CYBERARK®
THE IDENTITY SECURITY COMPANY®

Code of Conduct

Securing our identity with integrity

Table of contents

A message from our Executive Chairman

CyberArk has been built on trust. Our mission is to provide a modern approach to identity security centered on protecting against advanced cyberattacks.

To continue delivering on our mission and our **customer-first** strategy, it is critical that we conduct our business with the highest level of integrity. Customers and partners choose to work with us because they trust that our products and services will help protect them against cyberattacks and empower them to execute their mission-critical business strategies. Vendors trust us because we remain true to our values, operate with integrity and treat others with respect. Employees join and stay with us because we all work together to do **what is best for CyberArk** and are **innovators** excelling at everything we do. Our relationships with our customers, partners, vendors — and each other — are invaluable, and doing what is right will secure our long-term success.

This Code reflects CyberArk's values and is your personal guide as our **trusted expert**. It is part of a broad toolkit that includes practical policies, training, active engagement and an open-door policy. You may have heard me say this before, but it's worth repeating to ensure we're all **driven to win** the right way: No deal or business advantage is worth compromising our values, integrity or years of hard work.

Our people, our culture, our values and our integrity are inseparable from our success. We are all individually responsible for ensuring that we adhere to the law and act with integrity. Please read this Code carefully — it contains valuable guidance that can help you make business decisions and resolve issues. I also personally ask that you voice concerns, speak up and ask questions so we can all **continuously improve** at what we do and how we do it. Talk to your manager, contact the Compliance and Legal Team or report any concerns to our Speak Up hotline.

Winning with integrity starts with a strong culture. **We** work hard to create an inclusive work environment where everyone is empowered to do the right thing and act with integrity at all times. As we continue to grow and scale our business and team, promoting our culture and being **smart, bold but humble** is ever important! Let's do that together.

