

MITEL CLOUD SERVICES - ACCEPTABLE USE POLICY

Introduction

The Mitel Cloud Service is designed for general business use. This Acceptable Use Policy (“AUP”) applies to all Mitel customers and their Users (as defined in the Mitel Cloud Services - Global Terms of Service (“GTOS”)). It is intended to maintain the integrity of our network and the high performance of our Cloud Services. You may not use, encourage, promote, facilitate, or instruct others to use our Cloud Services in violation of this AUP.

Rules of Use

A. Customers may not use the Cloud Services:

1. in any manner that encumbers system or network resources to the point that usage causes interference with other customers' normal use of the cloud services, either on our system or network or any remote system or network;
2. with auto dialers;
3. in a manner that is abusive or fraudulent;
4. to make or attempt to make any unauthorized intrusion or entry into any part of, to violate or attempt to violate the security or integrity of, or to interfere or attempt to interfere with the proper operation of, our cloud services or any system or network of any other person (including, without limitation, any other customer of ours);
5. in any manner or for any purpose that violates (i) any applicable law, regulation or ordinance, whether, local or foreign law, including without limitations those related to electronic recordings of telephone conversations, (ii) the GTOS or (iii) any instructions we issued from time to time;
6. in any manner that may infringe upon or violate any copyright, trademark, service mark, patent, trade secret, other intellectual property right of, or other personal right, of any third party;
7. to transmit any information that is unlawful, harmful, threatening, abusive, harassing, tortious, defamatory, vulgar, pornographic, obscene, libelous, hateful or racially, ethnically or otherwise objectionable;
8. to impersonate any person or to misrepresent an affiliation with any person;
9. to transmit any information that you do not have a right to transmit, whether because of a contractual obligation (such as a confidentiality or non-disclosure agreement) or otherwise;
10. to transmit, send, place or post unsolicited telephone calls, texts or other information;
11. to send unsolicited or unauthorized advertising, promotional materials or any other form of solicitation or spam;
12. for inbound or outbound telemarketing or call center operations, except for Mitel CX;
13. to transmit anything that contains corrupted data or that contains a virus, Trojan horse, worm, time bomb, keystroke loggers, spyware, or cancelbot, or any other computer programming routine or engine that is intended to damage, detrimentally interfere with, surreptitiously intercept or expropriate any system, data or information;
14. to decipher, decompile, disassemble or reverse engineer any elements or our system or network or of any system or network of any other person, or to attempt to do so;
15. to perform any form of security testing (also known as penetration testing) on any system we manage without our express prior written authorization. Requests for authorization may be submitted to itsecurity@mitel.com, giving at least five (5) working days' notice. Requests should include the scope and type(s) of testing that is being requested as well as planned start and end times for the same. Our technical teams will then review the request and identify the set of addresses/systems, if any, that you are permitted to perform testing on, as well as testing that you are not permitted to perform. Mitel will then send you an email either authorizing you to perform certain tests or informing you that your request has been rejected. Testing results shall be considered Mitel confidential information and shared with Mitel. Mitel retains the right to for any reason, or no reason deny any security testing request;
16. to exploit or harm minors (e.g., expose them to inappropriate content; ask for personally identifiable information without parental consent.); or
17. the Services can only be used with Mitel products which have been purchased and for which customer is currently subscribing to software assurance.
18. the number of Users/ usage of the Cloud Service should not extend the number of users/ system limitations that are documented in the Mitel documentation.

B. In addition to the above, Customers cannot use the Unify Phone Cloud Service to:

1. collect or harvest any personally identifiable information, including account names, from Unify Phone Service and in particular from the Unify Phone Service Directory, save where you have the explicit permission of the affected Unify Phone Service Users;
2. the extent Unify Phone Service allows you to make outbound calls through other channels than your own telephone system, you may not call numbers (whether singly, sequentially or automatically) to generate income for yourself or others as a result of placing the call, other than for your individual business communications.

C. In addition to the above, the following applies to Customers' use of the Mitel CX service:

1. Third-Party Integrations and APIs
 - a. Only use approved or secure integrations
 - b. Ensure third-party apps comply with this acceptable use policy
 - c. Do not use unauthorized automation or bots
2. Content and Recording Policies
 - a. No unlawful surveillance or access to recordings
 - b. Inform users when calls are recorded

Changes to this Policy

We may revise this acceptable use policy in accordance with the corresponding sections on changing our terms to be found in the GTOS.

Waiver

Any failure or delay in us exercising or enforcing this policy shall not constitute a waiver of this policy or of any other right or remedy.

Reporting Abuse

If you become aware of any misuse of our Cloud Services by any person, please contact Mitel Customer Support at +1 (800) 721-1301 or +44 1291 436888. We may investigate any complaints and violations that come to our attention and may take proportionate actions to remedy the violation. We will only remove content, close user accounts, or terminate the entire contract where this is necessary to effectively stop a violation.