

# SAS ACCEPTABLE USE POLICY

---

## INTRODUCTION

This acceptable use policy (the "AUP") defines acceptable practices relating to the use of SAS's services (the "Service") by customers of SAS ("Customers") and by users that have gained access to the Service through Customer accounts ("Users"). By using the Service, you acknowledge that you and your Users are responsible for compliance with the AUP. You are responsible for violations of this AUP by any User that accesses the Services through your account.

This AUP applies to all SAS Service and as such accommodates the requirements of various SAS suppliers for SAS to pass on restrictions on the use of their services to Users. The provisions of this AUP must hence be read with reference to the Service you are taking from us. In the event of any uncertainty concerning the applicability of any particular part of this AUP to you, please ask us to clarify.

While it is not our intent to control or monitor online experience or the content of online communications, we may (or our suppliers may) edit or remove content that we deem to be in violation of the AUP or that we otherwise deem unlawful, harmful or offensive. The AUP applies to all aspects of the Service. "SAS" means The SAS Group of Companies Ltd, and all of its affiliates (including direct and indirect subsidiaries and parents). "SAS Network" includes, without limitation, constructed or leased transmission network, including all equipment, systems, facilities, services and products incorporated or used in such transmission network. As used in this AUP, "you" refers to Customers, and any reference to "Users" is intended to encompass, as applicable, both Customers and their Users.

This AUP is designed to assist in protecting the SAS Network, the Service, our Users and the Internet community as a whole from improper and/or illegal activity over the Internet, to improve Service and to improve Service offerings. In situations where data communications are carried across networks of other Internet Service Providers (ISPs), Users of the SAS Network must also conform to the applicable acceptable use policies of such other ISPs.

## RIGHTS OF SAS

SAS requires its customers to comply with SAS's instructions and all legal and regulatory requirements relevant to their system, network and any services they may provide within the countries in which they operate. Where a customer fails to meet such legal and regulatory requirements the customer agrees to indemnify SAS against all losses, expenses, costs (including legal costs) or damages which may be suffered or incurred by SAS in relation thereto. If Users engage in conduct or a pattern of conduct, including without limitation repeated violations by a User whereby correction of individual violations does not in SAS's sole discretion correct a pattern of the same or similar violations, while using the Service that violates the AUP, or is otherwise illegal or improper, SAS reserves the right to suspend and/or terminate the Service or the User's access to the Service. SAS will generally attempt to notify you of any activity in violation of the AUP and request that the User cease such activity; however, in cases where the operation of the SAS Network is threatened or cases involving unsolicited commercial email/SPAM, a pattern of violations, mail relaying, alteration of your SAS IP address information, denial of service attacks, illegal activities, suspected fraud in connection with the use of Service, harassment or copyright infringement, we reserve the right to suspend or terminate your Service or the User's access to the Service without notification. In addition, we may take any other appropriate action against you or a User for violations of the AUP, including repeated violations wherein correction of individual violations does not in SAS's sole discretion correct a pattern of the same or similar violations. SAS reserves the right to avail itself of the safe harbor provisions of the Digital Millennium Copyright Act. We do not make any promise, nor do we have any obligation, to monitor or police activity occurring using the Service and will have no liability to any party, including you, for any violation of the AUP.

## COOPERATION WITH INVESTIGATIONS

SAS will cooperate with appropriate law enforcement agencies and other parties involved in investigating claims of illegal or inappropriate activity. SAS reserves the right to disclose Customer information to the extent

authorised by applicable law authorities. As a reseller Customer of SAS's Services (if applicable), by using and accepting Services, you consent to our disclosure to any law enforcement agency, without the need for subpoena, of your identity as the service provider of record (including basic contact information), as applicable, for any User about whom SAS is contacted by the law enforcement agency.

## **MODIFICATIONS TO POLICY**

SAS reserves the right to modify this AUP at any time without notice. We will attempt to notify Customers of any such modifications either via e-mail or by posting a revised version of the AUP on our Web site. Any such modifications shall be effective and applied prospectively from the date of posting.

## **FILTERS AND SERVICE INFORMATION**

SAS reserve the right to install and use, or to have you install and use, any appropriate devices to prevent violations of this AUP, including devices designed to filter or terminate access to the Service. By accepting and using the Service, you consent to allowing us to collect service information and routing information in the normal course of our business, and to use such information for general business purposes.