Thank you,

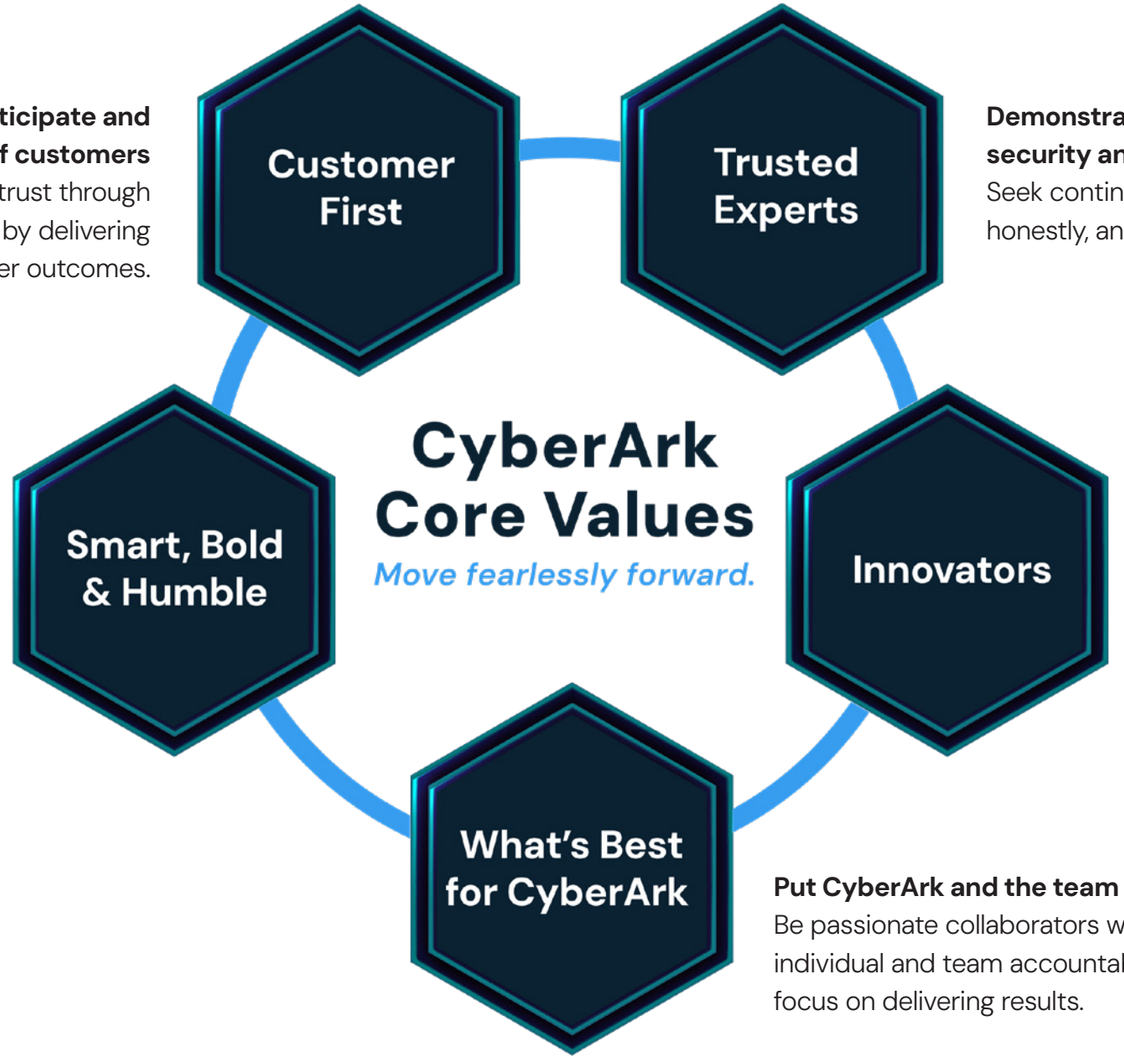
Udi Mokady

Udi Mokady, Executive Chairman

Our core values

Understand, anticipate and respond to the needs of customers and partners. Earn trust through consistent actions and by delivering exceptional customer outcomes.

Demonstrate thorough expertise in security and in individual work domains. Seek continuous learning, communicate honestly, and act with integrity.



Courageously pursue opportunities and confront problems while using experience, data and intuition to make decisions. Embrace diverse perspectives with respect and humility.

Pioneer the future of cybersecurity by creating market-leading solutions. Reimagine ways of working to solve complex business challenges for customers and for CyberArk.

Put CyberArk and the team before self. Be passionate collaborators who demonstrate individual and team accountability and a relentless focus on delivering results.

Importance of the Code

We act with integrity, using our good judgment and common sense.

We know that our success depends on every one of us doing the right thing — everywhere, every day. We stay true to the CyberArk values, are honest and transparent with one another and those we deal with, and keep our commitments.

Our values are the basis for our Code of Conduct (referred to as our Code). Together, both help us tackle ethical dilemmas and make the right decisions. This Code also supports our strategy, protects our colleagues and customers, and supports our reputation as a trusted expert.

Who is this Code for?

Our Code of Conduct is for everyone working at or for CyberArk. This includes anyone who devotes a substantial amount of their time to CyberArk. This does not impact engagement status or scope (such as full- or part-time employment, consulting or outsourcing) nor does it imply the existence of an employment relationship in any way. We also have a Vendor and Business Partner Code of Conduct for our business partners and vendors.

Each of us is responsible for:

- Acting responsibly, with integrity and in good faith.
- Reading and understanding CyberArk's policies and practices that apply to our roles.
- Following the law, our Code and our policies in both letter and spirit.
- Treating everyone with dignity and respect.
- Building trust by asking questions and speaking up.
- Thinking about how our decisions may affect others.

If you're a manager, you should also:

- Share our Code and relevant policies with your team and explain what they mean in practice.
- Be a role model.
- Hold your team accountable.
- Communicate openly and encourage your team to ask questions, raise concerns and speak up. When they do, listen carefully and act appropriately.

This Code cannot predict every situation that you might encounter at CyberArk.

