Violation Response Policy (hereinafter referred to as the Policy)

Date of publication: 27 July 2026
Effective date of this document (entry into force): from 27 July 2026
Provider: EZ Infrastructure Limited (Company Registration Number 80559003)

This Policy is an annex to the Provider's Public Offer and applies together with it. Reports of violations are sent to abuse@aeza.net; pre-trial claims are sent to legal@aeza.net.

1. General Provisions	1.1. This Policy establishes the procedure for detecting, recording, reviewing, suspending, removing, blocking, and documenting violations committed through the use of the services of hosting provider EZ Infrastructure Limited. 1.2. The Policy applies to all clients, users, and other persons using the Provider's infrastructure, including hosting services, file storage, virtual servers, backup, DNS, email, and other related services. 1.3. The Policy has been developed taking into account the legislation of the Hong Kong SAR, including the Personal Data (Privacy) Ordinance, the Copyright Ordinance, the Protection of Critical Infrastructures (Computer Systems) Ordinance, as well as other applicable provisions of criminal, administrative, and procedural law. 1.4. In the event of a conflict between this Policy and mandatory provisions of the law of the Hong Kong SAR, the provisions of law shall prevail.
2. List of Violations	**2.1. Copyright infringement.** 2.1.1. Hosting, storing, distributing, or providing access to materials that infringe copyright, rights in related subject matter, and other protected rights. 2.1.2. Hosting pirated software, activation keys, cracks, protection-bypass patches, as well as other content intended to circumvent technological protection measures. 2.1.3. Use of the Provider's infrastructure to organize the mass distribution of unlicensed content. **2.2. Violations in the area of personal data and privacy.** 2.2.1. Unlawful collection, use, storage, transfer, or disclosure of personal data. 2.2.2. Doxxing, including the publication of addresses, telephone numbers, identifiers, information about the place of work, bank details, passport data, and other identifying data for the purpose of causing harm, harassment, or pressure. 2.2.3. Hosting or distribution of databases obtained as a result of unauthorized access, a data breach, or other unlawful processing. 2.2.4. Mass scraping of personal data, where carried out without a proper legal basis and in breach of the requirements of the PDPO. **2.3. Cybercrime and malicious activity.** 2.3.1. Unauthorized access to computer systems, accounts, databases, and network infrastructure. 2.3.2. Development, hosting, storage, distribution, or administration of malicious software, including viruses, trojans, spyware, ransomware, and botnets. 2.3.3. Carrying out or facilitating denial-of-service attacks, including distributed attacks. 2.3.4. Phishing, theft of credentials, and the creation of counterfeit pages of banks, payment systems, government authorities, and other trusted services. 2.3.5. Exploitation of vulnerabilities for unlawful purposes, including the sale, transfer, or use of exploits for the commission of crimes. **2.4. Fraud and financial abuse.** 2.4.1. Creation, hosting, or support of resources intended for fraud, fictitious investment schemes, deception of consumers, or the wrongful obtaining of funds.

	2.4.2. Use of the Provider's services in schemes involving money laundering, the financing of criminal activity, or other financial abuse. 2.4.3. Distribution of forged documents, identity documents, bank cards, licences, and other counterfeit materials. **2.5. Unlawful and dangerous content.** 2.5.1. Materials related to the sexual exploitation of minors are subject to immediate removal and referral to the competent authorities. 2.5.2. Content containing incitement to violence, terrorism, extremism, or racial, religious, or other hatred. 2.5.3. Materials containing instructions for the manufacture of weapons, explosives, narcotic drugs, or other items and substances the circulation of which is restricted or prohibited. 2.5.4. Materials that breach court injunctions, prohibitions on the dissemination of information, or other binding judicial acts of the Hong Kong SAR. **2.6. Spam and abuse of electronic communications.** 2.6.1. Mass distribution of messages without the proper consent of recipients, where such distribution breaches applicable provisions of law. 2.6.2. Use of the Provider's infrastructure as an open relay, as well as the sending of messages with forged sender identifiers. **2.7. Network security violations and abuse of resources.** 2.7.1. Scanning networks and systems for the purpose of unauthorized detection of vulnerabilities. 2.7.2. Spoofing of network identifiers, concealment of the source of traffic, and other actions that impede identification of the person who committed the violation. 2.7.3. Excessive consumption of resources creating a risk of denial of service to other clients.
3. Response Procedure	3.1. The Provider accepts reports of violations from rightsholders, their representatives, data subjects, affected persons, and competent authorities. 3.2. A report must contain sufficient information to identify the alleged violation, including the address at which the material is hosted, a description of the violation, information about the reporting party, and contact details for communication. 3.3. If a report does not make it possible to establish the nature of the violation or does not contain sufficient identification of the material, the Provider may request clarification or leave the report unactioned until the necessary information is provided. 3.4. The Provider may suspend access to material, restrict the functionality of a service, or remove material where there are reasonable grounds to believe that continued hosting creates a risk of a breach of law, of the rights of third parties, or of the Provider's obligations. 3.5. In cases involving serious violations, manifest unlawfulness, a risk of substantial harm, the sexual exploitation of minors, or an active malicious attack, the Provider may take immediate measures without prior notice to the user.

