

VERICENTER ACCEPTABLE USE POLICY (AUP)[©]

Table of Contents

| | |
|--|----|
| Table of Contents | ii |
| 1 Purpose..... | 1 |
| 2 Policy Change Method..... | 1 |
| 3 Violations..... | 1 |
| 4 Violation Reporting Information | 1 |
| 5 Suspension and Cancellation of Service for AUP Violations..... | 1 |
| 6 Client Security Responsibility | 2 |
| 7 Reseller Policy | 3 |
| 8 Copyright Infringement Policy | 3 |
| 9 Bulk or Commercial E-Mail | 4 |
| 10 Malicious Uses and Activities | 6 |
| 11 Offensive Content | 8 |
| 12 Disclaimer | 9 |
| 13 IP Allocation and Blocking..... | 9 |
| 14 Internet Etiquette..... | 9 |
| 15 Cooperation with Investigations and Legal Proceedings..... | 9 |
| 16 Conduct on VeriCenter Premises..... | 10 |
| 17 Fraud | 10 |
| 18 AUP Copyright Information | 10 |
| Effective Date | 10 |

VERICENTER ACCEPTABLE USE POLICY (AUP)

1 Purpose

VeriCenter's Acceptable Use Policy (AUP) establishes the principles that govern the use of VeriCenter's managed and colocation services (including products and equipment) by our Customers and third parties. The AUP provides rules and guidelines to protect users of VeriCenter's services from inappropriate, abusive, and unlawful activities.

The AUP applies generally to the conduct of all of VeriCenter's managed and colocation Customers, and of their users and Customers, both online and on VeriCenter's premises. VeriCenter reserves the right to impose reasonable rules and regulations regarding the use of its services provided to all Customers. Such rules and regulations are subject to change without notice.

2 Policy Change Method

VeriCenter may revise the AUP by posting a new version on the VeriCenter Web site at <http://vericenter.com> (or any successor URL(s)). The revised policy is effective immediately upon posting. Customers are responsible for staying informed about the contents of the AUP currently in effect and for abiding by the terms of that AUP. Continued use of VeriCenter services after such changes to the AUP constitutes acceptance of any revisions to the AUP. Questions or comments about this policy should be sent to abuse@vericenter.com.

3 Violations

VeriCenter's Acceptable Use Policy is actively and strictly enforced. Violation of any part of the AUP is prohibited and may result in the termination or suspension of services. Please see the [Suspension and Cancellation of Service for AUP Violations](#) section of this document for further details.

4 Violation Reporting Information

Violations of this policy or suspected abuses beyond this policy should be reported by e-mail to abuse@vericenter.com or via postal mail to:

VeriCenter, Inc.
Security Operations
757 N. Eldridge Parkway, Suite 200
Houston, Texas 77079

5 Suspension and Cancellation of Service for AUP Violations

VeriCenter will use reasonable care in notifying Customer of AUP violations and in minimizing service interruptions. However, VeriCenter reserves the right to suspend or terminate service to any Customer for violations of this AUP *without notice*.

VERICENTER ACCEPTABLE USE POLICY (AUP)

Notification of AUP violation(s) will be issued via e-mail or telephone, with a stipulation to resolve the violation within 48 hours. Warning notifications will be sent to the primary and secondary Customer contacts listed in the VeriCenter Customer Account Database. Customers can update contact information (1) on VeriCenter's customer portal; (2) via e-mail to customerservice@vericenter.com; or (3) by phone at 1-866-VCenter (1-866-823-6837).

Failure to resolve the AUP violation within 48 hours may be a breach of contract and may result in suspension or termination of services. Customer will be charged for reconnecting services suspended as a result of AUP violation.

VeriCenter reserves the right to reduce the standard 48-hour resolution period for violations including but not limited to the following: violations involving law enforcement; phishing; fraud; harvesting/spidering of passwords or other personal information; network interference; denial or disruption of service (DoS); Internet relay chat (IRC) misuse; or other malicious activity.

Repeat violation of the above activities may result in the following actions.

