

2026 JumpCloud Code of Conduct

JumpCloud Inc. and its subsidiaries (“Company” or “JumpCloud”) and all those acting on JumpCloud’s behalf are required to conduct business ethically, fairly, honestly, and openly.

SCOPE:

This Code of Conduct applies to all directors, officers, contractors, employees of the Company and any others acting on the Company’s behalf. The Company expects anyone working on its behalf to conduct all activities related to, or reflecting on, JumpCloud business with integrity and according to the letter, spirit, and intent of all applicable laws and this Code of Conduct.

POLICY:

Standards of Performance and Conduct

JumpCloud is committed to building a strong culture underpinned by building connections, mutual respect, and fostering a healthy and positive work environment.

JumpCloud has zero tolerance for violence, threats of violence, or bullying of any kind. This includes: (i) inappropriately threatening, intimidating, bullying, or coercing any employee, contractor, customer, or vendor of or visitor to the Company, in any manner, including by use of abusive or vulgar language; (ii) engaging in any harassment or discrimination against any individual; (iii) engaging in illegal activities or conduct that poses a health or safety hazard; or (iv) engaging in disorderly conduct that could endanger, disturb, or interfere with any employee, contractor, customer, vendor, or partner of the Company.

JumpCloud expects all individuals associated with its business to act with integrity and, to the extent it does not restrict your rights under applicable law, JumpCloud does not tolerate: (i) possessing or using weapons, dangerous or unauthorized materials, liquor (unless authorized), or illicit drugs in the workplace; (ii) impairment by alcohol, illegal drugs, or intoxicants while on Company property or duty; (iii) falsifying, removing, or destroying any records without authorization; (iv) damaging, destroying, removing, or failing to return any property (physical or intellectual) belonging to the Company, fellow employees, customers, or other party; (v) improperly using or disclosing confidential information about the Company, customers, vendors, partners, or employees, unless required or permitted by law; or (vi) violation of this Code of Conduct or any Company rule, practice, or policy.

Business Ethics and Conduct

JumpCloud conducts its business in compliance with all applicable laws and regulations. Those acting on behalf of the Company are expected to act in accordance with the highest standards of business ethics, to avoid any appearance of impropriety, and to observe all applicable laws and regulations while conducting business on the Company’s behalf. Individuals are expected to cooperate with any inquiries or investigations concerning a possible or suspected violation of this Code of Conduct.

Ethical Standards

JumpCloud is committed to conducting business in a fair and open manner within the spirit and letter of the law, with the highest regard for customers, vendors, partners, and employees. The Company’s success depends not only on the knowledge, skills and abilities of its people, but also on sound judgment, self-discipline, common sense, and integrity. As such, those acting on behalf of the Company must maintain and uphold the following ethical standards:

- To pursue Company objectives in a manner that does not conflict with the integrity of the Company or the public interest;
- To be truthful and accurate in all you say and do;

- To protect confidential information;
- To treat others with respect and dignity;
- To observe all applicable laws, regulations, ordinances, and rules; and
- To maintain honest and fair relationships with all Company customers, vendors, and partners;

Conflicts of Interest

Those acting on behalf of the Company must avoid situations and conduct that would create an actual or potential conflict of interest or create the appearance of such a conflict.

Conflicts of interest arise when an individual's personal activity or personal interest is contrary to the interests of the Company. These personal activities or interests may influence judgment, causing the individual to make decisions based upon the potential for personal gain, rather than in the best interests of the Company or any other party they represent.

Some common conflicts of interest scenarios include:

- Receiving or giving of merchandise, money, services, travel, accommodations, or lavish entertainment that might appear to have been given to influence a business decision. Gifts offered or received at any time should be in compliance with the Company's Travel and Expense policy.
- Maintaining personal, business, or financial relationships with a customer or vendor where the employee has control or influence over the Company's relationship with that customer or vendor. For example, employees should not borrow from or lend personal funds to an individual that works with a customer or vendor.
- Using information developed or learned on the job for personal or familial benefit. This includes the use of Company databases, financial information, and intellectual property.
- Maintaining outside directorship, employment, or political office that might appear to or actually conflicts or competes with an employee's responsibilities.
- Conducting business (or influencing the Company to conduct business) with family members.
- Unauthorized sharing of confidential or proprietary Company-related information with business associates or representatives of other companies.

