Global Code of Conduct and Ethics

Our values.

Put Customers First

We only succeed when our customers succeed. Work every day to earn our customers' business and trust. Listen to our customers, understand their needs and pain points, and focus on what matters to them. Deliver products our customers love. Compete fairly and passionately.

Integrity Always

Be open, honest and respectful. Speak up and communicate candidly, even when it makes you uncomfortable or may be something others don't want to hear. Constructive, respectful disagreement and debate encourages better problem-solving and decisions. Commit fully when decisions are made.

Think Big

Be ambitious and have big goals. Do what matters and focus on what's important. Innovate and be willing to take prudent risks. Make a positive impact and a lasting difference. Plan to win, play to win and expect to win.

Be Excellent

Quality and excellence count in everything we do. Do your best work every day. Hold yourself and others to the highest standards. Common sense, creativity, practicality and simplicity matter. Think strategically, balancing today and tomorrow.

Get it Done

Results matter! Work hard and smart. Execute. Be precise and accountable, yet nimble and agile. Make commitments, follow through, and deliver.

Own It

Build our product and our company like it's yours, because it is. Hold yourself and others accountable at all times. Take initiative and ownership. Be responsible. Step up, own issues and resolve them. If you make a mistake, own it, fix it, learn from it and move on.

Make Each Other The Best

Treat people with kindness and respect. Be inclusive and collaborative, bringing people and ideas together. Offer help and ask for help when needed. Listen. Give and ask for constructive feedback. Give praise and celebrate success. Teach and learn every day. Give back to our communities in meaningful ways and inspire others with your actions.

Embrace Each Other's Differences

Accept and appreciate everyone from every walk of life. Be conscious and mindful that others may have a different experience from your own. Use our differences to strengthen who we are.

Global Code of Conduct and Ethics

Our values represent who we are at our best. They are the engine that drives Snowflake's growth and success. Snowflake is a global community, and each of us depends on everyone else to do the right thing every single day. Sometimes, though, the right thing isn't obvious, or you may not be aware of what the law requires you to do. This Global Code of Conduct and Ethics ("**Code**") is your guide for upholding Snowflake's values in your day-to-day activities. You must also understand and follow the laws and regulations that relate to your job.

This Code applies to all employees, members of Snowflake Inc.'s Board of Directors (the "**Board**"), contractors, and other contingent workers of Snowflake Inc. and its subsidiaries (together, "**Snowflakes**," "**representatives**" or "**you**").[1]

Snowflake managers and leaders play a special role in creating and preserving our culture. Your team takes its cues from you. Always lead by example and uphold the highest standards. Create an environment in which people feel accountable and comfortable asking questions or raising concerns. If someone raises an issue, make sure that it is handled quickly and correctly.

This Code does not replace Snowflake's other policies and procedures, and cannot cover every possible law or scenario. Snowflake's policies are on The Lift. If there is a conflict with our Employee Handbook, this Code will take precedence. If you have questions about the Code or the right thing to do, please contact Human Resources or Legal. Contact information for teams and individuals referenced in this Code is listed here.

Raising Issues and Concerns

You must report any suspected violation of laws, rules, regulations, or this Code to Human Resources or Legal immediately. **Snowflake does not tolerate retaliation.** Snowflake will not retaliate against anyone who, in good faith, reports violations or suspected violations, or assists in an investigation of a reported violation. Immediately report to Human Resources or Legal any acts that appear to be retaliation. Any manager who receives a report of a potential violation must immediately inform Human Resources or Legal. Suspected violations can be reported to Human Resources by contacting your HR Business Partner or the Chief Human Resources Officer, and to Legal by contacting the General Counsel or a Deputy General Counsel.

If you prefer to remain anonymous, you can also report your concerns through the Snowflake Whistleblower Hotline in one of two ways:

- **Phone**: 1 (844) 476-9147
- **Website Intake URL**: snowflake.ethicspoint.com

We encourage you to provide as much detail as possible about the complaint or concern, because Snowflake's ability to investigate depends on the quality and specificity of the information. All properly

[1] If you are an employee or contingent worker of any majority owned but non-wholly owned subsidiary of Snowflake Inc. ("**Indirect Personnel**"), specific processes for seeking approvals or making notifications may not apply to you. When reading the Code, look out for specific areas where the rules for Indirect Personnel are a little different.

reported potential violations of this Code will be promptly investigated. Violators will be subject to discipline up to and including termination. In addition, where appropriate, any violations of law will be reported to the appropriate law enforcement authorities.

Snowflake will try to keep discussions and actions relating to good faith reports confidential to the extent possible, consistent with its ability to investigate and respond appropriately, and subject to applicable privacy laws and regulations. If you report anonymously, Snowflake will protect your anonymity to the fullest extent possible, but cannot guarantee it.

Respect and Protect Each Other

Creating a safe and supportive environment is extremely important to us. Snowflakes should treat each other with respect and dignity. Everyone is entitled to work in an inclusive environment that is free from unlawful discrimination and harassment.

