



# Code of Ethics



# Contents

Commvault Systems, Inc. and its affiliates and subsidiaries (“Commvault”) established this Code of Ethics (the “Code”) which serves as a comprehensive guide to appropriate conduct and touches on various important issues like human rights and data privacy. For detailed policies, including those referenced in the Code, refer to [Connect](#), the [Trust Center](#), or reach out to [Compliance Team](#) for further information.

INTRODUCTION FROM SANJAY MIRCHANDANI	03	WE CONNECT	04	WE INSPIRE	06
		Personal Dignity and Respect	04	Honest and Ethical Conduct and Fair Dealing	06
		Conflicts of Interest	05	Anti-Corruption and Anti-Bribery	06
		Cybersecurity	05	Insider Trading	06
				Providing Company Information	07
WE CARE	12	WE DELIVER	15	Gifts and Entertainment	07
Following the Letter and Spirit of the Law	12	Use of Intellectual Property and Proprietary Information	15	Political Contributions	08
Human Rights	12	Software Code of Ethics	16	Charitable Contributions	08
Anti-Money Laundering	13	Protection of Corporate Assets	16	Social Responsibility and Sustainability	08
Antitrust and Competition Laws	13	Social Media and Other Online Activity	17	Records and Money	09
Global Trade	14	Assistance With Audits	17	Public Disclosure	09
				Safeguard Good Name and Reputation	10
SPEAK UP. ASK FOR GUIDANCE AND VOICE CONCERNS.			18	Confidential Information	10
				Data Privacy	10
				Responsible AI	11



We Connect.  
We Inspire.  
We Care.  
We Deliver.

These core values shape how we do business with our customers, partners, government agencies, and fellow team members all over the world.

## CODE OF ETHICS

This Code is a living, breathing document that establishes our legal and ethical standards of behavior, and supports our commitments to human rights, respectful treatment of others and equal opportunity.

We all have a shared responsibility to speak up and report any behaviors or actions inconsistent with this Code. We investigate all reports of misconduct and ensure there is no retaliation against individuals who report in good faith. While situations can sometimes present unique or complex challenges, our belief is simple: Do the Right Thing. If you aren't sure what that is, that's fine, you can always ask for help.

Please take the time to read and understand this Code and apply it to your everyday business activities. In doing so, you are helping Commvault to remain a successful company, rooted in integrity and trust, a source of pride for all of us and a driver of our continued success.

Sincerely,

**Sanjay Mirchandani**  
President, Chief Executive Officer  
& Director, Commvault





# We Connect.

---

"We are committed to fostering an inclusive workplace where talented people thrive."

## CODE OF ETHICS

### Personal Dignity and Respect

Personal integrity, practiced daily, is the foundation of corporate integrity. We are all expected to always act with honesty and strong moral principles. We should operate with the highest standards of individual and corporate ethics. To that end, each of us is personally responsible for supporting Commvault's core values.

We are committed to providing a work environment free of discrimination and harassment on the basis of race, color, national origin, sex, gender, gender identity or expression, sexual orientation, marital status, registered domestic partner status, citizenship status, religion, age, physical or mental disability, medical condition, genetic characteristics and information, ancestry, military and veteran status, or any other category. We give equal employment opportunity to all individuals in compliance with legal requirements because it's the right thing to do.

We are committed to fostering an inclusive workplace where talented people work, thrive, contribute to Commvault's success, and develop their careers and the careers of our colleagues. Supporting a diverse, engaged workforce allows us to be successful in building trust, empowering teams, and delighting our customers. Refer to our [Respect at Work Policy](#) for more details.



# We Connect.

"We operate with the highest standards of individual and corporate governance."