Use sound judgment and common sense in everything you do on behalf of CyberArk, and always make sure that your choices reflect our values.

WHEN IN DOUBT, ASK YOURSELF:

Is this legal and ethical?

Is this in line with our Code and Culture?

Is this right for our customers and shareholders?

Would I feel ok if management knew it or it became public?

If your answer to any of these questions is **"No"** or you are unsure, **STOP!**

Review the Code, the relevant policies and/or ask for advice.

Asking for help and speaking up

Asking questions, sharing our experiences and raising concerns helps all of us — and CyberArk — to continuously improve. While we may make mistakes, it is important we quickly recognize and correct them. Raising matters such as improper behavior, including fraud and illegal acts, helps create a better and safer workplace: We reduce risks and resolve issues before they escalate into significant incidents that could harm you, your colleagues, CyberArk or even our customers and partners.

Whichever Speak Up channel you choose to share your concern, we will address it promptly and protect your privacy and confidentiality to the fullest extent possible, disclosing information only to those who need to know it.

For general advice on a topic, please speak with your manager or reach out directly to the specialist team, such as Compliance, your team's dedicated Legal counsel or your local HR team.

No tolerance for retaliation

CyberArk does not tolerate any type of retaliation against anyone who makes a genuine report of a suspected or actual breach of the Code or supports a compliance investigation. Retaliation is a violation of this Code, and we will respond accordingly, including taking disciplinary action up to and including dismissal.

WHISTLEBLOWER POLICY | ASK A QUESTION

For any suspected breaches of the law or our Code, please raise your concerns as follows:

STEP 1

We encourage you to speak to your manager first.

STEP 2

If it's not appropriate to discuss the issue with your manager, please contact one of our internal specialists (such as Compliance for business conduct and your local HR team for HR related matters).

STEP 3

If you do not feel comfortable speaking up to somebody inside CyberArk, you can always raise your concerns independently using our confidential Speak Up hotline.

EthicsPoint - Palo Alto Networks

Our people and communities

In this section |

- Celebrating diversity, equity and inclusion
- Preventing bullying and harassment
- Promoting a safe and healthy work environment
- Protecting the environment and our global community
- Donations and political activities

Celebrating diversity, equity and inclusion

Our people are key to our success. We strive to create an environment where people want to come to work, feel valued, build strong relationships and, most importantly, achieve their full potential.

We celebrate the diversity of our people and respect people for who they are and what they bring to the organization. We are committed to hiring the best talent and bringing together people from across a wide variety of cultures, backgrounds, genders, races and ethnicities, religions, sexual orientations and ages. Diversity is central to how we work with each other, and discrimination of any form is not tolerated at CyberArk.

Our policy applies to providing equal opportunities in employment, as well as development and advancement. It is instrumental in enabling our employees to bring the best versions of themselves to their work by creating a safe, diverse and inclusive environment that promotes the free exchange of ideas. Ultimately, diversity makes our organization better and stronger.

WHAT WE DO

- Act fairly and respect others regardless of their culture, beliefs and lifestyles.
- Challenge discriminatory and abusive behavior.
- Raise any concerns through one of our Speak Up channels.

WHAT WE DO NOT DO

- Harass, abuse or be offensive, intimidating, malicious or insulting toward others.
- Discriminate or contribute to anything that excludes an individual or group.

“Guided by our core values, we cultivate a culture of great people — an inclusive environment rooted in fairness, where everyone can thrive.”

Kathy Cullen-Cote, Chief People Officer

Preventing bullying and harassment

What each of us does every day determines who CyberArk is and creates our unique culture. We are team players and treat everyone with dignity and respect, always focused on creating a working environment that promotes integrity and trust. We do not tolerate harassment, violence or threatening behavior of any kind by anyone toward our team, customers, partners, vendors or anyone else we deal with in our day-to-day work.

Promoting a safe and healthy work environment

CyberArk proactively strives to protect the health and well-being of our people to provide a safe working environment. Taking care of ourselves and others involved in our business is important, as it brings out the best in all of us.