Equal Opportunity Employment

Snowflake is an equal opportunity employer. We prohibit unlawful discrimination in employment opportunities or practices on the basis of gender, race, color, creed, religion, age, citizenship, sexual orientation, gender identity, gender expression, genetic information, marital status, pregnancy, national origin, ancestry, physical or mental disability or condition, military or veteran status, or any other protected class under applicable federal, state, or local laws. We also prohibit unlawful discrimination based on the perception that anyone has any of those characteristics or is associated with a person who has or is perceived as having any of those characteristics.

Harassment

Snowflake is committed to maintaining a respectful workplace, which includes a working environment that is free from harassment. Harassment and any conduct that may foster an offensive or hostile work environment, including unwelcome or unsolicited sexual advances, threats of physical harm or violent behavior, or use of discriminatory slurs or inappropriate conduct, remarks, or jokes, are strictly prohibited. We have a zero-tolerance policy for violence and threatening behavior. This policy applies to all work-related settings and activities, whether inside or outside the office, and includes business trips and work-related social events.

Respectful Communications

We are mission driven. Snowflake's reason for existence is to build the world's best data cloud. To do this, we need to live and breathe one of our core values: Embrace Each Other's Differences. The Snowflake community is diverse and multinational . We have different backgrounds, different cultures, different religions, different values, and different political beliefs. But we are all Snowflakes. Staying focused on what we have in common—our mission—and embracing each other's differences with respect is the only way we will succeed.

Embracing Each Other's Differences means being respectful, even if you disagree with something. Inherent in expressing yourself respectfully is an awareness that reasonable minds may differ. Comments about culture, politics, religion, health decisions, and other sensitive topics can easily make people feel like they can't express opposing views. Remember that people have a right to participate or decline to participate in the political process outside of work in their private capacities. Don't call out or shame people for their lawful, personal beliefs, activities, or statements on moral, political, or social issues. Calling out or shaming individuals for these or similar reasons can amount to harassment under this Code.

This policy extends to interactions with or about your peers, management, clients, customers, and Snowflake's other business contacts. It applies at all times during your Snowflake employment and includes Snowflake's community forums like Slack and Zoom. It extends beyond the workplace to off-site and work-related events. Our anti-harassment policy also applies to public statements that relate to or impact Snowflake, its reputation, or its employees, including social media posts using personal accounts

on platforms like LinkedIn or X (formerly Twitter). In short, it is everyone's responsibility to create a healthy and inclusive workplace environment, where all communication and interactions are marked by dignity and respect.

We take this policy extremely seriously, and anyone who violates it may be subject to discipline, up to and including termination.

Health & Safety

Snowflake strives to provide a safe, healthy, and sanitary work environment. You are responsible for helping to maintain a safe and healthy workplace for everyone by following safety and health rules and practices and promptly reporting accidents, injuries, and unsafe equipment, practices, or conditions.

Drugs & Alcohol

Snowflake's position on substance abuse is simple – it is incompatible with the health and safety of our employees, and we don't permit it. We may have beer and alcohol available at our offices, and you can choose to drink alcohol provided by Snowflake at company events, but use good judgment and never drink in a way that leads to impaired performance or inappropriate behavior, puts yourself or others in danger, or violates the law. You are strictly prohibited from driving a vehicle on Snowflake business (including transporting other Snowflakes to and from an event) while under the influence of alcohol, cannabis, non-medical or illegal drugs, or other controlled substances. Illegal and non-medical legal drugs in our offices or at sponsored events are strictly prohibited.

Protect Confidential Information and Intellectual Property

Confidential Information

We must protect all confidential information concerning Snowflake, as well as confidential information and personal information with which other parties like our customers, partners, vendors, and others have entrusted us. We must protect all information that is confidential in nature even if the information is not marked "confidential." Examples of confidential information are:

- financial data and projections, such as sales bookings, and pipelines;
- proprietary and technical information, such as trade secrets, patents, inventions, product plans, and prospect and customer lists;
- information about corporate developments, such as business strategies, plans for acquisitions or other business combinations, partnerships, major contracts, expansion plans, financing transactions, and management changes;
- personal information about individuals; and
- data (personal or otherwise) that our customers upload or import into our service for processing on their behalf (we have specific contractual and legal obligations with respect to this data).

If you have any questions about whether something is confidential, ask Legal.

Handling Snowflake's Confidential Information

In the course of your work, you will learn confidential information about Snowflake. As a general rule, you are prohibited from sharing Snowflake's confidential information with outsiders, even your close family or friends. This duty continues even if you leave Snowflake. Please see the non-disclosure agreement and Confidential Information and Invention Assignment (and, if you are based outside of the U.S., the employment contract) you signed when you joined Snowflake for more details.

Only share confidential information inside of Snowflake with people who actually need it to do their jobs. Only access or use Snowflake's confidential information for Snowflake's benefit. Protect it, and be careful not to reveal confidential information on the Internet, including through social media.

Sometimes you may need to share confidential information outside of Snowflake for a deal or project. Before doing so, make sure that the information is appropriate to share and that you have put safeguards in place to protect it (for example, a non-disclosure agreement is in place that covers Snowflake's confidential information, documents are marked "Confidential," and you are not sharing more than necessary). When sharing any confidential information outside of Snowflake, strictly follow our Information Security Policy and any other policies that apply to the specific type of information.