## CODE OF ETHICS

### Conflicts of Interest

A conflict of interest occurs when one's personal interests influence or could appear to influence one's ability to act in the best interest of the Company. We address conflicts of interest in an ethical manner to ensure the decisions we make involving Commvault are in the best interest of the Company. Our personal interests can affect our decisions even when we think they will not, and even the appearance of conflicts of interest can have a negative impact on the Company. We endeavor to avoid any real, potential or perceived conflicts of interest by communicating in a fair, transparent and timely manner. If any actual or potential conflict of interest is identified, it should immediately be disclosed to [Advisor-Approvals@commvault.com](mailto:Advisor-Approvals@commvault.com).

You have a conflict of interest if:

- Your actions or interests could prevent you from performing your duties in an honest, objective, and effective manner
- You have an incentive to benefit yourself, your friends, or family at Commvault's cost
- You, your friends, or family receive improper benefits as a result of your position at Commvault

Whether a conflict of interest exists is not always clear. When in doubt, please discuss the particular situation with your manager or navigate to the section [Ask Questions](#) section of this Code for additional ways to clarify responsibilities and obtain guidance.

### Cybersecurity

At Commvault, security is a shared responsibility. It is crucial to be aware of Commvault's information security and data protection policies and to remain vigilant against potential threats to our information, systems and customer-facing platforms. If you encounter suspicious emails (phishing), report them by using the 'Phish Alert Report Button' in Outlook or by emailing [phish@commvault.com](mailto:phish@commvault.com). For any other suspicious or concerning activities, report details to [Helpdesk](#).

Employees must use Company networks, devices, and resources responsibly and in accordance with security policies. Accessing unauthorized or high-risk online environments can expose the company to cybersecurity threats, data breaches, and legal risks. Any misuse may result in disciplinary action, up to and including termination. Employees should refer to the [Acceptable Use Policy](#) and [Information Security Policy](#) for detailed guidelines on the proper use of Company technology and data protection measures.





# We Inspire.

---

“What if I’m uneasy about something a customer or supplier asks us to do?”

Trust your instincts. If it doesn’t feel right, it probably isn’t. You can contact our [Compliance Team](#) anytime to help guide you through tough situations.

## CODE OF ETHICS

### Honest and Ethical Conduct and Fair Dealing

We deal honestly, ethically, and fairly with our customers, competitors, suppliers, and each other. We have an absolute commitment to treat others with dignity, respect, and equal opportunity. We conduct our business with honesty and integrity, and we expect our business partners’ values and business practices to mirror ours regarding compliance with the law, product quality, safety, human rights, treatment of employees, and environmental compliance. We are and aim to always be a company that is known for doing the right thing.

### Anti-Corruption and Anti-Bribery

We are committed to acting professionally, fairly and with integrity at all times. We never engage in bribery, kickbacks, or corruption. Under the Foreign Corrupt Practices Act (FCPA) and other applicable anti-bribery and anti-corruption laws, companies can be held responsible for the actions of third parties engaged to act on their behalf, even if the entity is unaware or does not approve of the third party’s actions. For that reason, employees should set clear expectations that third parties must adhere to anti-bribery and anti-corruption laws, and may need to ensure compliance from their subcontractors, consultants, agents, or representatives. Refer to the [Anti-Bribery and Anti-Corruption Policy](#) for more details.

### Insider Trading

Trading in securities based on material, non-public information about Commvault or other companies, or providing such information to others to trade our or other companies’ securities, is prohibited by law. Information is material if a reasonable investor might consider it important in deciding whether to buy or sell stock. Information is non-public until it has been appropriately disclosed to the public (such as through a public filing with the government, press release, or other appropriate public disclosure via the website).



# We Inspire.

## CODE OF ETHICS

Commvault's trade restriction windows, otherwise known as blackout periods, occur at regular intervals starting at close of market on the 15th day of the last month of the fiscal quarter and ending at close of market on the second trading day after the release of quarterly earnings, and from time to time, as circumstances arise. The general guideline to keep in mind is if the Company is in a blackout period, or a team member has material non-public information, buying or selling the Company securities is not permitted.

