FORTINET, INC.

ANTI-CORRUPTION POLICY

(As Adopted on November 1, 2023)

Fortinet, Inc. ("***Fortinet***") is committed to promoting the highest standards of ethical business conduct and to compliance with all applicable laws, rules, and regulations. As part of this commitment, all Fortinet employees worldwide, including individuals employed by or acting on behalf of Fortinet or its subsidiaries, are required to comply with the Foreign Corrupt Practices Act ("***FCPA***"), the UK Bribery Act, other anti-bribery laws, local laws, this Policy, and any procedures developed by management to implement this Policy.

I. CONDUCT PROHIBITED

Fortinet and its officers, employees, agents and representatives are prohibited from authorizing, making, offering, promising, requesting, receiving or accepting bribes or accepting kickbacks in any form:

- Do not authorize, make, offer, promise, request receive, or accept bribes, kickbacks, or other improper payments of any sort.

- This prohibition applies to all forms of bribery including commercial bribery as well as bribery of government officials.

The U.S. and other anti-corruption laws prohibiting bribery are very broad, so that many kinds of gifts or entertainment provided to government employees might be considered improper. For that reason, you may not give anything of value to any government official in order to wrongfully influence the government official, obtain or retain business or receive any advantage. This prohibition applies regardless of whether the payment or offer of payment is made directly to the government official or indirectly through a third party.

Examples of prohibited conduct include:

- payments made to a government official for an improper purpose;

- payments or gifts to third parties where you know or have reason to know that at least a portion of the payments or gifts is likely to be offered by the third party to a government official for an improper purpose;

- acts "in furtherance of" an improper payment, such as arranging for funds to be available for the improper payment; and

- payments to retain assets, such as an "under the table" payment to a tax official to settle a tax claim.

It is important to avoid even the appearance of impropriety. If you have any questions about whether a payment may be improper or violate this Policy, consult Fortinet's Legal Department before any payment or offer is made.

II. IMPORTANT CONCEPTS

"***Government official***" includes:

- any official or employee of a government, including any political party, administrative agency, or government-owned business;
- any person acting in an official capacity on behalf of a government entity;
- employees or agents of a business which is owned or controlled by a government;
- any person or firm employed by or acting for or on behalf of any government;
- any political party official, employee or agent of a political party, or candidate for political office (or political party position); and
- any family member or other representative of any of the above.

Any doubts about whether a particular person is a government official should be resolved by assuming that the individual involved is a government official for FCPA purposes.

"Anything of value" includes money and monetary equivalents (such as gambling chips and gift cards), entertainment, accommodations, and any other benefit. There is no "minimum" required under the FCPA – any amount can be sufficient to trigger a violation.

"Improper advantage" includes payments intended to wrongfully:

- influence a decision by an official, including a failure to perform his or her official functions;
- induce an official to use his or her influence to affect a decision by someone else in his or her government; and
- induce an official to use his or her influence to affect or influence any act or decision.

In addition to obtaining or retaining business, "improper advantage" includes reducing taxes, or duties, "looking the other way" at minor code or rule violations, and any form of preferential treatment.

III. GIFTS, ENTERTAINMENT, TRAVEL & PROMOTIONAL EXPENDITURES

Gifts in the business context can be an appropriate way for business people to display respect for each other. Fortinet expects the use of good judgment and moderation when giving or receiving entertainment or gifts. No gift or entertainment should ever be offered, given, provided or accepted by you unless it:

- is reasonable and not extravagant;
- is appropriate under the circumstances and serves a valid business purpose;
- is customary and appropriate under U.S. and local customs;
- is not being offered for any improper purpose, and could not be construed as a bribe, kickback or payoff;
- does not violate any Fortinet policy;
- does not violate any U.S., local or international laws or regulations; and
- is accurately described in your expense or other reports and Fortinet's books and records.

It is essential that you accurately report expenditures for gifts or entertainment so that the purpose, amount, and recipient of the gift are obvious (i.e., transparent) to finance and other personnel who may review our books and records. Expense reports should accurately state the purpose of the expenditures and the identities of the individuals receiving the gifts or entertainment and state whether the gift or entertainment was given to a public sector official or to any employee of a government entity.

Significant legal restrictions apply with regard to providing gifts, entertainment, travel and promotional expenditures related to government officials. You must make sure you fully understand all such restrictions and associated policies and procedures. In each instance: all gifts, entertainment, or promotional expenses which are intended to induce a government official to misuse his position or to obtain an improper advantage are prohibited, regardless of their value;

- you are required to submit for prior written approval to Fortinet's General Counsel for any expense provided to a government official above $100 per item, event or person;
- expenses must have a valid business purpose and be reasonable and necessary under the circumstances;
- gifts must be of token value (such as shirts or tote bags that reflect Fortinet's business name and/or logo), legal and customary, and openly given; and

- expenses and gifts must be fully and accurately reflected in Fortinet's books and records and backed by receipts.

You should avoid even the appearance of impropriety. Any gift or expense that is lavish or might otherwise prove embarrassing for Fortinet is prohibited. If you have any question regarding the appropriateness of any gift or expense, you should consult the Fortinet's Vice President of Legal and Compliance responsible for your region, prior to giving the gift or incurring the expense.