If you find yourself in a situation outside of a Snowflake deal or project where you think you may need to disclose confidential information (for example, you receive a subpoena or demand letter), contact Legal.

Handling Third-Party Confidential Information

In the course of your work, you may learn confidential information that belongs to or concerns other parties, like customers, prospects, job applicants, or partners.

When you have permission to use someone else's confidential information, handle it responsibly and follow any agreements we have with them. Specifically, you should:

- Follow any confidentiality obligations, including return or destruction obligations;
- Only use the information for the owner's intended purpose;
- When accessing any type of customer information, strictly follow our Information Security Policy and any other policies that apply to the specific type of information;
- Only share the confidential information with other Snowflakes who have a real business need to know it;
- Protect the information from being stolen or unintentionally released; and
- Do not take, accept, or use third-party confidential information without official permission. It goes without saying that you may not coerce or bribe anyone to share other companies' or individuals' confidential information.

You also need to follow any lawful confidentiality and non-use obligations that you have to companies you've worked with in the past. If you have or receive confidential information that you should not have, do not use it, access it, or delete it, and consult with Legal immediately.

Insider Trading

Never trade in the stock of Snowflake or any other company based on material nonpublic information that you know. This is not only a violation of Snowflake policy, it is illegal. You must also not "tip" a third party based on material nonpublic information. See Snowflake's Insider Trading Policy for more information.

Protecting Snowflake's Intellectual Property

Intellectual property is the heart of our business, and Snowflakes work extremely hard to create, market, and safeguard it. If we don't protect it, Snowflake risks losing its intellectual property rights and the critical competitive advantages they provide. Intellectual property covers many things, but common and valuable examples are our products and services, code, business strategy, customer and prospect lists, and trade names.

Protect our intellectual property by avoiding inappropriate disclosures (see "**Handling Snowflake's Confidential Information**" above). When disclosure is authorized, mark the information with a trademark, confidentiality, or patent legend (check with Legal if you're unsure about what to write). Please also refer to Snowflake's Data Classification Policy.

When you create new intellectual property on Snowflake's time or using Snowflake's resources, share it with your manager and the Legal Patents team so that Snowflake can decide whether to seek formal protection.

Information Security

Information security and data protection are core to our business. All of us must do our best to protect and maintain our and our customers' data (including personal data). It only takes one breach to cause serious damage to our business, reputation, and prospects.

With that in mind:

- Always secure your laptop, important equipment, files, and your personal belongings, even when you are at the office.
- Do not leave sensitive documents on your desk or on your computer screen when you walk away, even just for a minute.
- Only use company-issued USB drives. Do not plug any personal external drive into your Snowflake devices.
- Be paranoid in public. Don't work on a confidential presentation on a train or have a sensitive conversation while you're waiting in line at your local coffee shop.
- Don't modify or disable passwords or other security and safety features.
- Don't let anyone you don't know to be a Snowflake "tailgate" behind you through our doors, even if it feels a little awkward.
- Immediately report any security incidents (including lost, stolen, or accidentally distributed passwords, sensitive information, or confidential information) to security@snowflake.com.
- Report suspicious activity in the office to building personnel or the Workplace team.

Please see the Security Policies for more information.

AI, Data, and Privacy Compliance

We respect the privacy rights of our customers, suppliers, employees, and other people, and we follow applicable global data protection laws and contractual commitments that protect the information provided to Snowflake in the course of business or employment-related dealings.

We build data compliance and data privacy into our offerings and business operations to meet our data protection obligations. For example, when we process personal information on behalf of our customers, we comply with applicable data protection laws and contractual commitments, including following our customers' processing instructions. When we process personal information for our own purposes and operations, we follow our internal data privacy policies and comply with applicable data protection laws.

You have an obligation to:

- Keep personal information strictly confidential and observe appropriate security measures at

all times;

- Read and comply with Snowflake's Data Privacy Policies that apply to your role and responsibilities, including our Staff Personal Data Handling & Responsibility Policy;

- Read and comply with Snowflake's AI Policies and customer commitments, including Snowflake's AI Policy and AI Terms;

- Understand and respect commitments we make to our customers about their data, including access, use, and sovereignty requirements; and

- Only access and process (for example, collect, use, share, transfer, change, or store) personal information relating to Snowflake customers, personnel, vendors, and other third parties if you are authorized to do so and in order to meet a legitimate business purpose.

Snowflake Assets and Resources

We provide you with tools and technology you need to do your job. Please remember that these tools and technology (plus the work-related files on them) are Snowflake's or our licensors' property. To the extent permitted by law, Snowflake may monitor, access, and disclose communications and other information on Snowflake equipment, including laptops, our corporate electronic facilities or on our premises, with or without your knowledge or approval. Snowflake equipment should be used primarily for business purposes, although incidental personal use may be allowed, depending on the country. You may not use Snowflake assets or technology to violate corporate policy or the law. Please see Snowflake's Business Systems Use Policy for additional information.