Refer to our [Insider Trading Policy](#) for details. If you are unsure about the legalities of any purchase or securities sale reach out to the Legal team at [legal@commvault.com](mailto:legal@commvault.com).

## Providing Company Information

From time to time, stock analysts or consultants may contact current or former employees and offer to pay them for information or insights about Commvault. It is a breach of confidentiality to share information about Commvault that is not public and may not be publicly known, particularly for the purpose of gaining an investment edge. Participating in these schemes is a violation of insider trading laws. Should you be contacted for this purpose, decline to share any information and promptly inform the Company spokesperson and the [Compliance Team](#).

## Gifts and Entertainment

We understand that building relationships with customers, partners, and vendors is occasionally accomplished in social settings. Business gifts and entertainment on behalf of Commvault must always be guided by common sense and moderation. The Company permits gifts and entertainment including meals, travel, hotel accommodation, and experiences (e.g., concerts, sporting events, etc.) to business associates including government officials, under controlled circumstances. Business courtesies should always be reasonable and should never give the impression of any special treatment.

Due to the stringent gifting restrictions within the public sector, we recommend excluding public sector partners and customers from gifting activities, unless explicit exceptions are granted. Refer to the [Gifting and Entertainment Guidelines](#) for more information. All gifts and entertainments must comply with the Commvault's [Anti-Bribery Anti-Corruption Policy](#).



# We Inspire.

## CODE OF ETHICS

### Political Contributions

We are committed to fostering a “politics-free” environment at Commvault. Commvault funds are not used to support any political party, political committee, or candidate and strictly adheres to all laws governing campaign contributions in any federal, state, or local election in any country. Employees are free to use their own funds to make individual political contributions in accordance with applicable law. Commvault will not provide reimbursement in any form for political contributions.

Commvault remains politically neutral and prohibits personnel from making political contributions on its behalf, whether directly or indirectly.

### Charitable Contributions

We embrace our responsibility to the community at large. Being an active participant in our communities where our employees live, and work is integral to who we are. This commitment is exemplified by the number of Commvault employees involved in charitable organizations around the world, as well as the support we provide to these organizations. Our commitment is more than a corporate program; it’s part of the people and the culture at Commvault. To ensure transparency, all charitable contributions and sponsorships are reviewed for bribery or corruption risks.

To learn more about Commvault’s philanthropic programs, refer to the [Corporate Social Responsibility Report](#). Employees interested in participating may also reach out to [HR](#) for more information.

### Social Responsibility and Sustainability

Commvault recognizes the significant impact we can have on our communities and our planet. Our approach to Corporate Social Responsibility (CSR) is deeply rooted in our core values, focusing on our planet, people, and communities as key stakeholders. We are committed to embedding sustainability across our organization and beyond, whether we’re reducing the carbon footprint of our customers through our innovative solutions or giving back to our communities we serve. We continue to believe long-term sustainability isn’t just responsible or beneficial for our business; it’s essential. Sustainability is integral to our culture and is reflected in our products, customer interactions, and employee engagement. For additional information, see our [CSR Report](#).





We  
Inspire.

## CODE OF ETHICS

### Records and Money

We must report all business transactions honestly, accurately, and promptly, taking full responsibility for the accuracy of our records and reports. Accurate information and reporting are essential to Commvault's ability to meet legal and regulatory obligations. Commvault's policy is to provide full, fair, accurate, timely, and understandable disclosure in reports and documents filed with, or submitted to, the Securities and Exchange Commission and in other public communications. Team members may not enter into side agreements on behalf of the Company, whether written or verbal, which are intended to alter or provide additional terms, conditions, or commitments that are not reflected in the actual agreement with a third party.