The list above serves only to illustrate sources of possible conflicts of interest and does not constitute a complete list of all the situations that may result in a conflict of interest. Ultimately, it is the responsibility of each individual to avoid any situation that could affect his/her ability to judge situations independently and objectively, and any situation that could even appear to be a conflict of interest. It is important to note that under certain circumstances, conflicts of interest can amount to violations of criminal law. Questions should be directed to the legal department.

During scheduled work hours, individuals are expected to devote their full time and attention to their work responsibilities, Company property or resources may not be used for outside activities without permission or in violation of the Company's acceptable use policy.

Employment of Relatives and Significant Others

To avoid conflicts of interest and to promote stability and goodwill in the workplace, we usually don't hire or transfer relatives into positions in which they supervise or are supervised by another close family member. We also try to avoid placing them in positions in which they work with or have access to sensitive information about family members. If you develop a close personal

relationship with another employee or individual at another company that does business with JumpCloud, it is your responsibility to immediately report the relationship and seek guidance on whether such relationship constitutes a conflict of interest. If such a relationship develops and it creates an actual or perceived conflict, we reserve the right to use our discretion in hiring and placing employees in a manner designed to avoid these concerns.

No Improper Use of Information of Prior Employers and Others

Individuals are prohibited from using and disclosing the confidential information and trade secrets of any previous employer or other third party to whom they have an obligation of confidentiality.

Specifically, those acting on behalf of the Company:

- will NOT bring a former employer's confidential information, trade secrets, data, or intellectual property onto JumpCloud premises or systems (e.g., JumpCloud computer); and
- will NOT use or disclose any such information in connection with your work for or on behalf of JumpCloud.

Additionally, individuals must not breach any agreement with any former employer or other third party, including any non-compete agreement, non-disclosure agreement (NDA), or other agreement requiring them to keep information confidential.

No Use of Copyleft Code

Those acting on behalf of the Company will not incorporate into any JumpCloud software or otherwise deliver to JumpCloud any software code licensed under the GNU, GPL, or LGPL or any other license that, by its terms, requires or conditions the use or distribution of such code on the disclosure, licensing, or distribution of any source code owned or licensed by JumpCloud, unless explicit written approval has been obtained from the appropriate executives and legal department.

Recognizing & Reporting a Breach

The Company expects those acting on its behalf not only to abide by this Code of Conduct but also to report behavior by others that may violate the letter, spirit or intent of this Code of Conduct, Company policies, or applicable law.

The Company maintains reporting channels for possible violations. When in doubt about whether a situation constitutes an ethical problem, individuals should report it. The Company provides confidential and anonymous reporting options. The Company treats all concerns and complaints seriously and maintains confidentiality of information shared, except to the extent disclosure is necessary to properly investigate the complaint, is required by law, or is necessary to address the concerns raised.

The Company has a strict anti-retaliation policy. Individuals will not be penalized for good faith reporting of concerns or potential violations of this Code of Conduct, company policy, or applicable laws. Concerns about retaliation should be reported promptly through the Company's reporting channels.

Export Law

JumpCloud is committed to compliance with all export controls in the United States Export Administration Act, the Export Administration Regulations, and other relevant laws and regulations. This commitment extends to promoting strict compliance on an on-going basis with terms and conditions. It is Company policy that all employees, contractors, agents, and others performing services for or on behalf of JumpCloud comply with relevant export policies and regulations. Under no circumstances will exports be made contrary to U.S. export regulations by any individual operating on behalf of JumpCloud. Employees outside the United States may not re-export any commodity, technology, or software unless appropriate authorization has been obtained, and this includes foreign-produced items that are the direct product of U.S. technology and software and are subject to national security controls under the Export Administration Act. No activities will be undertaken that are in violation of the United States policies which seek to control nuclear proliferation, missile technology, and chemical and

biological weapons. The Company's IT policies provide additional detail regarding IT security and export control compliance obligations.