Third-Party Software

Unsanctioned software and services present a significant security risk to Snowflake. All third-party software used for Snowflake business or installed on Snowflake equipment must be pre-approved by Security and IT and be appropriately licensed. You should never make or use illegal or unauthorized copies of any software, since doing so may constitute copyright infringement and may expose yourself and Snowflake to civil and criminal liability. You should never download or use any software or code that has not been approved by Security and IT. Please see the Vendor & Tool Assessment Process for more information.

Legal Notice to Employees

You are not prohibited or limited from filing a charge or complaint with, or otherwise communicating with or participating in any investigation or proceeding conducted by, any federal, state, or local government agency , commission, or entity ("**Government Agencies**") without giving notice to, or getting permission from, Snowflake (a "**Government Communication**"). You are also not prohibited from disclosing documents or other information pertaining to Snowflake to Government Agencies in the course of a Government Communication. Notwithstanding the foregoing, you should not disclose any Snowflake attorney-client privileged communications or attorney work product, unless you are an attorney and disclosure is permitted by 17 CFR 205.3(d)(2), applicable state attorney conduct rules, or other applicable law. You should take all reasonable precautions to prevent any unauthorized use or disclosure of

Snowflake confidential information to any parties other than the Government Agencies.

In addition, pursuant to the Defend Trade Secrets Act of 2016, you will not be held criminally or civilly liable under any federal or state trade secret law for any disclosure of a trade secret that (i) is made (A) in confidence to a federal, state, or local government official, either directly or indirectly, or to an attorney; and (B) solely for the purpose of reporting or investigating a suspected violation of law; or (ii) is made in a complaint or other document that is filed under seal in a lawsuit or other proceeding. Further, if you file a lawsuit for retaliation by Snowflake for reporting a suspected violation of law, you may disclose Snowflake's trade secrets to your attorney and use the trade secret information in the court proceeding if you: (y) file any document containing the trade secret under seal; and (z) do not disclose the trade secret, except pursuant to court order.

Nothing in this Code is intended to abridge your rights under the National Labor Relations Act or local equivalent.

Speak Together

You are a Snowflake ambassador. What you say or post may be attributed to Snowflake, whether or not you mean it that way. Make sure that you reflect Snowflake culture and values.

Keep the following Dos and Don'ts in mind when communicating with outsiders about Snowflake:

DOs	DON'Ts
DO disclose your Snowflake affiliation if you share industry content, and include a disclaimer that your views are your own **DO** disclose whether you are acting as a Snowflake representative **DO** remember that what you publish might be public for a long time, even if deleted **DO** tell Marketing about any potential problems or issues you find about Snowflake **DO** use good judgment when accepting any public speaking engagement	**Do NOT** share any confidential, proprietary, or personal information of Snowflake or that Snowflake is obligated to protect (e.g., customer confidential information) **Do NOT** speak as an official Snowflake representative unless specifically authorized **Do NOT** use Snowflake's name in any social media identity (handle, username, screen name, etc.) **Do NOT** provide references for Snowflake partners or reference Snowflake customers without prior approval from Marketing **DO NOT** permit Snowflake's name or logo to be used for commercial purposes without prior approval from Marketing

Public Statements and Speaking With Reporters

Do not speak on behalf of Snowflake, either publicly or off-the-record, unless you are authorized to (which, unless you are an executive officer or on the PR team, you probably aren't–sorry). Occasionally, you may be contacted by outside sources, like the press, requesting information about Snowflake, including Snowflake products and financial information or information about current or former Snowflake employees, directors, or customers. All of this is Snowflake's confidential information and may not be shared. If contacted, you must decline to comment; immediately contact the Marketing team for direction; and, even if the Marketing team does instruct you to respond, keep the Marketing team in the loop so they can direct all follow-up engagement.

Protect Snowflake's Brand

Snowflake has become a world-class brand. Make sure to protect it. It is important that we all speak with one strong and consistent voice. Stick to the script and avoid changing our official company messaging and positioning. Don't alter our logo. The Marketing team runs all design and merchandising projects (like gear and posters), even if they are only for internal use. If you have any questions about branding, please contact Marketing.

Social Media Guidelines

As your employer, Snowflake reflects on you and therefore strives to be a place where you are proud to work. Similarly, you reflect on Snowflake, and your social media activity or public statements can easily bleed into the workplace. We know that social media is ubiquitous and respect your right to engage in lawful activities outside of work, including using apps like X (formerly Twitter), Facebook, LinkedIn, and Instagram. However, what you say on social media or in public can affect the reputation of Snowflake or its employees. It can also amount to an inappropriate use of your work time or Snowflake's resources. As a result, when using your social media accounts and making public statements, you must follow applicable law and Snowflake's policies, including its policies on harassment and equal opportunity employment. You must also follow Snowflake's Business Systems Use Policy, which has rules about the use of Snowflake's resources (like your laptop).

Please see the Corporate Disclosure Policy for more information about public disclosures.

Outside Activities

As representatives of Snowflake, it is important that we all use good judgment and make honest and ethical decisions for our teams, our work, and for Snowflake.

