

Acceptable Use Policy

SecureThread, a product of ArcByte Studios · Version 2026-10-25

PARTICULARS	DETAILS
Document	Acceptable Use Policy for SecureThread
Version	2026-10-25, published 25 October 2026
Provider	ArcByte Studios, a sole proprietorship of Aidan Daniel Rodrigues, registered in India as a micro enterprise under the MSME Udyam scheme
Udyam registration	UDYAM-KR-03-0759003
Registered address	GoSpace, Shelter 2, The Defence Enclave, K Narayana Pura Road, Kothanur, Bengaluru, Karnataka 560077, India
Contact	hello@securethread.co · privacy@securethread.co
Governing law	The laws of India; courts at Bengaluru, Karnataka
Online version	securethread.co/legal/acceptable-use

SecureThread is provided by ArcByte Studios, a sole proprietorship of Aidan Daniel Rodrigues, registered in India as a micro enterprise under the MSME Udyam scheme (Udyam Registration No. UDYAM-KR-03-0759003), of GoSpace, Shelter 2, The Defence Enclave, K Narayana Pura Road, Kothanur, Bengaluru, Karnataka 560077, India ("ArcByte").

This policy sets out what Customers and Users may and may not do with SecureThread. It applies to every workspace, every User and every AI agent that a User connects. It forms part of the Terms of Service. A breach can lead to the measures in section 9.

SecureThread is for business email to people with whom the sender already has a relationship, or who have agreed to hear from the sender. It is not a tool for cold or unsolicited bulk email.

01 BULK AND UNSOLICITED EMAIL

1.1 You must not:

- send bulk or cold email to people who have no relationship with you and have not agreed to hear from you;
- buy, rent, trade or borrow email lists;

- take addresses from web pages, directories, social media or other sources to start contact with people who have not given them to you for that purpose;
- keep sending to an address that has unsubscribed, complained, or hard-bounced; or
- send through a mailbox, relay or sending API for a domain you do not control or have not been approved to use.

- 1.2** For a campaign to people outside your organization, you must state the basis for the campaign when you prepare it. The basis is one of: an existing relationship, opt-in consent, or a transactional role. The Service asks for the basis, and it refuses a campaign to outside recipients when the basis is "internal".
- 1.3** Campaigns to people outside the organization need three things. An administrator must allow external recipients for the workspace, which is off by default. You must state the basis above. By default, the campaign also needs an approval before it is released, unless the person who prepared it may approve sends themselves.
- 1.4** Campaigns are not available while a workspace is in the sandbox.

02 UNSUBSCRIBES AND SUPPRESSION

- 2.1** Honor every unsubscribe request promptly. The Service records unsubscribes and adds the address to the workspace's suppression list. Campaigns skip suppressed addresses.
- 2.2** Suppression always applies to campaigns. Whether it also applies to every individual message is a workspace setting, and it is off by default. Whatever the setting, you must not email an address that has asked you not to.
- 2.3** Campaign mail to people outside your organization carries a one-click unsubscribe link in its List-Unsubscribe header, with the List-Unsubscribe-Post header that RFC 8058 requires.

03 AUTHENTICATION AND THE RULES OF MAILBOX PROVIDERS

- 3.1** Authenticate every domain you send from. Publish the SPF, DKIM and DMARC records your provider gives you. The Service checks the domain's records but does not set them for you.
- 3.2** Follow the bulk-sender requirements of the mailbox providers you send to, as they stand when you send. Those requirements include authentication, one-click unsubscribe for marketing mail, and a low rate of spam complaints.
- 3.3** Act on every complaint. Stop mailing a person who complains.

04 SENDER IDENTITY

- 4.1** Do not forge, disguise or misstate the sender. The From address of a message is the address of the mailbox or domain you connected. The Service sets it that way, and you must not try to change it to another person's address.

- 4.2** Do not use misleading headers, deceptive subject lines, hidden redirects, or false claims about who is sending.
- 4.3** Do not impersonate a person, an organization or a brand, including ArcByte.

05 PROHIBITED CONTENT

- 5.1** You must not send content that:
- is phishing, or is designed to obtain passwords, codes or payment details by deception;
 - contains malware, or links or attachments that you know to be malicious;
 - is illegal, or promotes or facilitates illegal activity;
 - harasses, threatens or intimidates any person, or promotes hatred against a group;
 - infringes another person's rights, including copyright, trademarks, privacy and publicity;
 - is sexual content involving children, in any form;
 - makes a regulated offer, such as a financial promotion, for which the law of the place where it is received requires a licence, registration or approval that you do not hold.
- 5.2** Do not email government identifiers, card numbers or passwords unless your process requires it and you have a lawful basis. The Service does not detect every such item, so you must not rely on it to stop them.
- 5.3** Each workspace has a built-in list of prohibited language. An administrator can add terms to it, allow terms that should never be flagged (such as a client's surname), and choose whether mild language is blocked too. The content policy blocks messages that contain prohibited language. The rules are in section 9.

