

Acceptable Use Policy

New Providence — The Bahamas — Revised August 2026

1. Introduction and Scope

1.1 Secure Shore Limited ("Secure Shore," "we," "us," or "our") is a Bahamian resident company operating a data center within a purpose-built Disaster Recovery Facility owned by Bahamas Logistic Centre LTD, a Bahamian sister company operating since 2008 (together, "Secure Shore Data Center").

1.2 Secure Shore Data Center provides services exclusively to reputable, well-regulated, and lawfully operating clients. Secure Shore Limited reserves the right to decline or terminate service to any prospective or existing client that it reasonably believes does not meet this standard.

1.3 This Acceptable Use Policy ("AUP") applies to every person or entity that accesses, uses, or causes traffic to be carried on Secure Shore's network, servers, colocation space, or any other service (each a "Client" or "you"), and to that Client's own end users, resellers, and downstream customers, for whose compliance the Client is responsible.

1.4 This AUP forms part of, and is incorporated by reference into, the Master Services Agreement, Order Form, or other contract governing your use of Secure Shore's services (the "Agreement"). In the event of a direct conflict, the Agreement's indemnification and limitation-of-liability provisions control; this AUP controls on all matters of acceptable use and compliance.

1.5 Use of any Secure Shore service constitutes acceptance of, and agreement to be bound by, this AUP in its current form. Continued use following any revision under Section 10 constitutes acceptance of the revised AUP.

2. Client Due Diligence and Know-Your-Client Requirements

2.1 Before service activation, and periodically thereafter, Secure Shore may require Clients to provide: (a) valid government-issued identification for the Client and its authorized representatives; (b) proof of business registration and beneficial ownership for corporate Clients; (c) a description of the intended use of the service; and (d) such other information as Secure Shore reasonably requires to assess regulatory, sanctions, and reputational risk.

2.2 Secure Shore reserves the right to refuse, suspend, or terminate service to any applicant or Client who declines to provide requested due-diligence information, provides false or misleading information, or is domiciled in, owned by, or controlled from a jurisdiction subject to applicable sanctions.

2.3 Clients must promptly notify Secure Shore of any material change in ownership, control, or the nature of the services or content hosted.

3. Sanctions, Export Control, and Legal Compliance

3.1 Client represents and warrants that it is not, and is not owned or controlled by, a person or entity listed on any applicable sanctions or restricted-party list (including those maintained by the UN, OFAC, or the Bahamian government), and that it will not use Secure Shore's services in a manner that would violate applicable sanctions, export control, or anti-money-laundering laws.

3.2 Client is solely responsible for determining which laws apply to its use of the service, including the laws of the Bahamas, the Client's own jurisdiction, and the jurisdictions of its end users, and for complying with all of them.

4. General Obligations and Enforcement

4.1 This AUP is provided to give Secure Shore's Clients and users a clear understanding of what Secure Shore expects of them while using the service. All users of Secure Shore's internet service, servers, and colocation services must comply with this AUP.

4.2 It is the Client's sole responsibility to ensure its own compliance, and that of its end users, with all applicable provisions of this AUP. Questions may be directed to secure@seureshore.cloud.

4.3 Secure Shore will investigate suspected or alleged breaches of this AUP and will endeavor to act reasonably. Where Secure Shore reasonably suspects a breach, illegal activity, or a threat to the security, stability, or reputation of its network, Secure Shore may, in its sole discretion and without prior notice to the Client:

- suspend, restrict, filter, or terminate any or all services;
- disconnect, quarantine, or take a forensic image of affected systems;
- remove, disable access to, or preserve specific content or data;
- refuse service or network access to any person; and
- take any other action Secure Shore deems reasonably necessary to protect its network, other clients, or third parties.

4.4 No suspension, removal, or other action taken by Secure Shore in good faith under this AUP shall give rise to any liability, refund obligation, or claim for damages by the Client, except to the extent such liability cannot be excluded under applicable Bahamian law.

4.5 Secure Shore reserves the right to run automated or manual compliance scans of Client systems (for example, scanning for open mail relays, open proxies, malware, or command-and-control traffic) at any time, with or without notice.

4.6 Secure Shore may cooperate with, and voluntarily disclose relevant account, connection, and traffic information to, law enforcement and regulatory authorities where Secure Shore reasonably believes such cooperation is necessary to comply with law, protect its rights or property, or prevent harm, without liability to the Client for such disclosure.