Conflicts of Interest

Doing what's right for Snowflake is extremely important. If you base work-related decisions and actions on anything other than the best interests of Snowflake, you run the risk of undermining Snowflake's success. For that reason, you must avoid any activity that creates or appears to create an actual or potential conflict of interest. A conflict of interest is a situation in which your actions or loyalties are, or may be, divided between personal interests and Snowflake's interests, or between Snowflake's interests and those of someone else. Conflicts of interest can arise not only with outsiders, such as customers, partners, or vendors, but also with colleagues, such as your manager or other employees. You can also have a conflict as a result of a relationship with a family member, friend, or business with which you are connected.

Some conflicts of interest are obvious and easy to avoid, while others may not be so clear. Although no list can include every possible situation in which an actual or perceived conflict of interest could arise, the following are examples of common conflicts:

- working on outside activities, either alone or with others, that may compete with Snowflake or offer similar services as Snowflake;
- having an interest in a company that is or wants to become a Snowflake competitor, customer, supplier, or partner;
- soliciting contributions (including political or charitable) for a personal cause or initiative from a Snowflake business partner;
- hiring a vendor that is affiliated with, or has any financial relationship with, a friend or relative; and
- hiring a relative or a person with whom you have a close personal relationship.

If you have an interest in a transaction involving Snowflake—including an indirect interest through a relative, friend, or business—you must disclose it in writing to the General Counsel, refrain from pursuing the transaction, and follow any instructions you receive. In exceptional circumstances, the General Counsel may permit such a transaction to move forward. Snowflake may at any time rescind prior approvals or clearances to avoid a conflict of interest, or the appearance of a conflict of interest.

In certain cases, potential conflicts may require approval by the Board or a committee of the Board. For example, certain transactions that involve directors or executive officers of Snowflake require approval by the Audit Committee of the Board (the "**Audit Committee**") under our Related Party Transactions Policy. If a transaction requires approval or ratification under our Related Party Transactions Policy, then Snowflake will follow the review process under that policy and not this Code.

If a previously approved or ratified transaction has changed or expanded, you must promptly inform the General Counsel. If a transaction is properly approved or ratified (including approval or ratification under our Related Party Transactions Policy), it will not be deemed a waiver of this Code.

Outside Activities[2]

Outside activities present opportunities for perceived or actual conflicts of interest. If you are an employee or full-time contractor, you'll need preclearance from your VP and the Legal team for certain activities. Please see The Lift article called "Outside Activities" for information about which activities require preclearance and the process for getting it.[3] For example, preclearance is required before you can work for any affiliate, customer, partner, supplier, distributor, reseller, licensee, or competitor of Snowflake or any other business that does or seeks to do business with Snowflake. If the Legal team thinks that the activity creates an actual, potential, or apparent conflict of interest or would interfere with your job at Snowflake, you may be asked to decline or end the outside engagement if you would like to continue your relationship with Snowflake. You may not, and may not solicit other Snowflake employees to, use Snowflake time or resources to work on outside activities that would violate this Code.

Personal Investments

Generally, you may invest in the shares of public companies without creating a conflict of interest, as long as you own less than one percent. Investments in private companies are also usually allowed, but you must get permission from the General Counsel before you or members of your family or household make or hold a significant investment in or serve as a director of any private business that competes with, does business with, or seeks to do business with Snowflake (or invests in such companies). In those cases, or if any investment would create an actual, perceived, or potential conflict, you'll need to notify the General Counsel and follow the rules described above under **"Conflicts of Interest."**

Personal Business Opportunities

By law, as directors, officers, and employees, we each have a fiduciary duty to Snowflake to always act in the best interests of the company and take no action that would harm Snowflake. This means that you may not take personal advantage of business opportunities that you become aware of through your role as a Snowflake (or through your use of Snowflake resources or information). You may only pursue such an opportunity if Snowflake does not have an interest in the opportunity and you have written permission from the General Counsel after you have shared all of the facts.

[2] This section is not applicable to non-employee members of the Board.

[3] Indirect Personnel should discuss all of their professional outside activities with their manager.

Follow the Rules

Compliance with Law

Snowflake takes its obligation to follow the law very seriously. You should proactively make sure that you understand the laws and regulations that apply to your work. Each of us is personally responsible for complying with all applicable legal requirements and prohibitions. If you are doing business outside of the U.S., you must comply with applicable U.S. and local laws. You may not do business with a third party on behalf of Snowflake if you know or should know that it engages in illegal activities. If this Code or any other Snowflake policy conflicts with law, follow the law. Ask the Legal team if you have any questions or comments about the correct course of action.

A few specific laws are easy to violate unintentionally, and are highlighted in the rest of this section.

Integrity and Fair Dealing in the Marketplace

You must deal honestly, ethically, and fairly with Snowflake's suppliers, customers, competitors, and employees. Anything you say about Snowflake's products or services must be true, and must not be misleading, deceptive, or fraudulent. You must not take unfair advantage of anyone through manipulation, concealment, abuse of privileged information, misrepresentation, or any other unfair-dealing practice. You also must never create or submit false, inaccurate, or misleading invoices, receipts, or other financial or business-related documents, or accept money from an entity that you know is engaging in an illegal activity in a manner that may cause Snowflake to violate anti-money laundering laws.

