ПРАВИЛА ПОЛЬЗОВАНИЯ СЕТЬЮ

Настоящие Правила Пользования Сетью (далее — ППС) являются обязательными для всех пользователей услугами Оператора.

Контроль за содержанием передаваемой по сети Оператора информации не входит в компетенцию Оператора, и он не несет ответственность за действия третьих лиц, направленные на незаконное либо некорректное использование сети Оператора.

Тем не менее, Заказчик обязан соблюдать условия ППС и отвечает за то, чтобы его конечные пользователи и(или) клиенты не нарушали условия ППС. Нарушение ППС может повлечь приостановление оказания Услуг и(или) расторжение Договора в порядке, установленном Договором и законодательством РФ.

Несмотря на то, что Оператор обеспечивает ограничение и возобновление доступа к информации, распространяемой посредством сети "Интернет", в порядке, установленном Федеральным законом от 27.07.2006 № 149-ФЗ (фильтрацию трафика), а также обеспечивает установку и функционирование технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории РФ сети "Интернет" и сети связи общего пользования, операторы связи, чьи сети присоединены к сетям Оператора, самостоятельно несут ответственность перед надзорными органами за исполнение требований п. 5-5.1 ст. 46 Федерального закона от 07.07.2003 № 126-ФЗ.

Законодательством РФ не предусмотрено освобождение оператора связи от установки в принадлежащей ему сети связи технических средств, предусмотренных п. 5-5.1 ст. 46 Федерального закона от 07.07.2003 № 126-ФЗ, в случае, когда сеть такого оператора присоединена к сети иного оператора, в которой соответствующие технические средства контроля установлены.

Оператор оставляет за собой право в любое время вносить изменения в ППС. Изменения вступают в силу с момента их публикации на сайте Оператора.

В сети Оператора запрещены:

1. Любая деятельность, которая считается незаконной на территории, на которой заказчику предоставляются услуги.
2. Хранение или передача материала, который нарушает авторское право или право на торговый знак.
3. Хранение или передача детской порнографии.
4. Использование услуг в мошеннических целях, для хищения персональных данных или иной вредоносной или мошеннической деятельности, включая предложение или распространение мошеннических товаров, услуг, схем, продвижений.
5. Использование услуг для распространения, контроля или иного взаимодействия с вредоносными компьютерными программами (вирусами, троянскими программами, «червями», шпионскими программами и иными хакерскими программами).
6. Пиратство программного обеспечения или иное медийное пиратство.
7. Нарушение местного импортно-экспортного законодательства.
8. Притеснение человека или организации, будь то посредством прямой угрозы, словесного запугивания или простого отказа прекратить указанные действия.
9. Тестирование на проникновение / уязвимость или несанкционированный доступ к сети Оператора и какой-либо операционной или административной системе Оператора.
10. Тестирование на несанкционированное проникновение / уязвимость или доступ к сети или системам любой иной компании.

АО «РетнНет»

Адрес: 115280, г. Москва, ул. Ленинская Слобода, д. 26, стр. 2
T: + 7 495 663 16 40
W: www.retn.net

ОГРН 1057747699261
ИНН 7725545445
Входит в группу компаний RETN Capital Ltd.
RETN Capital Ltd. сертифицировано по ISO 27001:2013

11. Электронные выдачу себя за другого человека или организацию, или другие обманные приемы.
12. Рассылка спама; нежелательная электронная рассылка; нежелательная реклама; сообщения, предназначенные для дестабилизации других услуг; сообщения содержащие вредоносный контент.
13. Фарминг (скрытное перенаправление жертвы на ложный IP-адрес) адресов электронной почты или иных индивидуальных онлайновых идентификаторов.
14. Фишинг (получение обманным путём доступа к конфиденциальным данным пользователей, в т.ч. логинам, паролям, платёжной информации и т.п.).
15. Несанкционированный перехват сообщений или иных данных.
16. Операционные сетевые услуги, как, например, открытые прокси-серверы, открытые почтовые трансляторы или открытые рекурсивные серверы доменных имён.
17. Общее вмешательство в сеть Оператора или её системы мониторинга.
18. Действия, которые нарушают правила пользования сетью поставщиков Оператора.
19. Действия, которые превращают сеть Оператора в цель DDoS-атак или прочих нацеленных атак.
20. Любые действия, ведущие к тому, что IP пространство Оператора заносится в черный список базами данных по злоумышленному использованию (Spamhaus и т.д.).
21. Действия, которые приводят или могут привести к прерыванию функционирования сети Оператора компетентными государственными органами.
22. Любые действия, которые приводят к прерыванию предоставления услуг другим клиентам Оператора.

Лица, нарушающие ППС, могут быть привлечены к гражданской, административной или уголовной ответственности в соответствии с действующим законодательством Российской Федерации. Оператор проводит проверку по такого рода нарушениям и оказывает содействие правоохранительным органам в их пресечении.