- Immediate disconnection of service without prior notification.
- Reactivation fees based on the time and expense required for VeriCenter to reestablish service. Charges will be billed at an hourly rate based on the **Tier 3** Skill Category of VeriCenter's Professional Services Time and Expense (T&E) Rate Schedule, plus actual expenses. The Rate Schedule is posted on VeriCenter's Customer Portal.

VeriCenter reserves the right to refuse, cancel, or suspend service at its sole discretion.

6 Client Security Responsibility

Customers must take reasonable security precautions, such as password protection, when using VeriCenter services. Customer is solely responsible for any breaches of security affecting the servers and applications in Customer's environment. A compromised server is potentially disruptive to VeriCenter's network and other Customers. Therefore, VeriCenter may take a server offline if it is accessed or manipulated by a third party without consent. No credits will be issued for outages resulting from disconnections due directly to breached applications. A Customer Security Assessment Request and Agreement must be executed between Customer and VeriCenter before Customer or authorized third party performs vulnerability testing and/or penetration testing on VeriCenter managed or colocation infrastructure. If Customer intentionally creates a security breach, the cost to resolve any damage to Customer's server or other servers will be charged directly to Customer.

It is also Customer's responsibility to ensure that VeriCenter services are in compliance with Customer's security guidelines, including compliance with any government or industry requirements to which Customer's environment is subject.

7 Reseller Policy

Resellers are responsible for the conduct of their Customers and by accepting this AUP, agree that their Customers will abide by the AUP. Resellers should make their prospective Customers aware of the AUP and the consequences of violation.

8 Copyright Infringement Policy

VeriCenter's data center infrastructure including network, leased hardware, colocation services, and other hardware located in our facilities may be used for lawful purposes only. Accordingly, Customer may not store any material or content on such hardware, or disseminate any material or content that in any manner constitutes an infringement of third-party intellectual property rights, including rights granted by U.S. copyright law. Owners of copyrighted works who believe that their rights under U.S. copyright law have been infringed may report alleged infringements in accordance with the Digital Millennium Copyright Act of 1998 ("DMCA"). Copyright owners may report alleged infringements of their works by sending VeriCenter a notification of claimed infringement that satisfies the requirements of DMCA.

Customers who believe their copyright is being infringed by a person using the VeriCenter network should send a written notice of copyright infringement to VeriCenter via e-mail or postal mail to the applicable address shown in the [Violation Reporting Information](#) section of this document.

The notice must include the following:

1. A physical or electronic signature of the person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed;
2. Identification of the copyrighted work claimed to have been infringed, or if multiple copyrighted works at a single site are covered by a single notification, a representative list of such works at that site;
3. Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit VeriCenter to locate the material;
4. Information reasonably sufficient to permit VeriCenter to contact Customer, such as an address, telephone number, and, if available, an e-mail address;
5. A statement that Customer has a good-faith belief that use of the material in the manner complained of is not authorized by the copyright owner, the copyright owner's agent, or the law; and

VERICENTER ACCEPTABLE USE POLICY (AUP)

6. A statement that the information in the notification is accurate, and under penalty of perjury that Customer is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

If affected Customer or user believes in good faith that the allegedly infringing works have been removed or blocked by mistake or misidentification, that person may send a counter notification to VeriCenter using the contact information shown in the [Violation Reporting Information](#) section of this document.

All counter notifications must satisfy the requirements of Section 512(g)(3) of the U.S. Copyright Act. Upon VeriCenter's receipt of a counter notification that satisfies the requirements of DMCA, VeriCenter will provide a copy of the counter notification to the person who sent the original notification of claimed infringement and will follow DMCA procedures with respect to a received counter notification. In all events, it is agreed that VeriCenter will not be a party to any disputes or lawsuits regarding alleged copyright infringement.

Repeated violations of VeriCenter's Copyright Infringement Policy may result in permanent suspension of Customer's account.