06 AI AGENTS

- 6.1** An AI agent may prepare work for you. Its policy decides whether a person must approve the work before it is sent. By default every send needs approval; an agent's owner can let it send within its own limits, up to the most the workspace's administrators allow. An assistant's own send requests go out without approval only where an administrator has switched on automatic sending, within the limits in the Terms. You are responsible for every message an agent you control sends.
- 6.2** Do not connect an AI agent to a mailbox or workspace that you do not control, and do not let an agent send mail without the human oversight you have set up.
- 6.3** Do not use AI tools to create false claims, impersonation or deceptive content.

07 LIMITS AND CONTROLS

- 7.1** Do not try to get around any of the following: sending quotas, recipient limits, rate limits, the sandbox, a sending pause, the content policy, a suspension, an approval step, or a platform-wide stop.
- 7.2** Do not share credentials between people, and do not create or use another account to avoid a suspension.

08 PROBING AND ATTACKS

- 8.1** Do not scan, probe or test the security of the Service, and do not attempt denial-of-service attacks against it. Do not try to reach another workspace's data, or data beyond what your role grants.
- 8.2** Security research on the Service is allowed only under a written agreement with ArcByte.
- 8.3** Report a suspected vulnerability privately through Help and support in SecureThread, or by email to security@securethread.co, and say that it is a security report. Do not report it in a public channel or issue.

09 HOW THE SERVICE ENFORCES THIS POLICY

9.1 What the Service does automatically today.

- **Sending pause.** The reputation check runs about every fifteen minutes. It measures each workspace's mail over the last 7 days, or since a pause was last lifted if that is more recent, and pauses sending when a threshold is crossed. The thresholds in the table below apply.
- **Content policy.** Every send is checked against the workspace's list of prohibited language. A blocked attempt is not sent and is counted as a warning; a campaign, schedule or workflow that repeats content already recorded is blocked without a new warning. After the number of warnings the administrator has set (three by default), the next blocked attempt suspends the sending User's account, except that the last active administrator is never suspended. The suspension ends the User's sessions and revokes its links and AI-assistant grants. Only an administrator can reactivate the account.
- **Sandbox.** A new workspace can send only to its own people, to verified domains and to up to ten test recipients who have confirmed they expect the mail, within daily limits, until the sandbox is lifted.
- **Limits.** Quotas, recipient caps, test-send limits and rate limits apply to every workspace.
- **Operator actions.** ArcByte can suspend a workspace, so that nobody signs in and nothing is sent. ArcByte can also stop sending across the whole platform.

9.2 Pause thresholds. These are the platform's current settings. They can change.

MEASURE	THRESHOLD	MINIMUM VOLUME IN THE LAST 7 DAYS	WHICH PROVIDERS IT MEASURES
Hard bounces	5% of recipients	40 recipients accepted for sending	Providers that report bounces back to SecureThread (HTTP email APIs with their webhook connected)
Spam complaints	0.3% of recipients	200 recipients accepted for sending	Providers that report complaints back to SecureThread
Refusals by receiving servers	5% of recipients	40 recipients submitted	Providers that report nothing after acceptance (Gmail, Microsoft 365 and SMTP)

Crossing a warning line (0.1% spam complaints or 2% hard bounces) sends a warning email, at most once a day. Sending pauses only when a pause line is crossed.

-
- 9.3** A workspace can have its own pause rates, set by ArcByte within these limits: hard bounces from 0.5% to 25%, and complaints from 0.05% to 5%.
- 9.4** Mail sent through Gmail, Microsoft 365 and SMTP servers is not reported back to SecureThread after the provider accepts it. The Service therefore cannot see complaints or later bounces for that mail. It measures only the recipients that a receiving server refuses outright.
- 9.5** **What a person decides.** A person at ArcByte reviews abuse reports, investigates complaints, considers appeals against an enforcement decision and responds to legal requests, without undue delay. Only ArcByte can lift a sending pause. An administrator of the workspace can reactivate a suspended account. To appeal a decision, write to abuse@securethread.co with the workspace name and the reasons.
- 9.6** **Ending the Terms.** ArcByte may end the Terms with immediate effect for a serious breach of this policy. For any other breach that is not put right, ArcByte gives 30 days' notice.

10 REPORTING ABUSE

- 10.1** Report spam, phishing, abuse or misuse of the Service through the abuse report form at <https://app.securethread.co/report-abuse>, or by email to abuse@securethread.co.

11 CHANGES

- 11.1** ArcByte may change this policy. Changes follow the process in section 17 of the Terms of Service.

This PDF reproduces version 2026-10-25 of the Acceptable Use Policy, as published at securethread.co/legal/acceptable-use. The online version is the authoritative one.