

ТОВ «ЮАСІТІ»

ПОЛІТИКА УПРАВЛІННЯ МЕРЕЖЕЮ

1. Призначення документа

1.1. Ця Політика описує загальні підходи Провайдера до управління мережею, трафіком, безпекою, аварійними подіями, технічним обслуговуванням і забезпеченням стабільності послуг.

1.2. Політика має інформаційний і договірний характер та застосовується разом із рамковим договором, Умовами надання послуг, AUP, SLA і законодавством України.

2. Загальні принципи

- Підтримання стабільної роботи мережі та належної якості послуг у межах погоджених технічних параметрів.
- Попередження, виявлення та локалізація аварій, перевантажень, шкідливої активності та несанкціонованого доступу.
- Використання розумних технічних заходів для захисту мережі, клієнтів і третіх осіб від атак, заражень та зловживань.
- Мінімізація впливу планових і аварійних робіт на користувачів.

3. Управління трафіком і безпекою

3.1. Провайдер може застосовувати фільтрацію, blackhole/null-route, rate limit, ACL, геофільтри, анти-DDoS заходи, ізоляцію заражених сегментів, тимчасове блокування портів або протоколів, якщо це об'єктивно необхідно для безпеки мережі, виконання AUP, захисту інших клієнтів або виконання вимог закону.

3.2. Такі дії, якщо вони вживаються добросовісно та пропорційно до ризику, не вважаються порушенням договору, якщо Провайдер діє з метою запобігання більшій шкоді або відновлення стабільності сервісу.

4. Планові та аварійні роботи

4.1. Планові роботи, модернізації, оновлення ПЗ, переналаштування мережі та переключення резервів за можливості виконуються у вікнах з мінімальним впливом на клієнтів.

4.2. Якщо це практично можливо, Провайдер повідомляє клієнтів про планові роботи завчасно через e-mail, особистий кабінет або інші погоджені канали.

4.3. У разі аварійних подій, ризику безпеці мережі або загрози більш тривалій перерви Провайдер може виконувати роботи без стандартного строку попередження.

5. Межі прозорості

5.1. Провайдер не зобов'язаний публічно розкривати детальні схеми мережі, конфігурації захисту, внутрішні адресації, параметри анти-DDoS або іншу чутливу інформацію, якщо її розкриття може зашкодити безпеці мережі.

5.2. За запитом бізнес-клієнта Провайдер може надати загальну інформацію про інцидент, planned maintenance або обмеження, якщо це не суперечить вимогам безпеки, конфіденційності та законодавству.