We are required to accurately account for all Commvault money and only spend such money on lawful, Commvault-related purposes. If our duties involve verification of expenditures or requests for reimbursement, we are each responsible for verifying that our expenditures legitimately comply with Commvault policies and applicable laws and that the amount of reimbursement received is accurate. We are each responsible for safeguarding Commvault assets, and, therefore, we need to ensure proper accounting of expenses incurred and accurate payment of reimbursement requests. All requests for reimbursement should be submitted in a timely manner and be supported by original receipts. In addition, our expenditures must be properly recorded and comply with all applicable Commvault policies, including the Travel and Expense Reimbursement Policy.

### Public Disclosure

All public communications, including filings with the Securities and Exchange Commission, must be accurate, timely, and clear. If you or any team member becomes aware of any material information or omission that may make our public disclosure misleading or inaccurate, bring that information to the attention of the Chief Accounting Officer, Chief Financial Officer, or Chief Trust Officer.



# We Inspire.

## CODE OF ETHICS

### Safeguard Good Name and Reputation

Commvault's good name is in your hands. We should always conduct ourselves in a manner that is consistent with protecting the Company's good name and reputation. To that end, do not make, or cause others to make, any false, disparaging, or derogatory statements in public or private to any person, entity, media, or social media outlet regarding Commvault's products, business affairs, financial condition, or relationship with any of its customers and partners.

### Confidential Information

We are dedicated to safeguarding the confidentiality of sensitive information to build and sustain the trust of our customers and partners. This commitment extends to protecting both our own confidential data and the information entrusted to us by third parties. Refer to the [Information Classification Policy](#) for more details.

Confidential information belonging to Commvault, or any other entity should only be shared with team members who need it to perform their job duties.

Do not discuss internal confidential information to anyone outside of Commvault unless it is required for your role and an appropriate confidentiality agreement is in place. This applies particularly to inquiries concerning Commvault from the media, investment professionals (e.g., analysts, investors, brokers), security holders, or via social media. If approached with such inquiries, refrain from commenting and direct the inquirer to one of our official spokespersons.

### Data Privacy

Data is always at our fingertips; it's the lifeblood of our business. In doing our part to honor the right to privacy and protect personal data, all Commvault employees and contractors are bound by the requirements set forth in Commvault's Data Protection Program, grounded in the EU's General Data Protection Regulation and other applicable data privacy laws.



# We Inspire.

## CODE OF ETHICS

Whether we are administering employee benefits, designing a new product, providing customer support, or procuring a third-party service, we must be sure to follow these key principles when handling and sharing personal data:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidence
- Accountability

Refer to our [Privacy Policy](#) for details. If you have any questions, contact our [Global Privacy Office](#).

## Responsible AI

At Commvault, we are committed to using Artificial Intelligence (“AI”) responsibly and ethically. All Commvault employees and contractors are bound by the principles set forth in Commvault’s AI Governance Policy, which requires that our AI systems are designed and deployed with fairness, inclusivity, and transparency.

Whether developing AI-powered products or integrating third-party AI technologies, we adhere to these key principles:

- Transparency and explainability
- Reliability, safety, and control
- Fairness and bias mitigation
- Human-centered approach
- Data privacy and security
- Accountability and governance

Refer to our [AI Governance Policy](#) for details. If you have any questions, contact the [Compliance Team](#).



# We Care.

“Use good judgment and when in doubt, ask for help. You can always seek advice from your manager, our Chief People Officer or our Chief Trust Officer.”

## CODE OF ETHICS

### Following the Letter and Spirit of the Law

We must comply with all applicable laws, rules, and regulations. Use sound judgment and seek guidance in unfamiliar situations. Any known violations by Commvault or by its employees should be promptly reported through the designated Reporting Channels.

While we always strive to resolve issues internally, you should not feel discouraged from reporting illegal activities to an appropriate authority when necessary. Employees reporting a violation in good faith must not be discharged, demoted, suspended, threatened, harassed, or in any other manner retaliated or discriminated against. This Code is not intended to, and should not be construed to prevent you from engaging in concerted activity protected by the rules and regulations of the National Labor Relations Board (or government labor agency or board in your jurisdiction), or from testifying, participating, or otherwise assisting in any state or federal administrative, judicial, or legislative proceeding or investigation.