While our working environment has changed considerably in recent years and many of us have had to manage challenging circumstances, what remains constant is how we work with each other. We will continue to be tolerant of views that differ from ours and will learn to adapt to the changing environment and requirements as best we can. Most importantly, we will offer support to our colleagues and raise any concerns we have for the health and well-being of the CyberArk team.

ANTI-HARASSMENT PAGE | HR PORTAL

Protecting the environment and our global community

We are committed to doing business with integrity, including protecting and advancing human dignity and human rights in our global business practices and throughout our supply chains. We require our vendors and business partners to follow these standards as well. We conduct our business in an environmentally responsible and sustainable manner and are committed to complying with all applicable environmental laws. We continually strive to positively affect the environment and promote sustainable business practices to better serve our team, customers, partners, shareholders and the communities where we live and work.

Donations and political activities

We have a long history of charitable giving and community involvement.

Our donations and charitable contributions reflect our shared values: to be helpful in resolving a social need and to positively contribute to our communities. We only make donations to charities that meet our eligibility criteria, following a compliance review and approval by our Donations Committee. Contributions to political groups may only be made in a personal capacity.

DONATIONS POLICY

Our assets and data

In this section |

- Data protection and privacy
- Confidential and proprietary information
- Protection and use of corporate assets and AI tools
- Using AI responsibly

Data protection and privacy

Cybersecurity is our business. Protecting our network, solutions, team, customers and partners is the foundation of our success. Our Cybersecurity and Privacy Programs are critical components of our overall strategy.

We pride ourselves on being an organization that has a privacy-minded culture, consistent with legal requirements around the world. We value privacy and safeguard the personal data of all individuals, including our colleagues, customers, business partners, vendors, candidates and any other third party with whom we collaborate. Our policies and procedures relate to the entire lifecycle of personal data we process to ensure we follow all applicable laws and regulations.

PRIVACY POLICY | ASK A QUESTION | REPORT INCIDENT

WHAT WE DO

- Approach other people's data thoughtfully, ethically and respectfully and handle it with care.
- Think carefully about who really needs access to personal data and limit access as relevant.
- Follow our Internal Privacy Policy and Handbook and review CyberArk's Privacy Notice for Staff.
- If our work relates to personal data of colleagues, customers or others, consult with the Privacy team about the practical implications of your work and any changes to it.
- Forward personal data requests or questions to Privacy.
- Report suspected security incidents immediately to the Security Operations Center.

WHAT WE DO NOT DO

- Collect or use personal data we do not actually need or retain it for longer than is necessary.
- Leave personal data unsecured or needlessly disclose, share or give access to personal data to anyone else.
- Use or store personal data differently from past use, including data shared with third parties, without completing the Privacy Questionnaire.
- Use customer data for any purpose other than to provide the service the customer has asked us for.

Confidential and Proprietary Information

Being a cybersecurity leader means information is one of our most valuable business assets. We are committed to safeguarding and protecting our information and any other information entrusted to us by our customers and business partners.

This commitment is shared by everyone at CyberArk and applies to confidential information (meaning information that is not public) and proprietary information (such as copyrighted data). Such information can be in different formats, whether written, digital or even oral. We handle all confidential and proprietary information with care and protect it in line with our Information Security policies and procedures.

We only use CyberArk authorized communication tools to discuss business and confidential information and do not discuss any internal business information on social media or other non-authorized means. We apply the same level of care to the confidential information of our customers, partners, vendors and other business associates. These obligations continue to apply, even after we leave CyberArk.

Only authorized representatives of CyberArk may speak publicly on our behalf. If you do make public comments, always make sure to clearly identify views and opinions as your own and not those of CyberArk.