The Foreign Corrupt Practices Act is a United States federal anti-bribery law that makes it unlawful for any U.S. citizen or any representative of a U.S. corporation to give *anything* of value to a foreign official in order to obtain or retain business (see "**Working with Governments–Improper Payments to Government Officials**" below). Most other countries also have laws designed to encourage and protect free and fair competition. These laws are broad and far-reaching and regulate Snowflake's relationships with its actual and prospective customers, partners, vendors, resellers, and distributors. Competition laws generally address the following areas: pricing practices (including predatory pricing, price fixing, and price discrimination), discounting, terms of sale, credit terms, promotional allowances, secret rebates, exclusive relationships, dealerships or distributorships, product bundling, restrictions on carrying competing products, termination, and many other practices. Please see our Anti-Corruption Policy for more information.

While Snowflake competes vigorously in all of our business activities, we are committed to dealing fairly with our customers and competitors, and conducting our global activities in accordance with all applicable laws, including competition laws. When representing Snowflake in the community, you are expected to compete energetically by promoting Snowflake on the merits. Product or service comparisons should be fair and accurate. Competition laws also govern relationships between Snowflake and its competitors. Collusion among competitors is illegal, and the consequences of a violation are severe. You must not propose, discuss, or enter into an agreement or understanding, written or oral, express or implied, with any competitor concerning, prices, discounts, or other terms or conditions of sale; profits or profit margins; costs; allocation of product, customers, markets or territories; limitations on production

or supply; boycotts of customers or suppliers; or bids or the intent to bid, or even discuss or exchange information on these subjects.

Gifts and Entertainment

Business gifts and entertainment are normal and can be a healthy part of business for non-government customers and partners. But gifts, meals, or trips that are extravagant or lack transparency or a legitimate business purpose may be viewed as bribes or as simply inappropriate. Generally, you are able to give and accept inexpensive "token" non-cash gifts and participate in occasional and moderate business meals and entertainment with prospective and actual non-government customers and partners. If you have any questions about whether any gifts or entertainment are appropriate, ask the Legal team first.

A problem can arise if you:

- receive a gift or entertainment that compromises, or could reasonably be viewed as compromising, your ability to make objective and fair business decisions on behalf of Snowflake;
- offer a gift or entertainment that is, or could reasonably be seen as, an attempt to obtain business through improper means or to gain any special advantage in our business relationships; or
- offer a gift or anything of value to a government entity or government employee.

No gift or entertainment should be given or accepted by any Snowflake, family member, or agent unless (i) there is no expectation of a favor, gift or action in return and (ii) it meets **ALL** of the following conditions:

- is not a cash gift (including gift cards that can be used at multiple business, like a Visa Gift Card);
- is consistent with customary business practices;
- is not excessive in value;
- cannot be construed as a bribe or payoff;
- does not violate any laws or regulations (such as applicable U.S. federal and state government gift and gratuity rules, the U.S. Foreign Corrupt Practices Act, and the UK Bribery Act);
- is not being given to or accepted from an employee, official, or agent of any government, political party, state-owned entity, or public international organization, without approval from Legal; and
- is not one of a series of small gifts or entertainments that can be construed as part of a larger, expensive gift.

All donations and some outside gifts require Legal pre-approval—see the "Outside Gifts, Meals, and Entertainment" article on The Lift for more information.[4] You must notify the Legal team if you receive or would like to give a gift that is excessive or unusual. It is also your responsibility to ensure that you

[4] Indirect Personnel should seek approval from their managers. As long as the gift or entertainment meets the requirements above and is within the Snowflake affiliate's authority to approve, then Snowflake Legal approval is not required.

comply with Snowflake's Global Travel and Expense Policy[5], Internal Gift Policy, and Anti-Corruption Policy.

See **"Working with the Public Sector–*Improper Payments to Public Sector Officials*"** below for important information about giving gifts or entertainment to, or receiving gifts or entertainment from, public sector officials.

Corporate Social Responsibility

Snowflake strives to comply with all applicable laws and respects internationally recognized human rights where we operate, and expects the same of our partners. All labor must be voluntary. We don't engage in child labor, forced, bonded, or indentured labor, involuntary prison labor, slavery, trafficking of persons, or physical punishment. We pay applicable legal wages under humane conditions. We comply with all applicable environmental laws and regulations. Please see the Anti-Human Trafficking Policy for more information.

[5] Indirect Personnel should follow their direct employers' policies with respect to travel and expenses and gifts. Snowflake's Global Travel and Expense Policy and Internal Gift Policy do not apply to them unless expressly stated.

Financial Records

We are required to follow strict accounting principles and standards, to maintain financial information accurately and completely, and to have appropriate internal controls and procedures to ensure that our accounting and financial reporting complies with law. Snowflake's financial and other disclosures must be full, fair, accurate, timely, and understandable.

Compliance with Rules, Controls, and Procedures

All transactions must be properly recorded, classified, and summarized in our financial statements, books, and records in accordance with our policies, controls, and procedures, as well as all generally accepted accounting principles, standards, laws, rules, and regulations for accounting and financial reporting (together, "**Accounting Rules**"). If you have responsibility for or any involvement in preparing financial or accounting records, you must understand and follow the relevant Accounting Rules. If you are a VP or higher, you must ensure that appropriate internal controls and procedures in your business area are in place, understood, and followed.