4.7 To report a complaint under this AUP, email secure@seureshore.cloud. Complaints regarding abusive email should include full headers; complaints regarding web content should include the specific URL; complaints regarding scanning or intrusion attempts should include the relevant log files.

5. Prohibited Content and Activity

5.1 Unlawful and High-Risk Content

5.1.1 You must not publish, store, process, transmit, or make available any material, or perform any activity, that is illegal under the laws of the Bahamas or any jurisdiction with a material connection to the content or activity (including the jurisdiction of the Client, its counterparties, or its end users).

5.1.2 Child sexual abuse material in any form is absolutely prohibited. Secure Shore will immediately terminate service without notice, preserve relevant evidence, and report to the appropriate authorities (including, where applicable, the National Center for Missing & Exploited Children or equivalent Bahamian bodies) upon detection or credible report of such material, with no obligation to notify the Client in advance.

5.1.3 Unauthorized access to any computer system is prohibited. You must be certain you are authorized before accessing any machine, network, or account.

5.1.4 You must not host, store, or transmit material that infringes any third party's intellectual property rights, or that is defamatory, and you must have all rights and permissions necessary to host any copyrighted or licensed content on your systems.

5.1.5 Pornography and other adult content of any kind must not be stored, transmitted, or otherwise associated with Client equipment co-located at Secure Shore.

5.1.6 Threatening behavior, harassment, incitement to violence, or content that promotes or facilitates terrorism, human trafficking, or the illegal sale of weapons or controlled substances is prohibited.

5.1.7 Commercial websites remain subject to applicable Bahamian distance-selling, consumer protection, and data protection laws, compliance with which is the Client's sole responsibility.

5.1.8 Impersonating any person, or forging headers, network addresses, or other identifying information, is prohibited.

5.2 Network Abuse and Security

5.2.1 You must not run scanning software against, or send data deliberately constructed to adversely affect, any remote machine or network without the explicit written permission of its owner, and you must not probe Secure Shore's own network without Secure Shore's prior written consent.

5.2.2 You must not monitor or attempt to monitor data or traffic on any network or system without the authorization of the system owner.

5.2.3 Your servers must be configured to prevent exploitation by third parties in a manner that would breach this AUP. Open proxy servers and open mail relays are expressly prohibited.

5.2.4 You must not host or distribute malicious content, including worms, viruses, ransomware, botnet command-and-control infrastructure, pre-packaged exploit code, credential-stuffing tools, or address-harvesting software.

5.2.5 You must not engage in, facilitate, or fail to promptly remediate conduct that results in a denial-of-service attack against Secure Shore's network, systems, employees, or other clients, or in retaliation of any kind against Secure Shore.

5.2.6 Unauthorized cryptocurrency mining, or any activity intended to exhaust shared disk, memory, CPU, or network capacity to the detriment of other clients, is prohibited unless expressly authorized in your service order.

5.2.7 All software connecting to other systems must conform to relevant IETF standards to minimize the risk of harm to remote systems from faulty data or protocols.

5.3 Email and Bulk Communications

5.3.1 Use of Secure Shore's service to transmit unsolicited bulk e-mail or Usenet messages is prohibited. Clients must be able to demonstrate, on request, that recipients have consented to receive email and that opt-out requests are honored.

5.3.2 Double opt-in procedures are required for any ongoing email list, and downloadable email address lists may not be stored unless every listed individual has consented to inclusion.

5.3.3 Clients may not host or send content that supports spammers or botnets, or that causes any Secure Shore IP space to be listed on a recognized spam or abuse database. Repeated listing may result in immediate suspension of the affected service.

5.4 Financial and Fraudulent Activity

5.4.1 Hosting or transmitting content that promotes financial scams (including "make money fast," Ponzi, pyramid, or advance-fee schemes), phishing infrastructure, or any other illicit financial activity is strictly prohibited.

5.4.2 Secure Shore may require documentary evidence of the legitimacy of any financial, payment-processing, or trading platform hosted on its infrastructure and may suspend service pending review.

5.5 Data Protection

5.5.1 All personal information collected or stored by a Client must be processed in accordance with the Bahamas Data Protection Act and any other applicable data protection law. Clients hosting personal data of individuals outside the Bahamas are responsible for complying with the data protection laws applicable to those individuals.

