SPEAK UP POLICY

1. Introduction

Why is speaking up important?

At CyberArk we are committed to doing business the right way, respecting each other, ethical standards and applicable laws – always living our values.

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

What is the purpose of this policy?

We want to encourage you to raise issues and concerns early. This policy explains how you can raise a concern in confidence and without fear of retaliation, and what happens after you have done so.

Who can Speak Up?

Anyone who wishes to raise a concern about possible misconduct that may potentially affect CyberArk can use our Speak Up process.

What concerns are covered?

You can raise concerns about possible violations of the law, our Code of Conduct, or our policies and procedures. Examples cover the following categories:

- Accounting or financial reporting irregularities
- Fraud and theft
- Bribery and corruption
- Workplace misconduct
- Discrimination, bullying and harassment
- Retaliation
- Conflict of interests
- Improper use of company resources
- Insider trading
- Export or sanctions regulations
- Antitrust, anti-competitive practices
- Data breaches and privacy violations
- Product quality and security concerns
- Intellectual property violations
- Misuse of information
- Environmental, health and safety issues
- Human rights violations
- Matters impacting our reputation

Do not use this policy to report:

- **Immediate threats to life or property.** If you need emergency assistance, contact your local emergency services
- False or misleading accusations

Why should I get involved?

We understand that speaking up is not always easy. Speaking up when we see behavior that does not reflect our values is a personal responsibility that we all share in order to safeguard CyberArk's future. To support this, CyberArk will ensure that the reporting process is safe and trustworthy.

How can managers support this process?

Managers play a vital role in supporting the Speak Up process. Besides role modelling expected behaviors, you should actively encourage your team to raise concerns early if they are aware of potential violations. If you receive any, listen carefully and refer these concerns to the relevant internal specialists.

2. How and when to Speak Up

How can I Speak Up?

You can raise your concerns through any of the following ways:

1. We encourage you to reach out to your manager first.
2. If it's not appropriate to discuss the issue with your manager, please contact Compliance or one of our internal specialists (such as your local HR team for workplace misconduct, or Privacy for data protection concerns or Information Security for cyber security incidents).
3. If you do not feel comfortable speaking up to somebody inside CyberArk, you can always raise your concern independently using our confidential Speak Up hotline: **CyberArk.ethicspoint.com**

Is it possible to report anonymously?

Information provided through all our reporting channels is kept confidential and only shared on a strict need-to-know basis. You can submit anonymous reports through our Speak Up hotline if permitted by the laws of your country, please pay attention to the information needed (listed below). Sometimes, in order to properly investigate a report, we require additional information. Please be sure to revisit the Speak Up service periodically and check your case number to see if we have any follow-up questions. Your responses will be sent to us anonymously as well.

What information do I need to provide?

When you raise a concern, try to provide as much information as possible to enable CyberArk to assess and investigate your concern. If possible, information should include:

- Background, history and reasons for the concern
- Names, dates, places and other relevant information
- Any supporting documentation

If you submitted your concerns anonymously, we may reach out with questions through the Speak Up hotline. Please follow up on your complaint to support our investigation.

What if I do not have all the information?

If you know about or suspect misconduct, then we encourage you to speak up as soon as possible with any information that you have at that time. Prompt reporting allows us to prevent a situation from escalating. You are not required to prove your concern is well-founded or correct – there's no need for your to conduct your own investigation to get supporting evidence.
Our internal specialists will try to obtain any missing information as part of their investigation and get in touch if they have questions. You will not face consequences if your genuine concern later turns out to be mistaken.

3. How we will protect you

Will my report remain confidential?

We treat all reports with the strictest confidence and discretion. This means that the information you provide, including your identity and those of witnesses, will only be shared with a limited number of authorized people on a strict need-to-know basis. As part of the investigation, we will need to inform the person who is the subject of the complaint, but your identity, if known, will not be disclosed to the extent practicable. You too can help with protecting confidentiality by being discrete and not discussing your report with others.

Will my privacy be protected?

We are committed to protecting the privacy of everyone involved. This means we will safeguard personal data from unauthorized access and processing. Personal data obtained as part of the Speak Up process will only be used for the purposes set out in this policy or in accordance with CyberArk's Privacy Policy consistent with applicable law. Access to the data obtained through the Speak Up process will be documented and limited to a need-to-know basis as detailed above.

For more details on how we protect personal data please see our internal Privacy Policy or our online Privacy Notice.

