;
- выявленная уязвимость на ресурсе, принадлежащем Стороне;
- выявленная уязвимость в ПО, предоставляемом/эксплуатируемом Стороной;
- заражение ВПО;
- попытки НСД к ресурсам Стороны;
- DDoS-атака на ресурсы Стороны – выявленная, закончившаяся или планируемая.

4.4. В целях оперативного взаимодействия Стороны назначают сотрудников, ответственных за обмен информацией о значимых Инцидентах (подозрениях на инциденты) кибербезопасности. Контактные данные сотрудников указываются в Приложении № 4 к Договору.

4.5. В случае устранения значимого Инцидента кибербезопасности Заказчик обязан уведомить Исполнителя о мерах, предпринятых для управления таким инцидентом, в течение 24 (Двадцати четырех) часов.

4.6. Стороны обмениваются информацией об инцидентах в свободном формате. Для повышения оперативности при передаче технической информации Стороны вправе использовать Электронную связь.

4.7. В рамках обмена информацией об Инцидентах кибербезопасности Стороны не обмениваются информацией, содержащей банковскую и государственную тайну, тайну связи и иную информацию ограниченного доступа.

4.8. В случае появления новых типов Инцидентов кибербезопасности, способов и механизмов их выявления, а также при необходимости оптимизации взаимодействия или изменения форматов передаваемых файлов в Соглашение, по взаимному согласованию Сторон, вносятся необходимые изменения (дополнения).

5. ОТВЕТСТВЕННОСТЬ СТОРОН

5.1. Стороны обязуются, в случае нарушения принятых на себя обязательств по Соглашению о соблюдении требований кибербезопасности возместить убытки, причиненные таким нарушением.

6. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

6.1. Исполнитель вправе в одностороннем порядке пересмотреть условия Соглашения по своей инициативе в следующих случаях:
- наличие у Исполнителя необходимости сохранить надлежащий уровень контроля и управления в отношении риска нарушения КБ Заказчиком;
- наличие у Исполнителя необходимости принять соответствующие меры для выполнения своих обязательств перед клиентами и контрагентами, а также перед уполномоченными органами исполнительной власти.