Требования кибербезопасности для Заказчиков-физических лиц

(далее – Требования)

Для целей настоящего документа принимаются следующие обозначения:

Исполнитель	–	Общество с ограниченной ответственностью «Облачные технологии» ИНН: 7736279160, ОГРН: 5167746080057
Заказчик	–	физическое лицо, акцептовавшее условия оферты на оказание Услуг Исполнителя (далее – «Договор»), 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. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данные Требования разработаны с учётом положений следующих документов:
- Политика кибербезопасности ООО «Облачные технологии»;
- Политика конфиденциальности ООО «Облачные технологии»;
- Политика обработки персональных данных ООО «Облачные технологии».

1.2. Использование Услуг должно осуществляться Заказчиком только для законных целей и законными способами.

1.3. Исполнитель не осуществляет предварительного контроля размещаемой и (или) распространяемой Заказчиком информации и (или) осуществляемых им действий при использовании Услуги.

1.4. Заказчик несёт полную ответственность за содержание размещённой на виртуальных ресурсах Исполнителя информации.

2. МЕРЫ ПО КОНТРОЛЮ И ПРЕСЕЧЕНИЮ НАРУШЕНИЙ

2.1. Источниками информации о признаках нарушений со стороны Заказчика являются объективные данные системы обеспечения информационной безопасности Исполнителя (СУИБ), публикации в СМИ, а также поступающие по официальным каналам связи Исполнителя жалобы на действия Заказчика.

2.2. При поступлении по официальным каналам связи Исполнителя жалобы на действия Заказчика Исполнитель проводит разбирательство в соответствии с внутренними требованиями.

2.3. В процессе разбирательства Исполнитель вправе:
- запросить у Заказчика информацию о характере его действий, имеющих признаки нарушений;
- запросить у Заказчика данные, подтверждающие его личность, если они ранее не были предоставлены в момент регистрации или в ходе оказания Услуг;
- вынести Заказчику предупреждение о возможной приостановке Услуг;
- приостановить оказание Услуг;
- прекратить предоставление Заказчику виртуальных ресурсов с удалением данных Заказчика, хранящихся на оборудовании Исполнителя.

2.4. К нарушениям требований кибербезопасности приравниваются[1]:

2.4.1. Осуществление любых действий, направленных на:
- сканирование сетей;
- обнаружение уязвимостей в безопасности программного обеспечения;
- подбор пароля и иных идентифицирующих данных;
- поиск открытых портов и незащищённых ресурсов;
- блокировку учётных записей;
- создание несанкционированных учётных записей от имени третьих лиц при отсутствии от них явно выраженного согласия.

2.4.2. Использование предоставленных Исполнителем ресурсов для запуска программного обеспечения, работа которого может привести к нарушению работоспособности программно-аппаратного комплекса и ресурсов Исполнителя и (или) третьих лиц.

2.4.3. Использование предоставленных Исполнителем ресурсов для запуска программного обеспечения с целью получения несанкционированного доступа к информации третьих лиц, вне зависимости от умысла Заказчика, в том числе в случае утраты Заказчиком контроля при пользовании Услугой.

[1] Перечень содержит некоторые характерные примеры нарушений и не является исчерпывающим.

2.4.4. Осуществление действий, создающих излишнюю (паразитную) нагрузку на ресурсы Исполнителя и (или) третьих лиц, а также действий, направленных на вывод из строя или нарушение функционирования программного обеспечения и (или) оборудования, обслуживающего такие ресурсы.

2.4.5. Множественная регистрация личных кабинетов и генерация ресурсов в них без продолжения эксплуатации после достижения нулевого или отрицательного баланса, в том числе с использованием потенциально вымышленных имён, фамилий, иных установочных данных и их сочетаний, которые невозможно подтвердить по запросу Исполнителя.

2.4.6. Размещение и распространение информации оскорбительного, нецензурного, порнографического характера, призывов к насилию, призывов к осуществлению экстремистской деятельности, а также использование средств коммуникации для отправки сообщений указанного характера.

2.4.7. Отправка фишинговых сообщений.

2.4.8. Передача, воспроизведение или распространение без разрешения владельца любым способом любых материалов, полностью или частично защищённых авторскими или другими правами.

2.4.9. Размещение, распространение, применение вредоносного программного обеспечения, которое может нарушить работоспособность ресурсов Исполнителя и (или) третьих лиц, привести к порче данных, включая их шифрование.

2.4.10. Размещение на ресурсах Исполнителя информации, прямо или косвенно направленной на извлечение прибыли и (или) получение иных благ путём обмана, мошенничества, вымогательства или с помощью иных незаконных способов.

2.4.11. Реклама и продажа услуг, товаров и иных материалов, оборот которых ограничен или запрещён действующим законодательством, в обход указанных ограничений или запретов.

2.4.12. Размещение и распространение информации о третьих лицах, прямо или косвенно порочащей их честь, достоинство и деловую репутацию.

2.4.13. Размещение и распространение информации, нарушающей требования законодательства в сфере защиты персональных данных.

2.5. Для аутентификации в зависимости от выбранного метода проверки подлинности пользователя (пароль, токен, сертификат и т.д.) должны использоваться надёжные параметры. В частности, настройки парольной политики должны удовлетворять следующим условиям:

2.5.1. Требования к паролям персональных учетных записей:

- пароль каждой персональной учетной записи должен быть уникальным и не должен содержать имя учетной записи или его часть;
- длина пароля должна быть не менее 14 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, в частности:
  - имена, фамилии;
  - даты рождения;
  - наименования учётных записей;
  - номера телефонов;
  - клички и прозвища;
  - наименования организаций и тому подобное;
- пароль не должен совпадать с паролями, использованными ранее (глубина проверки – 10);
- смена пароля должна производиться не реже 1 раза в 90 дней;
- рекомендуется применять второй фактор аутентификации (2FA) для подтверждения входа.

2.5.2. Дополнительные требования к паролям привилегированных учетных записей по сравнению с паролями к персональным учётным записям:

- длина пароля должна составлять не менее 18 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: $, #, %);

2.6. Дополнительные требования к паролям технических учетных записей по сравнению с паролями к привилегированным учётным записям:

- пароль должен состоять не менее чем из 24 символов;
- в пароле должны присутствовать комбинации символов:
  - 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);
- рекомендуется производить смену пароля для технической учётной записи не реже чем 1 раз в 360 дней (раз в год).

3. ОТВЕТСТВЕННОСТЬ СТОРОН

3.1. Заказчик обязуется в случае нарушения принятых на себя обязательств по Соглашению о соблюдении требований кибербезопасности возместить убытки, причиненные таким нарушением.