IV. FACILITATING PAYMENTS

The FCPA and other anti-bribery laws may provide limited exceptions for certain minor payments for the purpose of facilitating or expediting routine, lawful services or non-discretionary administrative actions, such as telephone installation. However, other anti-corruption laws prohibit such payments. Any and all facilitating payments require prior written approval from the Fortinet's Vice President of Legal and Compliance responsible for your region.

V. REPRESENTATIVES, PARTNERS, CONSULTANTS, DISTRIBUTORS, AGENTS, AND OTHER THIRD PARTIES

Before initiating a relationship with a representative, partner, consultant, distributor, agent, or other third party, you must conduct appropriate due diligence to assure yourself that the representative will not engage in any improper conduct. The business owners responsible for engaging the third party are responsible to perform reasonable due diligence upon engagement and are responsible for ongoing oversight and diligence during the engagement, as reasonably appropriate to ensure the third party will not engage in any improper conduct. Due diligence typically will include considering such factors as:

- the representative's qualifications for the position or task at issue;
- whether the representative has personal or professional ties to the government;
- the reputation of the representative's clientele and the representative's reputation with local bankers, clients, and other business associates; and
- the reasonableness of the compensation.

Consult Fortinet's Vice President of Legal and Compliance responsible for your region regarding the appropriate due diligence procedure for your situation.

Fortinet must terminate contracts with any third party who is unwilling or unable to represent Fortinet in a manner consistent with this Policy.

VI. RED FLAGS

While conducting due diligence and throughout any subsequent relationship, you must monitor for any "red flags." A "red flag" is a fact or circumstance which requires additional consideration and extra caution. Red flags may appear in many forms and can include:

- payments in a country with a history or reputation for corruption;
- refusal to provide a certification of compliance with the FCPA;
- unusual payment patterns or requests, including special pricing requests, unusual discounting, payments to third parties, in cash, and payments made to bank accounts outside the country;
- representations or boasting about influence or connections;
- use of a shell or holding company that obscures ownership without credible explanation;
- use of a reseller that is not adding any value but still would earn a profit on a deal (whereby that reseller may pass that profit on in an improper way, such as a kickback or bribe);
- engagement of a consultant that is not adding any value but is being paid (whereby that consultant may pass that compensation on in an improper way, such as a kickback or bribe);
- accusations of improper business practices (improper deal registration, credible rumors or media reports, etc.);
- family or business relationship with the government or a government official;
- requests for payments "up front" or statements that a particular amount of money is needed to "get the business," "make the necessary arrangements," or similar expressions;
- unusually high commissions, agents' fees, or payments for goods or services;
- apparent lack of qualifications or resources;
- whether the representative or joint venture partner has been recommended by an official of the potential government customer;
- requests to be able to make agreements without Fortinet's approval; and
- requests that agreements or communications be kept secret.

You are responsible for monitoring your email and other communications and documents for red flags. Any red flags should be brought promptly to the attention of the Fortinet's Vice President of Legal and Compliance or otherwise reported in the various methods discussed in Fortinet's Whistleblower Policy. Failure to do so is considered a violation of this Policy.

VII. BOOKS AND RECORDS

All employees must maintain accurate records of all transactions and assist in ensuring that Fortinet's books and records accurately and fairly reflect, with appropriate detail, all

transactions, expenses, or other dispositions of assets. To that end, every employee is prohibited from falsifying any business or accounting record and must truthfully report and record all dispositions of assets. Undisclosed or unrecorded funds or assets—for any purpose—are prohibited.

Any questions on how to record transactions should be referred to the Fortinet's Compliance Officer.

In addition to the guidelines set forth above, all employees must comply with Fortinet's Code of Business Conduct and Ethics and other policies.

VIII. REPORTING BREACHES OF THIS POLICY

Compliance with this Policy is, first and foremost, the individual responsibility of every Fortinet employee. All employees must report, in person or in writing, any known or suspected violations of this Policy to either the Chief Financial Officer or the Chair of the Audit Committee or otherwise in the various reporting methods discussed in Fortinet's Whistleblower Policy. Additionally, all employees may contact the Company's Vice President of Legal and Compliance responsible for your region, General Counsel, or the Chair of the Audit Committee with questions or concerns about this Policy. All good faith reports will be taken seriously and will be promptly investigated, and reports can be made confidentially and anonymously.

Fortinet will not allow any retaliation against any Fortinet employee who acts in good faith in reporting any violation of this Policy. Fortinet will investigate reported violations and will determine an appropriate response, including corrective action and preventative measures, and will involve the Chair of the Audit Committee or Chief Financial Officer when required and appropriate.

IX. CERTIFICATION AND ENFORCEMENT

From time to time, in Fortinet's discretion, Fortinet personnel may be required to complete compliance training and sign a certification acknowledging commitment to, full understanding of, and compliance with Fortinet's policies. Any Fortinet personnel who violate this Policy or who fail to make or falsify any certification required by Fortinet may be subject to disciplinary action, up to and including termination.