Global Reporting Concerns & Non-Retaliation Policy

Policy No.: C-9	Revision Date: February 1, 2023
Executive Owner: David Koeppel (VP, Deputy General Counsel, Chief Ethics & Compliance Officer)	
Custodian: Dirk McElravey (Sr. Dir. and Assoc. General Counsel, Ethics & Compliance – Investigations)	

Purpose

VMware is committed to the highest standards of conduct and ethical behavior in all its business activities. The purpose of this policy is to explain how VMware protects employees and stakeholders who report conduct that they suspect is improper, unethical or unlawful.

This policy explains how to report a concern and the measures VMware and its subsidiaries follow to protect those who make a report of possible improper, unethical or unlawful conduct by VMware, its employees or third parties VMware engages to conduct its business.

Scope

This policy applies to reports made by VMware employees, contractors (including contingent workers), partners, suppliers, vendors and others entitled to protection under applicable law.

This policy applies to the operations of VMware, Inc., and its wholly owned subsidiaries, which are collectively referred to in this policy as "VMware." This is a global policy that applies to all jurisdictions where VMware operates. If local laws or regulations provide a higher level of protection than what is included in this policy, those local laws will govern.

To the extent there is a conflict between this policy and any existing local VMware policy governing the same subject matter, this policy will control, subject to local legal requirements. After the adoption date of this policy, any new local policy must be approved by this policy's custodian before adoption.

Non-Retaliation Policy

VMware prohibits retaliation against any person who reports a concern about conduct that they suspect is improper, unethical or a violation of VMware's Business Conduct Guidelines, VMware policies, or applicable laws or regulations. VMware also prohibits retaliation against any person who provides information or otherwise assists in the investigation of a report.

Making a report may not protect you from the consequences flowing from your involvement in the conduct or wrongdoing that is the subject of your report or in knowingly making a false report. VMware may also raise any performance-related or contract issues with you that are unrelated to your report, so long as those issues remain separate from and uninfluenced by any reports that you have made.

I. Reportable Conduct

This policy applies to reports about suspected misconduct in relation to VMware, including but not limited to the following "Reportable Conduct":

- Conduct that is unethical or may violate VMware's Business Conduct Guidelines or any VMware policy or procedures;
- Conduct that may violate of applicable law or regulations;

- Conduct (e.g. unsafe work practices) that is potentially damaging to VMware, VMware's employees or a third party;
- Conduct that may cause economic loss or reputational damage to VMware or be otherwise detrimental to VMware's interests;
- Conduct that represents a danger to the public or financial system; or
- Conduct that involves harassment, discrimination, bullying, or other similar misconduct that violated VMware's Global Respectful Workplace Policy.

II. Making a Report

If you know, or have reason to believe, there has been a violation of applicable laws or regulations, the Business Conduct Guidelines or any VMware policy, promptly report such misconduct through one of the following communication channels:

- Your supervisor or manager
- Human Resources or Employee Relations
- Ethics & Compliance team
- Legal Department
- Board of Directors Audit Committee

You can also use ETICA, our ethics helpline, available online at:

www.vmwareethicshelpline.ethicspoint.com.

Suppliers, vendors, partners, contractors (including contingent workers) and others entitled to protection under the law are also encouraged to use ETICA for reporting of possible misconduct.

To assure confidentiality, ETICA is managed by an external vendor. The service is available 24 hours a day, seven days a week, in multiple languages, and includes options for making reports anonymously.

III. Protection for Reporters

A. No retaliation

As explained earlier, VMware does not permit retaliation against persons who report a concern, provide information or otherwise participate in the investigation of a report. This is the case even if the report is ultimately not substantiated.

If you believe you have been retaliated against, you should immediately notify VMware by using the reporting channels outlined in this policy. VMware will review all retaliation claims promptly and investigate when appropriate. VMware will treat any retaliation as serious misconduct that may result in corrective action, up to and including termination of employment or engagement.

B. Confidentiality

Any report made under this policy will be kept confidential to the maximum extent, consistent with applicable laws and business needs to ensure the fair treatment of employees mentioned in the report, including those who are the subject of the report.

If you make a report to VMware, measures will be implemented to safeguard the confidentiality of your identity throughout the investigation process and will only be shared if:

- You have consented;
- It is reasonably necessary to facilitate an investigation into the issues raised in your report;
- Your report is escalated to governmental or regulatory authorities or law enforcement; or
- Your report is disclosed by VMware to a legal practitioner for the purpose of obtaining legal advice or legal representation.

C. Anonymity

In most places, you may also report improper or ethical conduct anonymously, and you can remain anonymous during the investigation and after the investigation has been completed. To make an anonymous report, contact the ETICA VMware Ethics Helpline at 1-877-310-0382 or visit www.vmwareethicshelpline.ethicspoint.com.

Keep in mind that in some circumstances, it might be difficult or even impossible for VMware to investigate effectively anonymous reports. These limitations potentially include the inability to obtain additional information to facilitate the preliminary inquiry or investigation and to provide feedback on the outcome of the investigation. Therefore, VMware encourages you to share your identity when reporting.

IV. Handling of Reports and the Investigation Process

VMware will contact you, whenever possible, within seven days of receiving your report to acknowledge that it has been received.

VMware will assess your report as soon as practical and will determine if an investigation is warranted. You may be contacted by an investigator for additional information to assist in that determination.

If an investigation is initiated, it will be undertaken by the appropriate person in and/or outside VMware, depending on the nature of the report and the investigation. Those conducting the investigation will maintain confidentiality of the subject matter of the investigation, the identity of the reporter and the contributions of those who are asked to participate in the investigation as set forth above.

The scope and nature of the investigation will be determined by VMware. VMware may speak to anyone who may be affected by or involved in the report, including those who are the subject of the report, and their responses will be considered.

VMware will keep you updated during an investigation, as appropriate and required. VMware may not disclose the outcome of an investigation to you if doing so would contravene VMware's privacy policy, the law or is otherwise inappropriate.

Upon completion of the investigation, findings will be reported to appropriate VMware management personnel and other appropriate stakeholders. Management will then work with support personnel, including, for example, VMware's Human Resources, to determine and implement any required discipline or remediation.

The data collected and processed during an investigation (which might include personal information related to the employee or the accuser's name, position, and so on) will be treated confidentially and proportionate in relation to the specific purpose for which it is collected or further processed. Processed

personal data shall be retained no longer than required or permitted by applicable law. All information will be dealt with in accordance with the requirements of all local data protection legislation and VMware's Records Retention Policy.

Administration of this Policy

VMware will review and update this policy periodically, as required to maintain relevance and adherence to applicable laws.

This policy and any variations to this policy do not form a term of any contract, including any contract of employment and does not impose any contractual duties, implied or otherwise, on VMware.