EMPLOYEE SECURITY POLICIES

SOCIAL MEDIA POLICY

WHAT WE DO

- Carefully consider the nature of the information we handle.
- Take the required security steps to safeguard and access information, especially when away from the workplace.
- Only use CyberArk authorized tools and software for business/ work purposes.
- Only share confidential and proprietary information with those who need to know.
- Seek guidance from the Information Security team when we are unsure.

WHAT WE DO NOT DO

- Use information for anything other than a legitimate business purpose or as required by law.
- Use confidential information from a former employer.
- Disclose or discuss confidential information in public places.

“Securing our customers starts with securing ourselves: be mindful in our day-to-day actions and avoid autopilot mode.”

Omer Grossman, Chief Trust Officer and Head of CYBR Unit

Protection and use of corporate assets and AI tools

We protect and enhance CyberArk’s intellectual, digital and physical assets and respect the rights of others. We develop CyberArk’s intellectual property with ingenuity and creativity, without misusing or improperly relying on the intellectual property of others. Our assets must be used responsibly, efficiently and for legitimate business purposes only, avoiding waste and carelessness. Corporate assets include both physical assets (such as computers, laptops and mobiles) and intangible assets (such as customer lists, our intellectual property, trade secrets or other confidential, proprietary or personal information).

CyberArk reserves the right to monitor and inspect without notice computers or laptops owned by the Company or on the Company’s network or premises, including electronic communications, internet usage and inspections of their content. Any monitoring and investigative activities will be proportionate and limited to the extent necessary to address the legitimate business reasons identified by CyberArk. CyberArk will respect your privacy and autonomy as appropriate. However, note that use of the Company’s computers, laptops or the Company’s network and any communications relating to Company business cannot be guaranteed to be private.

Using AI responsibly

CyberArk encourages the responsible and ethical use of artificial intelligence (AI) tools to drive innovation and productivity. You are expected to use AI in ways that reflect our values, protect data security, and maintain trust in our decision-making processes. CyberArk's Internal Responsible AI Policy and your team-specific protocols provide for more detailed guidance on approved tools and ways of working with internal or sensitive data or developing code. When using AI tools – whether provided by CyberArk or accessed externally – you remain personally accountable for any input content as well as the outputs produced and decisions influenced by AI. You must apply critical thinking and ethical standards at all times, and avoid using AI in ways that could reinforce bias or result in unfair or discriminatory outcomes. AI should not be relied on without appropriate human oversight, especially to make sensitive or high-impact decisions. When developing CyberArk's own products and services, you may only input data within the permitted data categories – see the Guidelines for Using GenAI Tools for Product Development for further detail. If you are unsure whether an AI tool is appropriate, consult your team's guidelines or the Internal Responsible AI Policy, and reach out for support. Misuse of AI, including the use of prohibited tools or improper handling of data, may lead to disciplinary action in line with this Code.

Our business operations

In this section |

- Fighting bribery and corruption
- Giving and receiving hospitality
- Ensuring accurate records and disclosures
- Working with our business partners
- Complying with international export, customs and trade controls
- Competing fairly

Fighting bribery and corruption

We do not tolerate any form of bribery or corruption by anyone, wherever we do business.

Our success is based on the excellence of our products and services. We are proud of our reputation for doing business in the right way and consistently apply high global standards. Compliance with bribery and corruption laws is mandatory, regardless of local culture, business practices or customs. Our business principle is clear: We will not compromise the integrity of our customers and partners — or risk our own reputation — to gain an advantage or win a deal.

Bribes often consist of money or other financial benefits and can be anything of value, including gifts, trips, entertainment, charitable donations, favors, jobs or other improper actions. Violating bribery and corruption laws is a serious criminal offense for individuals and businesses and can result in large fines and even imprisonment. We can be held responsible if the illegal behavior is done by one of us or indirectly by anyone else working on our behalf, such as channel partners, consultants, agents and other business partners. Dealings with public officials are particularly high risk: Even the appearance of illegal behavior could cause significant damage to our reputation.