### Human Rights

Commvault is committed to the protection and preservation of human rights around the world. Our commitment to human rights is embedded in the culture and values that define our company and is reflected in our policies and actions toward our employees, partners, suppliers, and the communities and countries where we do business.

We require our customers and business partners to exhibit respect for fundamental human rights and human dignity and respect the equal rights of men and women while doing business with us. We are committed to an inclusive, safe, and ethical work environment, as demonstrated within our [Human Rights Policy](#), [Environmental Management Policy](#), [Health and Safety Policy](#), and [Supplier Code of Conduct](#).

Commvault strictly prohibits the use of child labor and forced labor in any form. All employees, contractors, and business partners must





We  
Care.

## CODE OF ETHICS

comply with applicable laws and regulations regarding minimum working age and ensure that no individual is subjected to involuntary or exploitative labor practices.

### Anti-Money Laundering

Commvault is committed to the fight against money laundering. It is an issue we take extremely seriously, and it continues to be a critical focus for governments, international organizations, and law enforcement agencies worldwide.

Money laundering is the process of concealing illicit funds or making them look as though they are legitimate. This includes concealing the criminal origin of money or other property – sometimes called the proceeds of crime – within legitimate business activities. It also covers the use of legitimate funds to support crime or terrorism.

We never condone, facilitate, or support money laundering, which means:

- We will always comply with anti-money laundering laws and regulations, including identifying clients, monitoring client activity, and reporting suspicious or unusual activity consistent with applicable laws.
- We will seek to minimize money risks through our anti-money laundering practices. These are designed to avoid receiving or being involved in an arrangement or transaction that relates to funds that may be the proceeds of crime.
- We take reasonable and appropriate actions to identify and assess the integrity of our business partners. We should be vigilant and exercise good judgment when dealing with unusual customer transactions.

Each one of us have a responsibility to actively safeguard our brand, products, and services from being used for money laundering.

### Antitrust and Competition Laws

Commvault supports free and fair competition. We do not engage in any conduct that would unfairly and unlawfully diminish competition in the marketplace. To ensure markets operate fairly and efficiently, many nations have implemented laws to prohibit anti-competitive practices. While antitrust and competition laws are complex, they generally forbid entering into formal or informal agreements or understandings regarding activities that may restrict competition.



# We Care.

“Where can I go to get more information about our global trade compliance program?”

Check out our [Sanctions Guide](#) for more information or contact [compliance@commvault.com](mailto:compliance@commvault.com) with any questions.

## CODE OF ETHICS

Examples of conduct that is generally prohibited under the antitrust and competition laws and this Code include:

- Agreements among competitors about price or margin.
- Agreements among competitors to allocate markets or customers.
- Coordinating agreements among customers not to make deals with competitors.
- Unlawful restrictions on resale.
- Sales unlawfully conditioned on agreements to purchase other products.
- Exchanging commercially sensitive information with competitors, even if there is no agreement of any kind.

## Global Trade: Export Controls, Restricted Countries, Imports, and Boycotts

Commvault complies with all applicable global trade laws and regulations. Each employee and the company site involved in the cross-border transfer of any goods, technology, or other items has the responsibility to ensure that our activities are conducted in compliance with all applicable import and export laws.

The U.S. and other governments impose sanctions or otherwise restrict transactions with certain individuals, entities, countries and territories. There are broad prohibitions on virtually all transactions with certain countries or territories subject to comprehensive sanctions or embargoes, as well as with their governments, entities, and residents. All Commvault employees worldwide must comply with applicable prohibitions or limitations on transactions with sanctioned or restricted parties and countries.