Accuracy of Records and Reports

Snowflake relies on records and reports to have complete, accurate, and timely information to make good decisions. Anyone involved in preparing financial or accounting records or reports, including financial statements and schedules, must make sure that those records and reports are complete, accurate, and timely. Anyone representing or certifying that records and reports are accurate should first make an inquiry or review adequate backup information to establish a good faith belief in their accuracy.

Even if you are not directly involved in financial reporting or accounting, you are probably involved with financial records or reports of some kind—a certification voucher, timesheet, invoice, or expense report. In addition, most employees have involvement with product, marketing, or administrative activities, or performance evaluations, which can affect Snowflake's financial condition or results that we may share from time to time. Therefore, Snowflake expects everyone to make sure that business records and reports are accurate, complete, and reliable.

If you believe that any financial record is misleading or if you become aware of any material information that you believe should be disclosed, you must bring this information to the attention of the Legal team or the Controller. If you believe that questionable accounting or auditing conduct or practices have occurred or are occurring, notify the General Counsel immediately.

Intentional Misconduct

You may not intentionally misrepresent Snowflake's financial performance or otherwise intentionally compromise the integrity of Snowflake's reports, records, policies, or procedures. For example, you may not:

- report information or enter information in Snowflake's books, records, or reports that fraudulently or intentionally hides, misrepresents, or disguises the true nature of any financial or non-financial transaction or result;
- establish any undisclosed or unrecorded fund, account, asset, or liability for any improper

purpose;

- enter into any transaction or agreement that accelerates, postpones, or otherwise manipulates the accurate and timely recording of revenues or expenses;
- intentionally misclassify transactions as to accounts, business units, or accounting periods;
- intentionally create any false or misleading records or documentation; or
- intentionally assist others in any of the above.

Dealing with Auditors

Our auditors have a duty to review our records in a fair and accurate manner. You must cooperate with independent and internal auditors in good faith and in accordance with law. In addition, you must not fraudulently induce or influence, coerce, manipulate, or mislead our auditors about financial records, processes, controls, procedures, or other matters. You may not engage, directly or indirectly, any outside auditors to perform any audit, audit-related, tax, or other services, including consulting, without prior approval from the Controller or Chief Financial Officer.

Obligation to Investigate and Report Potential Violations

You must report any of the following things to the Controller or the General Counsel:

- financial results that you have reason to believe are inconsistent with underlying business performance;
- inaccurate financial records, including travel and expense reports, timesheets, or invoices;
- the circumventing of mandated review and approval procedures;
- transactions that appear inconsistent with good business economics;
- the absence or weakness of processes or controls; or
- persons within Snowflake seeking to improperly influence the work of our internal or external financial or accounting personnel, or auditors.

Dishonest or inaccurate reporting can lead to civil or even criminal liability for those involved and Snowflake, damage our reputation, and lead to a loss of trust in Snowflake. Immediately report any case of suspected financial or operational misrepresentation or impropriety. Please see the Whistleblower Policy for more information.

Government and Regulatory

Working with the Public Sector

Special rules apply to our business and other dealings with the public sector, which includes governments, state-owned enterprises, quasi-governmental entities, and publicly-funded institutions. If you are involved in business with the public sector, it is critical that you read the Public Sector Code of Conduct and Ethics to ensure that you understand the complex rules that often apply to these types of customers. This section describes a few of the more common issues.

Public Sector Contracts

Selling to the public sector is often extremely complex, highly regulated, and subject to more risks compared to commercial customers. As a result, we must take special care when we sell to, or do business with, the public sector. It is important to accurately represent Snowflake, and avoid improperly soliciting or obtaining confidential information, such as sealed competitors' bids, from government officials prior to the award of a contract. Special processes apply when bidding for and signing agreements with public sector customers, and it's your responsibility to learn and follow them. See the Public Sector Code of Conduct for more information.

Improper Payments to Public Sector Officials

You may not bribe anyone for any reason, whether in dealings with governments or the private sector. Offering gifts, entertainment, business courtesies, or anything of value to a public sector entity or official could be perceived as a bribe. Several laws around the world, including U.S. state and federal government gift-giving restrictions, the U.S. Foreign Corrupt Practices Act and the UK Bribery Act, specifically prohibit offering or giving a gift to public sector officials or public sector entities to influence official action or to secure an improper advantage. In this context, a "gift" is anything of value and includes things like meals, travel, political or charitable contributions, and job offers (including jobs for family and friends of governmental officials). Never give gifts to public sector officials without Legal pre-approval. Please see the Anti-Corruption Policy and "Outside Gifts, Meals, and Entertainment" on The Lift for more information.

Hiring Public Sector Officials

Special laws may apply to hiring current and former public sector officials. For example, there are limitations on how we may recruit or hire public sector officials who were involved in Snowflake public sector contracts. In addition, public sector officials may be subject to ethics opinions which limit their work in the private sector. Contact Legal before discussing potential Snowflake employment with a current public sector official.

Requests by Regulatory Authorities

Refer all government requests for Snowflake information, documents, or investigative interviews to Legal immediately.