ANTI-CORRUPTION PAGE

WHAT WE DO

- Be mindful of “red flags” that indicate corruption risks and raise them with Compliance.
- Take extra care in markets with heightened risk of corruption.
- Be especially cautious when dealing with government officials.
- Ensure that our partners are aligned with our values and are aware of our zero-tolerance policy.
- Immediately report any suspected request or demand for a potentially corrupt payment to Compliance or your dedicated legal counsel.

WHAT WE DO NOT DO

- Offer, pay, authorize, request or accept a bribe, regardless of local laws or business culture.
- Ask or allow anyone else (such as our partners working on our behalf) to offer, give or accept bribes for us.
- Offer, pay or authorize facilitation or grease payments.
- Try to improperly influence our customers or put them in a position of conflict with their policies.

Giving and receiving hospitality

Hospitality helps us to build stronger and better business relationships, show courtesy or promote goodwill. While we may give or receive modest gifts, meals and entertainment in the ordinary course of business, we are mindful of the risks this may present, as anything of value could be considered bribery. Hospitality must never be given with the expectation of something improper in return and must not compromise our or the customer's ability to make objective and fair business decisions.

HOSPITALITY GUIDELINES

WHAT WE DO	WHAT WE DO NOT DO
Ensure hospitality is always reasonable, proportionate, infrequent and has a justifiable business purpose.	Offer or accept cash or cash equivalents as a gift.
Strictly follow our Hospitality Guidelines.	Offer or accept anything that could be perceived as illegal or improper.
If required, complete a Hospitality Request Form to seek prior approval from Compliance.	Circumvent the Hospitality Guidelines (such as providing inaccurate/partial information or covering expenses ourselves).
Properly expense hospitality and document all necessary details.	

Ensuring accurate records and disclosures

Accurate and reliable financial and business records and statements are essential to ensure compliance with our financial, legal and business obligations.

Our records are the basis of various reports and statements to the public, investors and government authorities. They also guide our business decision-making and strategic planning.

As a public company, we maintain a high standard of accuracy and completeness in our financial records, filings and disclosures. Together, we ensure that our public communications are full, fair, accurate, timely and understandable. It is vital that our financial books, records and statements properly document all assets and liabilities, and accurately and fairly reflect all transactions of the company.

We do not knowingly misrepresent or omit — or cause others to misrepresent or omit — material facts about the Company to others. Any significant discrepancies, material weaknesses in our controls or actual/suspected fraud in our books and records must be immediately reported to Compliance or to our Chief Financial Officer.

CyberArk will not make or approve any payment that could be used for something other than its stated purpose, nor any excessive discount that could be used for improper or illegal actions.

ANTI-CORRUPTION POLICY

FAIR DISCLOSURE POLICY

“Every successful relationship is built on trust, integrity and high ethical standards.”

Donna Rahav, Chief Legal Officer

Working with our business partners

Our continued success is dependent on building and maintaining relationships with trustworthy business partners. We take great care when selecting new partners or managing existing ones, conducting due diligence in line with our processes and demonstrating our ethical and integrity values when interacting with them. Most importantly, we require all of our business partners to comply with applicable laws and our Vendor and Business Partner Code of Conduct and to always operate with the highest levels of ethics and integrity when working with us.

VENDOR AND BUSINESS PARTNER CODE OF CONDUCT

Complying with international export, customs and trade controls

We are committed to following applicable exports control, customs and trade control laws, regulations and international sanctions. As a global company, CyberArk is subject to a complex set of trade sanctions and export controls. The United Nations, the United States, the European Union, the State of Israel and many individual countries have strict controls on exporting to and trading with certain countries, businesses and even individuals. Also, because our products contain encryption features, we are subject to further licensing and export restrictions.

Violations of these rules can carry serious consequences, such as potential criminal penalties like fines and imprisonment. They could also negatively impact our ability to sell products or provide services in certain countries. Any suspected trade control violations or irregularities must be immediately reported to Compliance.

TRADE CONTROLS COMPLIANCE POLICY

Competing fairly

We believe in vigorous yet fair competition and are committed to following all antitrust and competition laws that apply to our business.