9 Bulk or Commercial E-Mail

VeriCenter's services may not be used to send unsolicited bulk or commercial messages and may not be used to collect responses from unsolicited e-mail sent from accounts on other Internet hosts or e-mail services that violate this Policy or the Acceptable Use Policy of any other Internet Service Provider. Moreover, unsolicited e-mail may not direct the recipient to any Web site or other resource that uses VeriCenter's services. Activities that have the effect of facilitating unsolicited commercial e-mail or unsolicited bulk e-mail, whether or not the e-mail is commercial in nature, are prohibited. Forging, altering, or removing electronic mail headers is prohibited.

Customer must comply with the CAN-SPAM Act of 2003 and other laws and regulations applicable to bulk or commercial e-mail. In addition, Customer must be able to demonstrate all of the following to VeriCenter's reasonable satisfaction:

1. Customer's intended recipients must give their consent to receive e-mail via some affirmative means, such as an opt-in procedure;
2. Customer's procedures for soliciting consent must include reasonable means to ensure that the person giving consent is the owner of the e-mail address for which the consent is given; Customer must retain evidence of the recipient's consent in a form that may be produced promptly on request, and Customer must honor recipient's and VeriCenter's requests to produce consent evidence within 72 hours of receipt of the request. If positive and verifiable proof of opt-in cannot be provided, complaints from recipients of the mailing are considered proof that they

VERICENTER ACCEPTABLE USE POLICY (AUP)

did not subscribe and the mailing is unsolicited.

3. Customer must have procedures in place that allow a recipient to easily revoke his or her consent – such as a link in the body of the e-mail, or instructions to reply with the word "Remove" in the subject line. Revocation of consent must be honored within 72 hours, and Customer must notify recipients that revocation of their consent will be honored within 72 hours;
4. Customer must post an e-mail address for complaints (such as abuse@yourdomain.com) in a conspicuous place on any Web site associated with the e-mail; Customer must register that address at <http://abuse.net>, and must promptly respond to messages sent to that address;
5. Customer must have a Privacy Policy posted for each domain associated with the mailing;
6. Customer must have the means to track anonymous complaints; and
7. Customers may not obscure the source of their e-mail in any manner. Customer's e-mail must include the recipient's e-mail address in the body of the message or in the "To" line of the e-mail.

These policies apply to messages sent using VeriCenter services, or to messages sent from any network by Customer or any person on Customer's behalf that directly or indirectly refer the recipient to a site or an e-mail address hosted via Customer's VeriCenter services.

VeriCenter may test and otherwise monitor Customer's compliance with its requirements, and may block the transmission of e-mail that violates these provisions.

Block removal: If a Customer's actions have caused VeriCenter mail servers or VeriCenter IP address ranges to be placed on black-hole lists and other mail-filtering software systems used by companies on the Internet, Customer will be charged administrative fees to remove and protect mail servers and IP ranges, billed at an hourly rate based on the **Tier 3** Skill Category of VeriCenter's Professional Services Time and Expense (T&E) Rate Schedule, plus actual expenses. The Rate Schedule is posted on VeriCenter's Customer Portal.

1. Drop-box accounts: Using VeriCenter's network for the receipt of replies to unsolicited mass e-mail (spam) sent from a third-party network is prohibited.
2. Header forgery: Forgery of e-mail headers ("spoofing") is prohibited.
3. Proxy spamming: Spamming via third-party proxy, aggregation of proxy lists, or installation of proxy mailing software is prohibited.

VERICENTER ACCEPTABLE USE POLICY (AUP)

4. Relaying: Configuration of a mail server to accept and process third-party messages for sending without user identification and authentication is prohibited.

10 Malicious Uses and Activities

Violations of system or network security are strictly prohibited, and may result in criminal and civil liability. VeriCenter investigates all incidents involving such violations and will cooperate with law enforcement if a criminal violation is suspected. VeriCenter's network may not be used to publish or transmit, foster, or promote illegal, abusive, offensive, or irresponsible behavior. Content "published or transmitted" via VeriCenter's network or equipment includes Web content, e-mail, bulletin board postings, chat, and any other type of posting or transmission that relies on the Internet or local network.

