



ACCEPTABLE USE POLICY

Introduction

This Acceptable Use Policy governs the use of all the hosting services, hosting solutions, cloud services, managed services and other offerings (the “Services”) made available by Navisite, LLC, a Delaware corporation (“Navisite”), and its suppliers and affiliates. It defines the policies of Navisite which are designed to protect Navisite, its customers and any other persons, parties or entities from any negative impact caused by inappropriate or illegal activities regarding the Services. Any person or entity (“you,” “your” or words of like import) who receives access to facilities or Services by or through Navisite shall adhere to this Acceptable Use Policy and agrees to be bound by and subject to the terms and conditions set forth below.

The purpose of this Acceptable Use Policy is to set forth guidelines for the expected conduct of users of the Services and the types of actions and content that are contrary to Navisite’s mission and philosophies. Navisite may suspend or terminate your right to access and use the Services if, in its sole determination, it believes you have violated this Acceptable Use Policy.

This Acceptable Use Policy is an integral part of your agreement with Navisite and is incorporated by reference into the terms pursuant to which Navisite provides you the right to access or use the Services. Access to or use of the Services constitutes your acceptance of this Acceptable Use Policy. Navisite reserves the right to alter this Acceptable Use Policy at any time and such modifications shall become immediately effective upon notification to you of the modified Acceptable Use Policy. By using Navisite’s Services or facilities after the posting of any such modifications, you acknowledge your agreement to those modifications. If at any time you choose not to accept this Acceptable Use Policy, you must immediately discontinue use of all Services and facilities.

Reports of any violations of this Acceptable Use Policy should be sent to legal@Navisite.com.

Navisite reserves the right to audit, test, and investigate the security of your environments to ensure that security protections are maintained and that your environments do not bypass, or allow others to bypass Navisite security controls. If, in its sole discretion, Navisite believes that systems located within Navisite’s facilities or through our services are being used in an unlawful or improper manner (whether civil or criminal) or for unlawful or improper activities, Navisite will fully cooperate with civil and criminal-enforcement authorities conducting investigations of such use or activities. Navisite will also support the investigation of the prohibited activities listed below and any other activities that Navisite, in its sole discretion, believes impact the operations or security of Navisite, its customers or other systems accessible by you or any of your employees, agents, representatives, affiliates, customers, clients or users.

Disclaimer

Navisite is under no duty to monitor the activities of you or any of your employees, agents, representatives, affiliates, customers, clients or users, and Navisite disclaims any responsibility for any misuse of the Services. Navisite has no responsibility for any material or information created, stored, maintained, transmitted or accessible on or through the Services, and is not obligated to monitor or exercise any editorial control over such material. In the event that Navisite becomes aware that any such material violates this Acceptable Use Policy and/or exposes Navisite to civil or criminal liability, Navisite may, but is not required to, block access to such material. Unless otherwise stated in this Acceptable Use Policy, Navisite disclaims any obligation to any person who has not entered into an agreement with Navisite for use of the Services and has not agreed to the terms of this Acceptable Use Policy.

Acceptable Use

You have access to and may perform management activities on your systems, data and/or content. You are responsible for ensuring that these activities do not impose risks to, or negatively impact Navisite (including without limitation any of Navisite’s employees, representatives, agents or affiliates), its other customers or other environments or systems. You are also responsible for adhering to all local, state,

federal and international laws and regulations relating to all of your operations and the use and access of any computing systems hosted by Navisite or its suppliers. You must fully comply with all software licenses while using any information technology resources provided by or through Navisite. You are expected to read, understand and conform to the license requirements of any software product(s) you use or install.

Prohibited Activities

You are responsible for ensuring that you do not allow any of your systems hosted by or on behalf of Navisite to be used for any of the following purposes:

1. gaining, or attempting to gain, unauthorized access to any system that does not belong to you;
2. sending unsolicited e-mail or other messages or communication in any form (e.g., spam);
3. altering, defacing or otherwise causing any unauthorized or unapproved modification of any system belonging to Navisite, another Navisite customer or any other system on the Internet;
4. storing, transmitting or processing material in a manner that violates intellectual-property rights or laws or regulations, including, without limitation, those associated with trade secrets, copyrights, patents and trademarks;
5. violating the privacy rights of others, including, without limitation, the collection of information about individuals without their knowledge or consent, except as allowed by applicable laws and regulations;
6. transmitting or storing any material that is unlawful, obscene, harassing, libelous, abusive or hateful; that encourages unlawful acts; or that may be interpreted as violating the civil rights of others;
7. storing or transmitting material that violates local, state, federal or international laws or regulations;
8. engaging in, or permitting any activity that leads to a degradation or denial of service for Navisite, another Navisite customer or any other system or site on the Internet;
9. violating the rules or policies of any other hosting provider, message service, chat room, bulletin board, newsgroup or similar system, service or provider;
10. intentionally, recklessly or negligently omitting, forging, deleting or misrepresenting transmission information – including, without limitation, headers, return-address information and IP addresses – that is intended to cloak or hide the identity or source of information transmitted by your systems, customers or users;

You are prohibited from assisting any persons or entities in using any of your systems maintained by or through Navisite to engage in any of the activities listed above. If you become aware of any such activity, you must remedy the situation immediately. You must also notify Navisite by telephone within four hours and in writing within 24 hours of the detection of a violation by you or any of your employees, agents, representatives, affiliates, customers, clients or users.