Governments may also attempt to advance their political agendas by pressuring companies to boycott the products or companies of other nations. U.S. anti-boycott laws forbid Commvault from agreeing or complying with unsanctioned boycott requests, whether oral or in writing. Commvault is also required to report these requests to the U.S. government. If we receive any requests to support an unsanctioned boycott, we must ignore, or, in some cases, strike or remove the requests from the documents in which they appear and report them to our managers and the [Compliance Team](#). Refer to the [Sanctions Guide](#) for more information about how we comply with global trade laws.



# We Deliver.

**"I don't work in IT or Sales, how does protecting intellectual property apply to me?"**

As representatives of a technology company, we must respect the value of software licenses and intellectual property. Every employee plays a part in the protection of our proprietary information.

## Use of Intellectual Property and Proprietary Information

Commvault's intellectual property (patents, copyrights, trademarks, trade secrets) and other proprietary information are valuable assets. Protecting these assets, including documenting their creation and maintaining their secrecy, is critical to Commvault's continued success. Patentable inventions include new and useful products, compositions, devices, methods, and techniques. Trademarks include words or symbols used to identify the entity and its products and services. Copyrights protect creative expression but can include works such as software product labels, manuals, and website content. Trade secrets include data or information that is treated as secret, derives value from not being known outside Commvault, and that is unavailable to those outside Commvault except under confidentiality agreements. Proprietary information includes data or other information that has been developed or assembled on Commvault's (or a third party's) time or at Commvault's (or a third party's) expense and is non-public or not easily determined or re-created by others.

It is our duty to protect Commvault's intellectual property and proprietary information and not share such information with anyone outside or within Commvault who is not authorized to receive and does not have a business need to receive that information.

All material used in the course of our business that is protected by the intellectual property rights of others must be appropriately used with permission from the third party that owns or controls such rights. Questions about whether permission is needed, or whether the material may already have been licensed by Commvault, should be directed to the [Compliance Team](#).



# We Deliver.

## CODE OF ETHICS

### Software Code of Ethics

As representatives of a technology entity, it is vital that we respect the value of software licenses and the underlying intellectual property in software, whether Commvault software or third-party software we use in the scope of our work. Unauthorized duplication of copyrighted computer software violates the law and is contrary to Commvault's standards of conduct. Commvault adheres to the following principles:

- Commvault will provide and use legally acquired software to meet legitimate software needs in a timely fashion and in sufficient quantities for its needs.
- Commvault will comply with all license or purchase terms regulating the use of any software it acquires or uses.
- Commvault will enforce internal controls to prevent the making or using of unauthorized software copies, including effective measures to verify compliance with these standards and appropriate disciplinary measures for violation of these standards.

If you have questions, please contact Commvault's Chief Technology Officer.

### Protection of Corporate Assets

All team members play a role in protecting Commvault assets and using those assets efficiently and appropriately. Assets provided to team members or paid for by Commvault, including desktops, laptops, mobile devices, and data stored within them, remain the exclusive property of Commvault. Theft, carelessness, and waste have a direct impact on Commvault's financial performance. Report loss of any Commvault device or data to your manager and the Information Technology department.

Keep in mind that Commvault's intellectual property includes not only patents and trademarks, but also trade secrets, know-how, and other product and technical information that is not publicly known. Protection of this intellectual property is critical to Commvault's continued success. Use care not to disclose this information purposefully or inadvertently to parties outside of Commvault. There may be instances when disclosure of intellectual property to third parties is appropriate, in which case team members should seek guidance from [Commvault's Compliance Team](#) prior to any such disclosure to ensure that appropriate protections are in place.





# We Deliver.

## CODE OF ETHICS

### Social Media and Other Online Activity

Employees using social media are responsible for ensuring that their activities align with Commvault policies, as well as applicable laws and regulations. Social media use is not required for employment unless specified with clear guidelines. Only personnel authorized by the Company's Chief Marketing Officer (CMO), Chief Financial Officer (CFO) and/ or Chief Trust Officer, may publish content to the official company social media accounts or make official statements on behalf of Commvault.