Antitrust and competition laws are designed to encourage a free market and continuous innovation. Anti-competitive behavior undermines this, hurting our customers and ultimately our business. It is against everything we stand for, in particular our customer-first agenda — we have fair and consistent price and discount structures. Such behavior can include price fixing, market or customer sharing and bid rigging, or simply the exchange of commercially sensitive information with competitors. Failure to comply with antitrust and competition laws can have serious consequences for businesses and individuals involved, such as very large fines based on our annual global turnover, reputational damage and even imprisonment.

As part of our strategy to meet our customers' needs, we monitor our competitive environment. This process enables us to respond to our customers' needs and ensures that our products remain effective in the continuously evolving cyber threat landscape. We ensure that information and insights are used legally; as part of this process, we do not share information with competitors, including indirectly via a third party.

WHAT WE DO

- Always make business decisions independently.
- Limit interactions with competitors and avoid discussing commercially sensitive topics with them.
- Seek legal advice before joining trade bodies/associations.
- Immediately remove ourselves from any potential anti-competitive discussions and report the incident to Compliance.

WHAT WE DO NOT DO

- Exchange commercially sensitive information with a competitor (including via an intermediary) without Compliance approval.
- Enter into formal or informal agreements or otherwise collaborate with competitors on prices, commercial terms or strategy, or divide territories, customers or product categories.
- Establish minimum resale prices for our channel partners, either directly or indirectly.

Our integrity

In this section |

- Avoiding conflicts of interests
- Preventing insider trading

Avoiding conflicts of interests

Conflicts of interests can have a significant negative impact on our business, operations and results, and can undermine our ability to achieve what is best for CyberArk. We always put CyberArk's interests first and our personal interests aside. If you have any reason to believe that you or someone you work with may be in a position where a conflict of interest could arise, please contact Compliance immediately.

How do conflicts arise?

Conflicts of interest can sometimes occur without any action on our part. They can arise from a variety of situations, such as:

- A partner, family member or close relative is employed by one of our competitors, suppliers, customers or partners.
- A romantic relationship between an employee and their manager or a senior decision maker.
- A direct reporting line between relatives.
- An employee, partner, family member or close relative has a personal financial interest in a CyberArk transaction.
- A second job competes with an employee's ability to do their job.

WHAT WE DO

- Proactively avoid situations where personal relationships or financial interests conflict with CyberArk's best interests.
- Immediately disclose any potential personal, business or financial conflicts of interests to Compliance.
- Obtain Compliance approval before making a personal investment that may conflict with CyberArk's best interests, in particular shareholdings in competitors, customers and suppliers exceeding 1%.
- Consult with Compliance if we feel that our judgment on work-related decisions may be compromised.

WHAT WE DO NOT DO

- Engage in any outside activity that may, or could be, perceived to affect our work.
- Abuse our position for personal benefit or for the benefit of someone with whom we have a personal relationship.
- Hide any personal relationship, connection or employment that could be considered a conflict.
- Take up roles with our competitors, suppliers, customers or other related entities without prior disclosure to Compliance.
- Intentionally ignore or hide business-related opportunities from CyberArk.

Preventing insider trading

We follow securities laws and do not make improper use of insider information of CyberArk or any other listed company.

As part of our work, we may obtain sensitive information that is not available to the public and that a reasonable investor would likely consider important in deciding whether to buy or sell our company's shares (or other publicly traded companies) — so-called insider information. This could include financial performance data, a major strategic move by a company or a cybersecurity breach that is not known to the public. Trading or encouraging others to trade on insider information or giving it to unauthorized parties is a criminal offense in many countries and may result in fines and imprisonment.

INSIDER TRADING PAGE

WHAT WE DO

- Treat sensitive information with extra care and share it only when absolutely necessary.
- Comply with our rules on the release of information.
- Only trade CyberArk shares in line with our internal processes and applicable blackout periods.