## **PROHIBITED USES**

### **Illegal Activity**

SAS's Network and Services must be used in a manner that is consistent with their intended purposes and may be used only for lawful purposes. The Service shall not be used for any unlawful activities or in connection with any criminal or civil violation and the Services shall in all cases be used in compliance with applicable law. Use of the Service for transmission, distribution, retrieval, or storage of any information, data or other material in violation of any applicable law or regulation (including, where applicable, any tariff or treaty) is prohibited. This includes, without limitation, the use or transmission of any data or material protected by copyright, trademark, trade secret, patent or other intellectual property right without proper authorization and the transmission of any material that constitutes an illegal threat, violates export control laws, or is obscene, defamatory or otherwise unlawful.

### **Unauthorised Access/Interference**

A User may not attempt to gain unauthorised access to, or attempt to interfere with or compromise the normal functioning, operation or security of, any portion of the SAS Network. A User may not use the Service to engage in any activities that may interfere with the ability of others to access or use the Service or the Internet. A User may not use the Service to monitor any data, information or communications on any network or system without authorisation. A User may not attempt to gain unauthorised access to the user accounts or passwords of other Users.

### **Unsolicited Commercial Email/Spamming/Mailbombing**

A User may not use the Service to transmit unsolicited commercial e-mail messages or deliberately send excessively large attachments to one recipient. Any unsolicited commercial e-mail messages or a series of unsolicited commercial e-mail messages or large attachments sent to one recipient is prohibited. In addition, "spamming" or "mailbombing" is prohibited. Use of the service of another provider to send unsolicited commercial email, spam or mailbombs, to promote a site hosted on or connected to the SAS Network, is similarly prohibited. Likewise, a User may not use the Service to collect responses from mass unsolicited e-mail messages. Any mail server connected to the SAS Network must not be configured as an open relay. Such a server could be used for the unauthorised transmission of bulk email, should this occur the transmission would be considered to have originated from the Customer. SAS may in its sole discretion rely upon information obtained from anti-spamming organizations (including for example and without limitation spamhaus.org, spamcop.net, sorbs.net, and abuse.net) as evidence that a User is an active "spam operation" for purposes of taking remedial action under this AUP.

### **Spoofing/Fraud**

Users are prohibited from intentionally or negligently injecting false data into the Internet, for instance in the form of bad routing information (including but not limited to the announcing of networks owned by someone else or reserved by the Internet Assigned Numbers Authority) or incorrect DNS information. A User may not attempt to send e-mail messages or transmit any electronic communications using a name or address of someone other than the User for purposes of deception. Any attempt to impersonate someone else by altering a SAS IP address information or by using forged headers or other identifying information is prohibited. Any

attempt to fraudulently conceal, forge or otherwise falsify a User's identity in connection with use of the Service is prohibited. Actions considered unacceptable include, but are not limited to, network probing, network mapping, vulnerability scanning or the exploitation of vulnerabilities or misconfigurations in systems or networks, without prior authorisation with the intention of gaining unauthorised access or for any other purpose.

### **USENET Postings**

All postings to USENET groups must comply with that group's charter and other policies. Users are prohibited from cross posting to unrelated news groups or to any news groups where the post does not meet that group's charter. Continued posting of off-topic messages, including commercial messages (unless specifically invited) is prohibited. Disrupting newsgroups with materials, postings or activities that are (as determined by SAS in its sole discretion) frivolous, unlawful, obscene, threatening, abusive, libellous, hateful, excessive or repetitious is prohibited.

### **COMPLAINTS**

SAS receives complaints directly from Internet users, through Internet organisations and through other parties. SAS shall not be required to determine the validity of complaints received, or of information obtained from anti-spamming organizations, before taking action under this AUP. A complaint from the recipient of commercial email, whether received directly or through an anti-spamming organisation, shall be evidence that the message was unsolicited. SAS has no obligation to forward the complaint to the User or to identify the complaining parties.

The following activities are also prohibited:

- Intentionally transmitting files containing a computer virus or corrupted data.
- If we have specified bandwidth limitations for your user account, use of the Service shall not be in excess of those limitations.
- Attempting to circumvent or alter the processes or procedures to measure time, bandwidth utilisation, or other methods to document use of SAS's services.
- Advertising, transmitting, or otherwise making available any software, program, product, or service that is designed to violate this AUP, which includes the facilitation of the means to deliver unsolicited commercial email.
- Any activity that disrupts, degrades, harms or threatens to harm the SAS Network or the Service.
- Any use of another party's electronic mail server to relay email without express permission from such other party is prohibited.
- Networks must be configured so as not to accept external broadcast traffic
- Any other inappropriate activity or abuse of the Service (as determined by us in our sole discretion), whether or not specifically listed in this AUP, may result in suspension or termination of the User's access to or use of the Service.
- containing fraudulent offers for goods or services or any promotional materials that contain false, deceptive or misleading statements, claims or representations.
- generally, in a manner that may expose SAS or any of its personnel to criminal or civil liability.
- This listing of prohibited activities is not exhaustive and SAS reserves the right to determine that any conduct that is or could be harmful to the SAS Network, SAS's Customers or Internet users is in violation of this AUP and to exercise any or all of the remedies contained in this AUP.