Examples of prohibited activity include, but are not limited to, the following:

1. Unauthorized access to or use of data, systems or networks, including any attempt to probe, scan, or test the vulnerability of a system or network or to breach security or authentication measures (including those belonging to VeriCenter and its Customers) without an executed *Customer Security Assessment Request and Agreement* between VeriCenter and the owner of the system or network.
2. Using an Internet account or computer without the owner's authorization, including, but not limited to Internet scamming (tricking other people into releasing their passwords), password robbery, security-hole scanning, and port scanning. All scanning activities require an executed *Customer Security Assessment Request and Agreement* between VeriCenter and the owner of the system or network.
3. Engaging in sender address falsification, forging anyone else's digital or manual signature, or performing any other similar fraudulent activity.
4. Executing any form of network activity that will intercept data not intended for Customer's server.
5. Collecting responses from unsolicited messages.
6. Phishing: Using hosting software, scripts, executables, or other resources designed to fraudulently collect names, addresses, authentication, credit card, or any other personal data.
7. Using hosting software, scripts, executables, or other resources intended to facilitate the commission of any unlawful acts, or acts violating this AUP.
8. Harvesting/spidering : Fraudulently collecting identifiers (such as e-mail addresses, passwords, credit card information, screen names, or other personal information) of others without their prior consent, or participating in the use of

VERICENTER ACCEPTABLE USE POLICY (AUP)

software (including spyware) designed to facilitate this activity.

9. Social engineering: Obtaining confidential information through misrepresentation (including impersonation of any person or entity) and manipulation of legitimate users.
10. Engaging in conduct designed to avoid restrictions or access limits to specific services, hosts, or networks, including but not limited to the forging of packet headers (“spoofing”) or other identification information.
11. Interfering with service to any user of the VeriCenter or other network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system, and broadcast attacks.
12. Using VeriCenter services to introduce malicious programs into the network or server, including but not limited to viruses, worms, Trojan horses, key loggers, and other executables intended to inflict harm.
13. Advertising, transmitting, storing, or using any software, script, program, product, or service designed to violate this AUP.
14. Spamvertised sites: Hosting Web pages advertised by spam sent from another network.
15. Using VeriCenter services for distribution of advertisement delivery software unless:
 - a. the user affirmatively consents to the download and installation of such software based on a clear and conspicuous notice of the nature of the software, and
 - b. the software is easily removable by use of standard tools for such purpose included on major operating systems (such as Microsoft's "add/remove" tool).
16. Uploading, posting, publishing, transmitting, reproducing, creating derivative works of, or distributing in any way information, software, or other material obtained through VeriCenter services or otherwise that is protected by copyright or other proprietary right, without obtaining permission of the owner.
17. Initiating, perpetuating, or in any way participating in any pyramid or other illegal soliciting scheme.
18. Engaging in any conduct that is likely to result in retaliation against the VeriCenter network or Web site, or VeriCenter's employees, officers, or other agents, including behavior that results in any VeriCenter-managed infrastructure being the target of a denial of service attack.

11 Offensive Content

Customers may not publish or transmit via VeriCenter's network and equipment any content or direct links to any content that VeriCenter reasonably believes constitutes, fosters, or promotes child pornography. VeriCenter will cooperate fully with any criminal investigation into a Customer's violation of the *Child Protection Act of 1984* concerning child pornography. Customers are ultimately responsible for the actions of their clients over the VeriCenter network, and will be liable for illegal material posted by their clients.

Violations of the Child Protection Act should be reported to the U.S. Customs Agency at 1-800-BEALERT.

Other offensive content that will not be tolerated includes but is not limited to content that:

1. Is excessively violent, incites violence, threatens violence, or contains harassing content or hate speech;
2. Is unfair or deceptive, as determined by the consumer protection laws of any jurisdiction, including chain letters and pyramid schemes;
3. Is defamatory or violates a person's privacy;
4. Creates a risk to a person's safety or health, creates a risk to public safety or health, compromises national security, or interferes with an investigation by law enforcement;
5. Improperly exposes trade secrets or other confidential or proprietary information of another person;
6. Is intended to assist others in defeating technical copyright protections;
7. Clearly infringes on another person's trade or service mark, patent, or other property right;
8. Promotes illegal drugs, violates export control laws, relates to illegal gambling, or illegal arms trafficking;
9. Is illegal or solicits conduct that is illegal under laws applicable to Customer or to VeriCenter; or
10. Is malicious, fraudulent, or may result in retaliation against VeriCenter by offended viewers.

