Политика реагирования на нарушения (далее — Политика)

Дата публикации 24.08.2026

Дата вступления в силу настоящего Документа 24.08.2026

Провайдер: EZ Infrastructure Limited (Company Registration Number 80559003)

Настоящая Политика является приложением к Публичной оферте Провайдера и применяется совместно с ней.

Обращения о нарушениях направляются на abuse@aeza.net, претензии в досудебном порядке — на legal@aeza.net.

1. Общие положения

1.1. Настоящая Политика определяет порядок выявления, фиксации, рассмотрения, приостановления, удаления, блокирования и документирования нарушений, совершаемых с использованием услуг хостинг-провайдера EZ Infrastructure Limited.

1.2. Политика применяется ко всем клиентам, пользователям и иным лицам, использующим инфраструктуру Провайдера, включая услуги хостинга, размещения файлов, виртуальных серверов, резервного копирования, DNS, электронной почты и иных сопутствующих сервисов.

1.3. Политика разработана с учетом законодательства САР Гонконг, включая Personal Data (Privacy) Ordinance, Copyright Ordinance, Protection of Critical Infrastructures (Computer Systems) Ordinance, а также иные применимые нормы уголовного, административного и процессуального права.

1.4. В случае противоречия между настоящей Политикой и обязательными нормами права САР Гонконг применяются нормы права.

2. Перечень нарушений

2.1. Нарушения авторских прав.

2.1.1. Размещение, хранение, распространение или предоставление доступа к материалам, нарушающим авторские права, права на смежные объекты и иные охраняемые права.

2.1.2. Размещение пиратского программного обеспечения, ключей активации, кряков, патчей обхода защиты, а также иного контента, предназначенного для обхода технических средств защиты.

2.1.3. Использование инфраструктуры Провайдера для организации массового распространения нелицензионного контента.

2.2. Нарушения в сфере персональных данных и приватности.

2.2.1. Незаконный сбор, использование, хранение, передача или раскрытие персональных данных.

2.2.2. Доксинг, включая публикацию адресов, телефонов, идентификаторов, сведений о месте работы, банковских реквизитов, паспортных и иных идентифицирующих данных с целью причинения вреда, преследования или давления.

2.2.3. Размещение или распространение баз данных, полученных в результате несанкционированного доступа, утечки либо иной незаконной обработки.

2.2.4. Массовый парсинг персональных данных, если он осуществляется без надлежащего правового основания и нарушает требования PDPO.

2.3. Киберпреступления и вредоносная деятельность.

2.3.1. Несанкционированный доступ к компьютерным системам, аккаунтам, базам данных и сетевой инфраструктуре.

2.3.2. Разработка, размещение, хранение, распространение или администрирование вредоносного программного обеспечения, включая вирусы, трояны, шпионские программы, программы-вымогатели и ботнеты.

2.3.3. Проведение или содействие атакам типа отказ в обслуживании, включая распределенные атаки.

2.3.4. Фишинг, кража учетных данных, создание поддельных страниц банков, платежных систем, государственных органов и иных доверенных сервисов.

2.3.5. Эксплуатация уязвимостей в противоправных целях, включая продажу, передачу или использование эксплойтов для совершения преступлений.

2.3.6. Разработка, размещение, хранение, распространение, продажа, реклама или иное предоставление доступа к читам, чит-программам, скриптам автоматизации, ботам, а также иному программному обеспечению или сервисам, предназначенным для получения несправедливого преимущества в компьютерных играх, обхода или отключения античит-систем и иных технических средств защиты игрового программного обеспечения, а равно для несанкционированного вмешательства в работу серверов и клиентского программного обеспечения третьих лиц.

2.4. Мошенничество и финансовые злоупотребления.

2.4.1. Создание, размещение или поддержка ресурсов, предназначенных для мошенничества, фиктивных инвестиций, обмана потребителей или неправомерного получения денежных средств.

2.4.2. Использование услуг Провайдера в схемах по отмыванию денег, финансированию преступной деятельности или иным финансовым злоупотреблениям.

2.4.3. Распространение поддельных документов, удостоверений личности, банковских карт, лицензий и иных подложных материалов.

2.5. Незаконный и опасный контент.

2.5.1. Материалы, связанные с сексуальной эксплуатацией несовершеннолетних, подлежат немедленному удалению и передаче компетентным органам.

2.5.2. Контент, содержащий призывы к насилию, терроризму, экстремизму, расовой, религиозной или иной ненависти.

2.5.3. Материалы, содержащие инструкции по изготовлению оружия, взрывчатых веществ, наркотических средств или иных предметов и веществ, оборот которых ограничен или запрещен.

2.5.4. Материалы, нарушающие судебные запреты, запреты на распространение информации либо иные обязательные судебные акты САР Гонконг.

2.6. Спам и злоупотребление электронными коммуникациями.

2.6.1. Массовая рассылка сообщений без надлежащего согласия получателей, если такая рассылка нарушает применимые нормы права.

2.6.2. Использование инфраструктуры Провайдера как открытого ретранслятора, а также отправка сообщений с поддельными идентификаторами отправителя.

2.7. Нарушения сетевой безопасности и злоупотребление ресурсами.