Political Contributions

Snowflake's assets—including funds, volunteer time during Snowflake hours, premises, and equipment—must not be used for, or be contributed to, political campaigns or political activities without

the General Counsel's prior written approval. A political contribution isn't limited to donating money to a candidate. It also includes non-monetary contributions–sometimes called "in-kind" contributions–which are anything of value, like hosting a fundraiser or donating your time.

Additionally, "pay-to-play" laws may limit or prohibit you from making personal political contributions to U.S. state and local public sector entities. To ensure that you and Snowflake remain compliant with applicable political contribution laws, certain directors, officers, or employees on the Snowflake teams that support public sector customers must comply with the U.S. State and Local Political Contribution Policy.

Third Party Lobbying

Snowflake may communicate its position on important issues to elected representatives and other government officials. It is Snowflake's policy to comply fully with all applicable laws regarding political contributions and lobbying. If you'd like to work with a third-party lobbyist, please follow the pre-approval process at "Lobbyist Engagement Process" on The Lift.

Export Controls and Denied Persons

U.S. and international trade laws control (a) where Snowflake may send or receive its products and services; (b) which employees can access certain technologies; and (c) to whom Snowflake may sell its products and services. Trade laws are designed to ensure that transfers of products, services and technology are accomplished in a manner that is consistent with national security and foreign policy goals. The laws are complex, and apply to:

- imports and exports from or into the U.S.;
- imports and exports of products from or into other countries, with additional concerns when those products contain components or technology of U.S. origin;
- exports of services or providing services to non-U.S. persons;
- exports of technical data or providing technical data to non-U.S. persons, especially when the technical data is of U.S. origin.

What constitutes an "import" or "export" is broad, and includes tangible shipments, as well as deliveries of electronic software, services and support. For example, the following situations can all constitute exports and imports under U.S. law:

- exposing or allowing access by non-U.S. persons to U.S. technical data or certain technology, regardless of what country the exposure occurs in (including in the U.S.) (for example, persons from countries designated by the U.S. government (currently North Korea, Iran, Syria, and Cuba) should not access our encryption technology without special permission from the government);
- non-U.S. persons offering support to a customer whose data is subject to export control restrictions;
- sending a server from one country into another country;
- permitting software to be downloaded or used in a different country;
- transporting technical data or software on your laptop, phone, or equipment in your luggage to another country; and

- direct or indirect payments to a U.S. government sanctioned bank.

In addition, as of the date this Code was last amended, we are prohibited from procuring goods or services from, and selling goods or services to, entities and individuals in –the Crimea, Luhansk, and Donetsk Regions of the Ukraine, Belarus, Cuba, Iran, Russia, Syria, and North Korea, as well as individuals and entities designated on U.S. government Denied Party Lists. In addition, you may not conduct business in, work from, or bring any Snowflake assets (like your laptop) to the countries listed on the High Risk Countries Policy. These lists are subject to change.

In sum, if you are involved in sending or making available Snowflake products, services, software, or any form of technical data from one country to another, work with Legal to make sure that the transaction complies with applicable export and other laws.

Administration, Waiver, and Amendment

Snowflake Inc.'s Board has adopted this Code and oversees compliance. This Code may be amended by the Board or the Audit Committee; however, non-material amendments (for example, updates to the whistleblower hotline provider, references to new or amended policies, or policy locations) may be approved by the General Counsel. Any transaction that would normally require CEO approval will instead require Board approval if the transaction relates to the CEO, and any transaction that would normally require General Counsel approval will instead require CEO approval if the transaction relates to the General Counsel (in each case, in addition to any other approvals required). Any waivers of this Code must be approved in writing by the General Counsel or, with respect to executive officers or members of the Board, by the Audit Committee. Any waiver will be reported as required by federal securities laws and applicable stock exchange rules, if applicable. Any matter which has been approved in accordance with the processes set out in or referenced by this Code will not be considered a waiver.

Adoption and Amendment History:

Adopted by the Board of Directors, effective as of October 1, 2018.
Amended by the Audit Committee, effective as of August 21, 2020.
Amended by the Audit Committee, effective as of August 23, 2021.
Amended by the Audit Committee, effective as of August 22, 2022.
Amended by the Audit Committee, effective as of August 21, 2023.
Amended by the Audit Committee, effective as of August 19, 2024.
Amended by the Audit Committee, effective as of August 25, 2025.

ACKNOWLEDGEMENT OF RECEIPT OF CODE OF BUSINESS CONDUCT AND ETHICS

I have received and read Snowflake's Global Code of Conduct and Ethics (the "**Code**") and all other policies referred to therein (together with the Code, the "**Policies**"). I understand the standards and policies contained in the Policies and understand that there may be additional policies or laws specific to my job. I understand that Snowflake Inc.'s Board of Directors or its designees may update the Policies from time to time, and I agree to comply with the Policies (including all future updates). I understand that my failure to comply with this Code may result in disciplinary measures up to and including termination.

If I have questions concerning the meaning or application of the Policies, any other Company policies or procedures, or the legal and regulatory requirements applicable to my job, I know that I can consult with Snowflake's Legal or HR teams.

Name: _____

Signature: _____

Date: _____