Will I be protected from retaliation?

Speaking up is a responsibility we all share to safeguard the continued success of CyberArk. We do not tolerate any form of retaliation against anyone who raises a genuine concern or supports an investigation.

Retaliation can include threats, harassment, intimidation, or other adverse consequences to your role. It can also include more subtle indirect actions, such as excessive scrutiny of your work, inappropriate project reassignments or being excluded from team social events. If an action discourages you from speaking up, it may also be retaliation.

Our promise of protection against retaliation applies to all forms of retaliation, including attempts, threats or actual retaliation against you or individuals connected to you. Retaliation is a serious violation of our Code of Conduct, and we will respond accordingly, including taking disciplinary action up to and including dismissal. If you notice retaliation against yourself or anyone else, please report this through our Speak Up channels. Your report will be treated like any other Speak Up report.

4. What happens after you Speak Up

What happens after I submit my report?

Once you have submitted your report, you will receive an acknowledgment of receipt within 7 days. We take every report of possible misconduct very seriously. For example, reports submitted through our Speak Up hotline are automatically delivered to CyberArk's Chief Legal Officer (CLO) and the Chairperson of the Audit Committee of our Board of Directors (in addition to Compliance).

Unless immediate action is required, we will conduct an initial review to determine if your report requires further investigation (and, if so, by whom and how). On average, we aim to close cases as soon as possible, though due to the seriousness or complexity of a matter investigations can take some time to complete. Either way you will receive an update within 3 months, and we will

also inform you of its outcome once a case is closed. Please note the details we can share will be limited for reasons of confidentiality, privacy, and the legal rights of all parties involved.

Who will act on my concern and how?

The nature, urgency and potential impact of your concern determines who addresses it. In general, Compliance or one of our internal specialist teams (such as HR, Privacy or Information Security) become the investigative lead. We may also engage external experts (such as law firms) if appropriate, for example due to the seriousness of your concern, the seniority of the accused or a potential conflict of interests.

Compliance, or the relevant internal specialist investigating a matter, will update the CLO of its progress and key findings. If appropriate, the CLO will update relevant executives or members of the Audit Committee.

Due to the seriousness and nature of the following matters, any concern that relates to them will be promptly shared with the Chairperson of the Audit Committee and the CLO (regardless of the Speak Up channel used to submit it):

- Accounting irregularities
- Internal accounting controls
- Auditing matters
- Bribery, banking and financial crime.

If necessary, these matters are investigated by the Audit Committee in a manner to be determined by it (including engaging an external investigator). In such cases, the Audit Committee will update Compliance (or outside counsel) at least quarterly to support an evaluation of whether an external disclosure is required by law.

As part of the appointment of the investigative lead, we also assess potential conflict of interests to ensure the investigation is unbiased and objective. For example, if a report relates to our CLO, the Audit Committee will appoint a suitable alternative.

How is an investigation conducted?

We follow the guiding principles of objectivity and impartiality to ensure investigations are run in an independent, fair and unbiased manner with respect to all parties involved and in line with relevant legal requirements.

Following the initial review and assignment of the investigative lead, we start the investigation, which is an objective fact-finding process that can include evidence reviews and witness interviews. As part of that process, the investigative lead may contact you, if they have follow-up questions. Details of the case and the identities of all individuals involved are kept confidential throughout and after the investigation (to the extent permitted by law).

What is expected of me during an investigation?

If you ever become part of an investigation, we will need you to do the following:

- Cooperate and answer all questions completely and honestly
- Keep the details of the investigation confidential
- Do not destroy, delete or hide any information or documents potentially relevant to the investigation
- Do not attempt to influence the investigation.

What happens after an investigation is closed?

If our investigation concludes that misconduct has taken place, we will take appropriate corrective and disciplinary actions in line with applicable law and CyberArk's Code of Conduct, which may include warnings, demotions, loss of benefits, or even termination.

If you believe your concern, a concern raised against you, or an investigation has not been managed correctly, please immediately contact the CLO. For matters investigated by the Audit Committee, please raise your concern through the Speak Up hotline.

5. Need more information?

If you have questions relating to this Speak Up Policy or if you need help making a report, please contact:

- Your manager or your local HR team
- Compliance at Compliance@cyberark.com

Document Management	
Document Type	Global Policy
Name	Speak Up Policy
Owner – Department, Function	Legal, Chief Legal Officer
Last Reviewed/Updated	August 17, 2023