5.5.2 Clients remain the data controller for content they host and are solely responsible for maintaining lawful bases for processing, honoring data-subject rights requests, and notifying affected individuals and regulators of any breach as required by law.

6. Client Responsibility, Warranties, and Indemnification

- 6.1** You are solely responsible for your website, applications, and hosted content, and for the acts and omissions of your end users, resellers, and anyone else you permit to access the service.
- 6.2** You will be held responsible for, and accept full responsibility and liability for, any defamatory, infringing, confidential, unlawful, or otherwise objectionable material made available via your service, regardless of whether Secure Shore had actual knowledge of it.
- 6.3** You agree to indemnify, defend, and hold harmless Secure Shore Data Center, its officers, directors, employees, and agents from and against any and all claims, damages, losses, liabilities, costs, and expenses (including reasonable legal fees) arising out of or relating to: (a) your breach of this AUP; (b) content or activity hosted, transmitted, or facilitated using your service; (c) your violation of any law or third-party right; or (d) any act or omission of your end users or resellers.
- 6.4** Secure Shore reserves the right, at its own expense, to assume the exclusive defense and control of any matter otherwise subject to indemnification by you, in which event you agree to cooperate with Secure Shore's defense.

7. Disclaimers and Limitation of Liability

- 7.1** Services are provided on an “as is” and “as available” basis. To the fullest extent permitted by Bahamian law, Secure Shore disclaims all warranties, express or implied, including any warranty of merchantability, fitness for a particular purpose, or non-infringement.
- 7.2** Secure Shore shall not be liable for any loss, howsoever occasioned, arising from the suspension, removal, filtering, or unavailability of material hosted or facilitated through its service, or from any action taken in good faith under this AUP.
- 7.3** To the fullest extent permitted by law, Secure Shore's aggregate liability to the Client arising out of or related to the services, however arising, shall not exceed the total fees paid by the Client to Secure Shore in the three (3) months immediately preceding the event giving rise to the claim, and Secure Shore shall have no liability for indirect, incidental, consequential, special, punitive, or exemplary damages, or for loss of data, revenue, profits, or business opportunity.
- 7.4** Nothing in this AUP limits or excludes liability that cannot lawfully be limited or excluded, including liability for fraud or for death or personal injury caused by Secure Shore's negligence.

8. Suspension, Termination, and Effect

- 8.1** In addition to any rights under the Agreement, Secure Shore may immediately suspend or terminate service, without notice and without liability, where the Client: (a) is convicted of, charged with, or under credible investigation for an offense connected to its use of the service; (b) is found to have breached Section 5 of this AUP; (c) fails a periodic due-diligence review under Section 2; or (d) becomes subject to applicable sanctions.
- 8.2** Fees paid for services terminated for cause under this AUP are non-refundable, and any prepaid or outstanding fees for the remainder of the then-current term remain due and payable, except where prohibited by law.
- 8.3** On termination for cause, Secure Shore may retain Client data and equipment for a reasonable period as necessary to comply with legal obligations, preserve evidence, or respond to a law enforcement request, before deletion or return.

9. Special Offers

9.1 Special offers such as discounts or credits are personal to the Client and may only be used in connection with Secure Shore's own services.

9.2 Exchanging special offer benefits of any kind for cash, or transferring them to a third party, is not permitted.

10. Amendment, Severability, and Governing Law

10.1 Secure Shore Limited reserves the right to revise this AUP from time to time and apply it immediately, as it is not possible to codify in advance every instance of acceptable or unacceptable use, and community norms evolve over time. Material revisions will be posted on Secure Shore's website or communicated to Clients; continued use of the service after such notice constitutes acceptance.

10.2 As the internet is a collection of privately owned networks interconnected by consent, Secure Shore must maintain a good reputation for dealing responsibly with network abuse; a poor reputation could impair Secure Shore's ability to provide service to all of its clients, and this AUP is enforced with that shared interest in mind.

10.3 If any provision of this AUP is held unenforceable, that provision will be limited or eliminated to the minimum extent necessary, and the remaining provisions will remain in full force and effect.

10.4 This AUP is governed by the laws of the Commonwealth of the Bahamas, without regard to conflict-of-law principles, and the courts of the Bahamas shall have exclusive jurisdiction over any dispute arising from it, subject to any arbitration clause in the Agreement.