You are responsible for ensuring that security controls are not circumvented by way of actions taken by you or individuals accessing your systems.

You must not:

1. configure your systems to bypass security controls, including, without limitation, the installation of programs or services that allow the systems to be managed or accessed insecurely or through unauthorized means;

2. conduct online security audits or tests against or through Navisite systems or networks without coordination with and the explicit, written consent of an authorized officer of Navisite;
3. gain, or attempt to gain, unauthorized access to Navisite networking, security, management, backup, storage or monitoring systems;
4. install programs or configure systems to allow the monitoring or “sniffing” of data traveling over a shared network;
5. access, or attempt to access, security-relevant information, such as password files that may, among other things, be used to gain unauthorized access to system accounts;
6. install or use software for the purpose of cracking encrypted data, including, without limitation, stored passwords; or
7. remove or disable security software or services, including, without limitation anti-virus software, logging utilities or authentication services; or
8. violate the CAN-SPAM Act of 2003, as heretofore amended, and other laws and regulations applicable to bulk or commercial email.

Additionally, you

1. are responsible for any misuse of accounts on your systems located at Navisite;
2. must implement measures and procedures to ensure that your accounts are not accessed or used in an unauthorized manner;
3. shall not transfer or allow the transfer of Remote-access accounts from one individual to another, nor share or allow such accounts to be shared between individuals;
4. shall ensure that each user has an individual remote-access account that uniquely and accurately identifies the owner of the account; and
5. assume all responsibility for the consequences of the use of your accounts by an unauthorized individual.

Violations and Remedies

In order to protect its customers’ data security, to ensure that its customers have access to their systems and data and to prevent breaches by other customers from affecting such security and access, Navisite reserves the right to suspend or terminate at any time your account if, in the sole discretion of Navisite, you fail to adhere to this Navisite Customer Acceptable Use Policy or Navisite reasonably believes that your use of any facilities or services has resulted or will negatively impact other customers’ security or use of or access to their respective systems or data (including without limitation, actions by customers that may result in denial of service attacks or other outages, privacy violations or intellectual property infringement) . Navisite will endeavor to provide you with advance notice prior to restricting your access to your environment and services, to the extent that the circumstances of the situation shall merit, but shall not be required to do so in all cases. Navisite has the right to seek legal remedies for any damages, costs or expenses that may be incurred as a result of a violation of any of these policies by you or your employees, agents, representatives, affiliates, customers, clients or users.

Depending on the nature of the violation or alleged violation, Navisite may be notified of violations in any number of ways, including by an external organization, agency, entity or individual that is affected by your activities or, when a violation is detected internally, by a source within Navisite.

Navisite retains the sole right to determine whether a violation of this policy has occurred. In general, Navisite will attempt to work with you to address violations of this policy in accordance with the steps outlined below but is not required to do so. However, based on the severity of the violation or the number or nature of complaints received, Navisite, in its sole discretion, has the absolute right to immediately terminate all services and facilities access.

Upon notification of a violation, Navisite will attempt to contact you and describe the violation. In general, your contact will be called or emailed with the information. Navisite will define a specific timeframe within which you must rectify the violation. A letter may be sent to your contact formally notifying you of the violation and setting forth the time frame for you to remedy the violation. If, in Navisite's sole discretion, the violation or complained-of violation is such that Navisite elects not, or is unable, to contact you, Navisite may take whatever steps it deems appropriate under the circumstances.

Navisite reserves the right to immediately suspend any or all access to all facilities and services to you without notice to, or approval from, you, if Navisite, in its sole and absolute discretion, deems such suspension necessary to protect its systems, facilities or interests or those of its employees, representatives, agents, affiliates, customers or other third parties, including, without limitation, in response to any perceived threat of a computer virus, exploit scripts or other malicious software or denial-of-service attack on Navisite's or its other customers' or suppliers' systems or network; provided, however, that Navisite will use commercially reasonable efforts to notify you prior to such suspension.

Nothing in this Acceptable Use Policy shall limit Navisite's rights and remedies at law or in equity that may be available.

Service Level Credits

No credit will be available under a Navisite service level guaranty or agreement for interruptions of access to facilities or services resulting from your violation of this Acceptable Use Policy.

[End of Document]