WHAT WE DO NOT DO

- Trade in shares of CyberArk or any other listed company if we have insider information.
- Share insider information with family and friends and/or encourage trading on such information.
- Spread false or inaccurate information about CyberArk or other listed companies to influence share prices.

Enforcing this code and law enforcement actions

There are very serious consequences for not complying with our Code or the law. We may take disciplinary action and even dismiss people when necessary.

Any manager who directs, approves or ignores any conduct that violates the Code or the law may also be subject to disciplinary action. If necessary, we may also refer such violations to law enforcement authorities, and it is our policy to fully cooperate with appropriate government investigations.

Our Chief Executive Officer and senior financial officers are also required to promote compliance with this Code by all employees and to abide by this Code and other Company standards, policies and procedures.

Any approaches by regulators, enforcement authorities or governmental organizations regarding alleged violations of our legal obligations must be immediately reported to Compliance and Legal, and any related interaction must be led by Compliance and Legal. Also, you must share any legal claims or threatened lawsuits against CyberArk with Legal as soon as you become aware of them.

Waivers of our Code of Conduct must be approved in writing. Waivers for Board members and executive officers require Board approval, and waivers involving any other team member require the written approval of our Chief Legal Officer. We will publicly disclose any waivers of this Code made to any executive officer or director of the Company as required by the Securities Exchange Act of 1934 and any applicable rules of the Nasdaq Stock Market LLC.

WHAT WE DO

- Follow our Values and the Code in letter and spirit.
- Refer law enforcement agencies and regulators to Compliance and Legal.
- Share legal claims with Legal.
- Seek prior written approval for exceptions to the Code.

WHAT WE DO NOT DO

- Respond to legal claims on your own.
- Be willfully blind to issues and concerns we encounter.
- Proceed with actions that are not aligned with our Code.
- Take enforcement of the Code and policies into our own hands.

Closing message from our CEO

Thank you for taking the time to read our Code. We hope it helps you with understanding how to spot and manage the different types of compliance risks that you may come across as part of your day-to-day role. Most importantly, when we do business, we should always focus on doing it the right way — there is no deal or business scenario for which it is ever worth compromising CyberArk's values or reputation.

If you encounter an ethical dilemma and are unsure what to do, please speak to someone — your manager, Legal, Compliance or HR. They are here to support you. Also, if you come across a situation that might not be in line with our Code and commitment to an ethical culture, please raise your concerns as soon as possible. Speaking up is a responsibility we all share when **securing our identity with integrity**.

Thank you,

Matt Cohen

Matt Cohen, Chief Executive Officer

CyberArk is the global leader in identity security. Centered on intelligent privilege controls, CyberArk provides the most comprehensive security offering for any identity — human or machine — across business applications, distributed workforces, hybrid cloud environments and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets. To learn more about CyberArk, visit www.cyberark.com, read the CyberArk blogs or follow on LinkedIn, X, Facebook or YouTube. is the global leader in Identity Security.

©Copyright 2025 CyberArk Software. All rights reserved. No portion of this publication may be reproduced in any form or by any means without the express written consent of CyberArk Software. CyberArk®, the CyberArk logo and other trade or service names appearing above are registered trademarks (or trademarks) of CyberArk Software in the U.S. and other jurisdictions. Any other trade and service names are the property of their respective owners. CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice.

THIS PUBLICATION IS FOR INFORMATIONAL PURPOSES ONLY AND IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER WHETHER EXPRESSED OR IMPLIED, INCLUDING WARRANTY OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, NON-INFRINGEMENT OR OTHERWISE. IN NO EVENT SHALL CYBERARK BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND IN PARTICULAR CYBERARK SHALL NOT BE LIABLE FOR DIRECT, SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE OR LOSS OF USE, COST OF REPLACEMENT GOODS, LOSS OR DAMAGE TO DATA ARISING FROM USE OF OR IN RELIANCE ON THIS PUBLICATION, EVEN IF CYBERARK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

U.S., 02.26 Doc: 5048654600

CYBERARK®