VERICENTER ACCEPTABLE USE POLICY (AUP)

12 Disclaimer

VeriCenter is under no obligation, and this AUP does not constitute an obligation, to monitor or police our Customers' activities, and VeriCenter disclaims any responsibility for any misuse of the VeriCenter network. However, VeriCenter has the right to monitor Customers' transmissions and postings from time to time for violations of this AUP and to disclose, block, or remove transmissions and postings in accordance with this AUP and any other applicable agreements and policies. VeriCenter disclaims any obligation to any person who has not entered into an agreement with VeriCenter for services.

13 IP Allocation and Blocking

VeriCenter administers an Internet network on which multiple Customer servers reside. Customers may use only IP addresses assigned to them by VeriCenter staff in connection with Customers' VeriCenter services. Any server using IP addresses outside of the assigned range will be suspended from network access until such time as the IP-address overlap can be corrected.

Customers may not take any action that directly or indirectly results in VeriCenter-assigned IP space being listed in any of the various abuse databases. If Customer's actions cause VeriCenter-assigned IP space to be placed on black-hole lists and other mail-filtering software systems used by companies on the Internet, Customer will be charged administrative fees to remove and protect VeriCenter-assigned IP space, billed at an hourly rate based on the **Tier 3** Skill Category of VeriCenter's Professional Services Time and Expense (T&E) Rate Schedule, plus actual expenses. The Rate Schedule is posted on VeriCenter's Customer Portal.

Customers must have valid and current information on file with Customer's domain name registrar for any domain hosted on the VeriCenter network.

14 Internet Etiquette

Customer must comply with the rules and conventions for postings to any bulletin board, chat group, or other forum in which Customer participates, such as IRC and USENET groups, including their rules for content and commercial postings. These groups usually prohibit the posting of off-topic commercial messages, or mass postings to multiple forums.

Customer must comply with the rules or policy of any other network Customer accesses or participates in while using VeriCenter services.

15 Cooperation with Investigations and Legal Proceedings

In response to a formal or informal request from a law enforcement or government agency, or in response to a formal request in a civil action that meets the requirements for such a request, VeriCenter may provide any information it has about Customer without notice to Customer. VeriCenter may also report to the authorities any conduct that it believes violates applicable criminal law. VeriCenter is also obliged by United States

VERICENTER ACCEPTABLE USE POLICY (AUP)

law to comply with a formal request to gain access to, or intercept information to and from Customer's environment.

16 Conduct on VeriCenter Premises

Failing to comply with VeriCenter's procedures relating to the activities of Customers on VeriCenter's premises is a violation of this AUP. Violators of the policy are responsible, without limitations, for the cost of labor to correct all damage to the operation of the network and business operations supported by the network. Such labor is categorized as emergency security breach recovery and is charged at an hourly rate based on the **Tier 3** Skill Category of VeriCenter's Professional Services Time and Expense (T&E) Rate Schedule, plus actual expenses. The Rate Schedule is posted on VeriCenter's Customer Portal.

17 Fraud

By agreeing to this AUP, Customer affirms that the contact and payment information provided to VeriCenter identifies Customer, and that Customer is authorized to use the payment method. Commitment of fraud, or obtaining services or attempting to obtain services by any means or device with intent to avoid payment is prohibited.

18 AUP Copyright Information

This document and all portions of the VeriCenter Web site, including images, text, and scripts where ownership is not held by third parties are copyright 2007 VeriCenter, Inc. This AUP, whole or in part, may be reproduced only with the written permission of VeriCenter, Inc.

Effective Date

This policy is effective as of April 4, 2007.