Confidential information, including trade secrets, financials, personal data, and material non-public information as defined in the Commvault's Insider Trading Policy, must not be shared on social media.

Content posted to Company Accounts or about Commvault on social media must reflect Company's values and ethics. It must be factual and respectful. Personnel must avoid commenting on sensitive topics like legal or financial issues, business strategy etc. Refer to our [Global Social Media Policy](#) for more information.

### Assistance With Audits

Our commitment to accurately and honestly reporting Commvault's business transactions depends on maintaining an open and transparent relationship with independent auditors. No team member shall, directly or indirectly, make or cause the making of a materially false or misleading statement to an accountant in connection with any audit, task, review, or examination of Commvault's financial statements or the preparation or filing of any document or report with the Securities and Exchange Commission.

If you have a concern or complaint regarding an accounting, auditing, internal accounting control or task matter, you may confidentially and anonymously submit those concerns or complaints in writing at the addresses provided at the end of this Code. Any such concerns or complaints may also be communicated confidentially and, if you desire, anonymously, pursuant to our [Ethics and Integrity Reporting Policy](#). All complaints will be reported to the Audit Committee of the Board of Directors.



# Speak Up.

## Ask for Guidance and Voice Concerns

## CODE OF ETHICS

### Participating in an Investigation

Commvault has a responsibility to monitor compliance with this Code and take action when it becomes aware of violations. By seeking advice, raising concerns, or reporting actual or suspected misconduct in good faith, we uphold the principles of our Code and demonstrate integrity. We should all feel comfortable reporting actual or suspected misconduct and participating in an investigation without fear of losing our jobs or other harm.

### Non-Retaliation Policy

Each team member can make a tremendous difference to the company, so it is vital that we all act with integrity, respect, and in accordance with applicable laws. Commvault strictly prohibits retaliation against any team member who reports a complaint or concern in good faith or participates in an investigation. This protection applies even if the investigation does not uncover misconduct.

Retaliation is a direct violation of our Code. Any individual found engaging in retaliatory behavior will face disciplinary action, up to and including termination. Refer the [Ethics and Integrity Reporting Policy](#) for more details. If you or someone you know is the victim of retaliation, report it immediately using our [Reporting Channels](#).

### Ask Questions

Speaking up is essential to maintaining our ethical culture and protecting the integrity of our business. Ignoring concerns or looking the other way can lead to serious consequences for both individuals and Commvault. By asking questions and raising concerns, we contribute to identifying and addressing potential issues before they escalate. If you suspect illegal or unethical behavior or believe there has been an actual or potential violation of the Code or any other Commvault policy, it is your responsibility to report it.



# Speak Up.

## Ask for Guidance and Voice Concerns

## CODE OF ETHICS

### Ways to Raise Questions and Report Concerns

You can report any ethical concerns or issues through the following methods:

- **Online:** Submit concerns confidentially and anonymously through Commvault's dedicated website, [Integrity Counts](#)
- **Email:** Contact [Human Resources](#) leadership team, Chief People Officer and Chief Trust Officer or use [Company's Ethics and Integrity Reporting Platform](#)
- **Reach out** to [HR and Legal](#)
- **Hotline:** Report concerns confidentially and anonymously via the [Employee Ethics Hotline](#)

### Consequence of Violations

Compliance with this Code and all related policies is mandatory for all employees, contractors, and business partners. Any breach of this Code, other Company policies or any legal requirement may result in disciplinary action ranging from corrective measures to termination, depending on the severity of the violation. In cases involving legal or regulatory breaches, further action, including reporting to authorities, may be taken.

### Training and Awareness

All personnel must complete mandatory compliance and security trainings as required by the Company and in accordance with applicable laws. These trainings, conducted at the time of hire and periodically thereafter, are essential for promoting awareness, understanding policies, and upholding the Company's commitment to ethical and secure practices.