2.7.1. Сканирование сетей и систем с целью несанкционированного выявления уязвимостей.

2.7.2. Подделка сетевых идентификаторов, сокрытие источника трафика и иные действия, затрудняющие установление лица, совершившего нарушение.

2.7.3. Чрезмерное потребление ресурсов, создающее угрозу отказа в обслуживании для других клиентов.

3. Порядок реагирования

3.1. Провайдер принимает сообщения о нарушениях от правообладателей, их представителей, субъектов данных, пострадавших лиц и компетентных органов.

3.2. Сообщение должно содержать достаточные сведения для идентификации предполагаемого нарушения, включая адрес размещения материала, описание нарушения, сведения о заявителе и контактные данные для связи.

3.3. Если сообщение не позволяет установить характер нарушения либо не содержит достаточной идентификации материала, Провайдер вправе запросить уточнение либо оставить сообщение без исполнения до предоставления необходимых сведений.

3.4. Провайдер вправе приостановить доступ к материалу, ограничить функциональность услуги либо удалить материал, если имеются разумные основания полагать, что продолжение размещения создает риск нарушения закона, прав третьих лиц либо обязательств Провайдера.

3.5. В случаях, связанных с тяжкими нарушениями, очевидной противоправностью, риском причинения существенного вреда, сексуальной эксплуатацией несовершеннолетних или активной вредоносной атакой, Провайдер вправе применять немедленные меры без предварительного уведомления пользователя.

4. Процедура по авторским правам

4.1. Сообщение о нарушении авторских прав рассматривается в соответствии с Copyright Ordinance и действующим Code of Practice.

4.2. Уведомление должно позволять идентифицировать правообладателя, защищаемое произведение, нарушающий материал и основание требования о прекращении доступа.

4.3. После получения надлежащего уведомления Провайдер удаляет материал или блокирует доступ к нему в кратчайший технически возможный срок.

4.4. Пользователь, в отношении которого применены меры, вправе представить возражение или иные доказательства законности использования материала.

4.5. Если предусмотренная законом процедура встречного уведомления применима, Провайдер действует в соответствии с ней и восстанавливает доступ только при соблюдении соответствующих условий.

4.6. Все уведомления, переписка, доказательства и сведения о принятых мерах подлежат хранению в течение срока, необходимого для целей рассмотрения соответствующего обращения, исполнения настоящей Политики, осуществления внутреннего контроля, а также защиты прав и законных интересов Провайдера, но не менее срока, разумно необходимого для урегулирования соответствующего инцидента, и в любом случае не дольше, чем это допускается применимым законодательством САР Гонконг.

5. Нарушения в сфере персональных данных

5.1. Провайдер принимает все практически осуществимые меры для защиты персональных данных от несанкционированного доступа, обработки, утраты, уничтожения или использования, в соответствии с Data Protection Principle 4 по PDPO.

5.2. При выявлении инцидента, связанного с персональными данными, проводится немедленная оценка масштаба, характера данных, категории затронутых лиц и вероятного вреда.

5.3. Уведомление Уполномоченного по защите персональных данных и затронутых лиц осуществляется в порядке, рекомендованном PCPD, если обстоятельства указывают на риск реального вреда либо иное значимое негативное последствие.

5.4. При доксинге Провайдер вправе немедленно ограничить доступ к материалу, зафиксировать доказательства и, при необходимости, уведомить компетентные органы.

6. Сохранение данных и взаимодействие с органами власти

6.1. Раскрытие данных третьим лицам допускается только при наличии законного основания, включая судебный акт, обязательный запрос компетентного органа или иное основание, прямо предусмотренное законом.

6.2. По законному запросу компетентных органов Провайдер обеспечивает сохранение логов, метаданных и иных данных, необходимых для расследования, в пределах и сроках, допустимых законом.

6.3. Если клиент или его системы подпадают под режим Protection of Critical Infrastructures (Computer Systems) Ordinance, Провайдер исполняет применимые требования по взаимодействию, уведомлению и документированию инцидентов в соответствии с этим режимом.

7. Санкции к клиенту

7.1. В зависимости от тяжести нарушения Провайдер вправе применить одно или несколько из следующих мер: предупреждение, временная приостановка услуги, удаление материала, ограничение функций, расторжение договора, отказ в дальнейшем обслуживании, передача сведений компетентным органам.

7.2. При наличии риска уголовной ответственности, существенного вреда третьим лицам или нарушения обязательных требований закона Провайдер вправе прекратить оказание услуг немедленно.

8. Документирование и аудит

8.1. Каждый инцидент фиксируется в журнале учета с указанием даты, времени, категории нарушения, принятых мер, основания принятого решения и ответственного подразделения.

8.2. Политика подлежит пересмотру не реже одного раза в год, а также при изменении законодательства или практики применения соответствующих норм.

9. Заключительные положения

9.1. Настоящая Политика вступает в силу с даты утверждения.

9.2. Провайдер обеспечивает доведение Политики до сведения клиентов путем размещения на официальном сайте.

9.3. В случае противоречия между настоящей Политикой и обязательными нормами законодательства САР Гонконг, судебными актами или законными требованиями компетентных органов применяются указанные нормы, акты и требования.