### **RESPONSIBILITIES OF CUSTOMERS**

Users are entirely responsible for maintaining the confidentiality of password and account information, as well as the security of their network. You agree immediately to notify SAS of any unauthorised use of your account or any other breach of security known to you. If you become aware of any violation of this AUP by any person, including Users that have accessed the Service through your account, you are required to notify us. SAS does not make any guarantee about the security of data travelling over its networks. While SAS takes every practical step to protect such data it remains the responsibility of the communicating parties to ensure the security and integrity of their data.

SAS accepts no responsibility for the security of customer systems connected to the SAS Network. Such security remains the responsibility of the Customer. Where a Customer feels their security / privacy may have been compromised via a system connected to the SAS Network it is entirely the customer's responsibility to

seek redress from any third parties. SAS will take all lawful and practicable steps to assist in any such investigation which may be required, subject to the rights of such third parties.

SAS Customers must not engage in any activity, either lawful or unlawful, which SAS considers detrimental to its subscribers, operations, reputation, goodwill or customer relations. Customers are expected to make themselves aware of any laws relevant to the service they are providing. SAS is not responsible if a Customer fails to make themselves properly aware of laws effecting the service(s) they provide.

## **IMPENDING SECURITY EVENT NOTIFICATION**

All Users of the SAS Network are responsible for notifying SAS immediately if they become aware of an impending event that may negatively affect the SAS Network. This includes extortion threats that involve threat of "denial of service" attacks, unauthorized access, or other security events.

## **CONFIGURATION**

All Users of the SAS Network are responsible for configuring their own systems to provide the maximum possible accountability. SAS shall not be liable for any damage caused by such system configurations regardless of whether such configurations have been authorized or requested by SAS. For example, Users should ensure there are clear "path" lines in news headers so that the originator of a post may be identified. Users should also configure their Mail Transport Agents (MTA) to authenticate (by look-up on the name or similar procedures) any system that connects to perform a mail exchange, and should generally present header data as clearly possible. As another example, Users should maintain logs of dynamically assigned IP addresses. Users of the SAS Network are responsible for educating themselves and configuring their systems with at least basic security. Should systems at a User's site be violated, the User is responsible for reporting the violation and then fixing the exploited system. For instance, should a site be abused to distribute unlicensed software due to a poorly configured FTP (File Transfer Protocol) Server, the User is responsible for re-configuring the system to stop the abuse.

## **COMPLAINTS**

In most cases, we will notify our Customer(s) of complaints received by us regarding an alleged violation of this AUP. You agree to promptly investigate all such complaints and take all necessary actions to remedy any violations of this AUP. We may inform the complainant that you are investigating the complaint and may provide the complainant with the necessary information to contact you directly to resolve the complaint. You shall identify a representative for the purposes of receiving such communications

## **PRIVACY**

Because the Internet is an inherently open and insecure means of communication, any data or information a User transmits over the Internet may be susceptible to interception and alteration. We make no guarantee regarding, and assume no liability for, the security and integrity of any data or information a User transmits via the Service or over the Internet, including any data or information transmitted via any server designated as "secure."

## **ADDITIONAL TERMS AND CONDITIONS**

The use of the SAS Network by a Customer of SAS is subject to the terms and conditions of any agreements entered into by such Customer and SAS. This AUP is incorporated into such agreements by reference.

## **COMPLAINTS AND CONTACT INFORMATION**

Any complaints regarding prohibited use or other abuse of the SAS Network, including violations of this AUP, should be sent to SAS. Please include all applicable information that will assist SAS in investigating the complaint, including all applicable headers of forwarded messages. Sites experiencing live attacks from SAS Customers should call into our UK Network Operations Centre to submit a complaint as quickly as possible. Describe the urgency of the situation should you need immediate attention. If you are unsure whether any contemplated use or action is permitted, please submit questions or comments to SAS.