4. Copyright Procedure	4.1. A report of copyright infringement is reviewed in accordance with the Copyright Ordinance and the applicable Code of Practice. 4.2. A notice must make it possible to identify the rightsholder, the protected work, the infringing material, and the basis of the request to disable access. 4.3. Upon receipt of a proper notice, the Provider removes the material or blocks access to it within the shortest technically feasible time. 4.4. A user in respect of whom measures have been taken may submit an objection or other evidence of the lawfulness of the use of the material. 4.5. Where the counter-notice procedure provided for by law is applicable, the Provider acts in accordance with it and restores access only where the relevant conditions are met. 4.6. All notices, correspondence, evidence, and information about the measures taken are retained for the period necessary for the purposes of reviewing the relevant report, performing this Policy, exercising internal control, and protecting the rights and legitimate interests of the Provider, but no less than the period reasonably necessary to resolve the relevant incident, and in any event no longer than permitted by the applicable legislation of the Hong Kong SAR.
5. Personal Data Violations	5.1. The Provider takes all practicable steps to protect personal data against unauthorized access, processing, loss, erasure, or use, in accordance with Data Protection Principle 4 under the PDPO. 5.2. Upon detection of an incident involving personal data, an immediate assessment is carried out of its scale, the nature of the data, the categories of affected persons, and the likely harm. 5.3. Notification of the Privacy Commissioner for Personal Data and of affected persons is carried out in the manner recommended by the PCPD, where the circumstances indicate a risk of real harm or another significant adverse consequence. 5.4. In cases of doxxing, the Provider may immediately restrict access to the material, preserve evidence, and, where necessary, notify the competent authorities.
6. Data Retention and Interaction with Authorities	6.1. Disclosure of data to third parties is permitted only where there is a lawful basis, including a judicial act, a binding request from a competent authority, or another basis expressly provided for by law. 6.2. Upon a lawful request from competent authorities, the Provider ensures the preservation of logs, metadata, and other data necessary for an investigation, to the extent and for the periods permitted by law. 6.3. If a client or its systems fall within the regime of the Protection of Critical Infrastructures (Computer Systems) Ordinance, the Provider complies with the applicable requirements for interaction, notification, and documentation of incidents in accordance with that regime.
7. Sanctions Against the Client	7.1. Depending on the severity of the violation, the Provider may apply one or more of the following measures: a warning, temporary suspension of the service, removal of material, restriction of functions, termination of the agreement, refusal of further service, or referral of information to the competent authorities. 7.2. Where there is a risk of criminal liability, of substantial harm to third parties, or of a breach of mandatory requirements of law, the Provider may cease the provision of services immediately.

8. Documentation and Audit	8.1. Each incident is recorded in a register indicating the date, time, category of the violation, the measures taken, the basis of the decision taken, and the responsible unit. 8.2. The Policy is subject to review at least once a year, as well as upon changes in legislation or in the practice of applying the relevant provisions.
9. Final Provisions	9.1. This Policy enters into force from the date of its approval. 9.2. The Provider ensures that the Policy is brought to the attention of clients by posting it on the official website. 9.3. In the event of a conflict between this Policy and mandatory provisions of the legislation of the Hong Kong SAR, judicial acts, or lawful requirements of competent authorities, the said provisions, acts, and requirements shall prevail.