Competition Law

The Company holds a policy of compliance with all laws applicable to its operations worldwide and as such, requires strict compliance with all antitrust legislation. Because circumstantial evidence is frequently the basis upon which antitrust liability is found, the Company and those acting on behalf of the Company also must avoid even the appearance of anti-competitive conduct. We should also be mindful regarding the language we use in written communications. Phrases such as 'destroying the competition' can be misconstrued. Each employee must understand and comply with antitrust laws as they may bear upon his or her activities and decisions.

While competition laws can vary by jurisdiction, employees and those acting on behalf of the Company are expected to follow these following principles: We do not engage in price fixing or resale price maintenance, we do not misuse confidential information provided by a third party except as permitted under any applicable non-disclosure agreement, we do not discuss competitively sensitive information about JumpCloud or its vendors, customers or suppliers with any third party, except pursuant to a non-disclosure agreement, and we do not agree to competitors to divide markets, customers or

recruiting efforts. Competition laws sometimes can be very complicated, we encourage you to consult with the Legal department if you have questions.

Anti-Bribery and Anti-Corruption / Accurate Books and Records

JumpCloud prohibits bribery and other forms of corruption. The Company, each employee as well as vendors and customers are responsible for complying with the U.S. Foreign Corrupt Practices Act and the anti-bribery and anti-corruption laws and regulations in each country where we operate, as well as our Anti-Bribery and Anti-Corruption Policy. These laws and our policies prohibit giving any sort of payment or anything of value to a Government Official, or anyone else, where the intent is to improperly influence the Government Official or other person to obtain or retain business or some other commercial advantage for JumpCloud, or accepting any sort of payment or anything of value from anyone, where the intent is to be influenced to act improperly (e.g., a breach of an expectation that a person will act in good faith, impartially or in accordance with a position of trust). While some countries make a distinction between Government Officials and other third parties, this Code does not. A bribe can take many forms and includes money, gift, hospitalities, expenses, favors, political or charitable contributions, or indirect consideration. Our anti-bribery policy prohibits direct action by employees and other parties and indirect action through others (e.g., third parties) who are performing services on behalf of JumpCloud, such as consultants, advisors, suppliers, distributors or agents.

If you wish to provide promotional, entertainment, or travel expenses for any Government Official, you must first get approval from the Legal department. If you believe that a local written law permits certain payments that are not allowed by the Company, please consult the Legal department.

Expenses incurred as a result of illegal payments must never be hidden or purposefully misclassified and must always be accurately recorded and accounted for. International anti-bribery laws require detailed and accurate accounting records for all transactions, including cash and bank accounts. Violation of this requirement may result in prosecution of individuals and/or JumpCloud.

Violation of the Policy

Violations of this Policy will be grounds for discharge, termination of contracts, or other disciplinary action, adapted to the circumstances of the particular violation. Disciplinary action will be taken against individuals who authorize or participate

directly in a violation of the Code. Disciplinary action also may be taken against any of the violator's managerial superiors, to the extent that the circumstances of the violation reflect inadequate supervision and leadership by the superior. Compliance with the Code will be considered in the evaluation of performance.

Training

Individuals will be required to complete training on a regular basis to ensure that they are familiar with this Code. We each have a responsibility for holding each other accountable to assure we follow this Code.

Questions or Reports

If you want to ask a question about this Code, contact the Legal department.

If you are concerned that a violation of this Code could occur, is occurring, or has occurred, report the matter immediately to the Legal Department or via our reporting hotline.