

FORTINET, INC.**WHISTLEBLOWER POLICY
(Financial Information Integrity Policy)**

Fortinet, Inc. (“Fortinet”) is committed to conducting business with integrity and in compliance with the letter and the spirit of the law. Fortinet’s commitment to conducting business with the highest level of ethics, standards, and responsibility is reflected in its Code of Business Conduct and Ethics and other policies, such as its Employee Handbook, Travel & Expense Policy, Procurement Policy, and Insider Trading Policy. The Audit Committee of the Fortinet Board of Directors takes very seriously all complaints and concerns regarding conducting business with ethics and integrity and in compliance with laws, including accounting, internal controls over financial reporting and auditing matters. Fortinet’s financial information guides the decisions of the Board of Directors and management and is relied upon by Fortinet’s stockholders, employees and business partners. Fortinet promotes an open door policy and its policies and practices have been developed to maintain the highest business, legal and ethical standards.

You are **required** to report any known or suspected violations of Fortinet policies or the law, including questionable accounting or auditing matters, instances of corporate fraud, violation of applicable laws, corruption, unethical behavior, side agreements, bribes, kickbacks, and conflicts of interest ("Compliance Matters").

All good faith reports will be taken seriously and will be promptly investigated. Information disclosed during the course of the investigation will be maintained as confidential to the fullest extent practical, consistent with the need to conduct an adequate review and applicable laws.

Retaliation against any person who has in good faith reported a violation or a suspected violation of law, this Policy or other Fortinet policies, or against any person who is assisting in good faith with any investigation, is prohibited.

Reporting Complaints***Duty to Report***

If you have reason to believe that you have become aware of questionable Compliance Matters, you must immediately report those facts pursuant to this Policy. Examples of matters requiring you to make a report include (but are not limited to) the following:

- fraud, deliberate error, or gross negligence in the preparation, evaluation, review or audit of any of Fortinet’s financial statements;
- fraud, deliberate error, or gross negligence in the recording and maintaining of Fortinet’s financial records;
- deficiencies in, or noncompliance with, Fortinet’s internal controls;
- misrepresentation, or false statement, to or by an employee regarding a matter contained

- in Fortinet's financial records, financial reports or audit reports;
- the existence of side letters, side agreements or side arrangements containing items such as return rights, future deliverables, or other matters with Fortinet customers, distributors or resellers;
- bribes, kickbacks, or stealing or misappropriating Fortinet assets;
- misappropriation by Fortinet personnel of third parties' intellectual property or other assets;
- violation of laws against trading on inside information, or any non-compliance with any Fortinet insider trading policy;
- violation of Fortinet's policy against conflicts of interest;
- violation of U.S. federal securities laws or Fortinet's anti-corruption policies, including the Foreign Corrupt Practices Act (FCPA), or similar laws,
- violation of trade laws and import / export laws; and/or
- deviations from full and fair reporting of Fortinet's financial condition.

Procedures to Make a Report

For any concerns regarding Compliance Matters, including accounting, internal accounting controls, or auditing matters, Fortinet employees must submit such concerns (confidentially and anonymously, if they wish) in any one or more of the following ways:

- via electronic mail directly to the Chairperson of the Audit Committee at auditcommittee@fortinet.com;
- via electronic mail to Fortinet's General Counsel at generalcounsel@fortinet.com;
- via the Internet website operated by NAVEX (<http://www.ethicspoint.com>) or through a link provided on Fortinet's internal website;
- via telephone by calling the various hotlines operated by NAVEX toll-free, including in the US at 888-359-6290; or
- via regular mail to:

Accounting Concerns
c/o General Counsel
Fortinet, Inc.
899 Kifer Road
Sunnyvale, California 94086

or

Audit Committee Chairperson
c/o Corporate Secretary
Fortinet, Inc.
899 Kifer Road
Sunnyvale, California 94086.

Except for complaints sent directly to the Audit Committee, all complaints hereunder will be forwarded to the General Counsel's Office for coordination of their treatment as set forth below.

Treatment of Complaints

1. Receipt of complaints will be acknowledged to the sender, within a reasonable period following receipt, if appropriate information for response is supplied.

2. Complaints involving non-accounting, non-internal control matters, and/or non-auditing shall be forwarded to the appropriate person or department for possible investigation (*e.g.*, Human Resources), unless the General Counsel deems other treatment is necessary (*e.g.*, such complaint involves a finance employee or executive officer).

3. With respect to complaints not initially directed to the Audit Committee regarding accounting, internal controls, and/or auditing matters, the General Counsel will report promptly to the Audit Committee matters he or she deems significant. The Audit Committee shall oversee an investigation of such significant complaints, as well as any complaints initially directed to the Audit Committee, as it determines to be appropriate.

4. All other complaints regarding accounting, internal controls and/or auditing matters shall be reviewed under the direction and oversight of the General Counsel, who will involve such other parties (*e.g.*, members of the Finance Department or outside advisors) as deemed appropriate. The General Counsel shall provide the Audit Committee with a periodic report of all significant accounting or auditing complaints received and an update of pending investigations. The Audit Committee may assume the direction and oversight of an investigation of any such complaint.

5. Confidentiality will be maintained to the fullest extent practical, consistent with the need to conduct an adequate review and applicable laws.

6. Reprisal, threats, retribution or retaliation in any way against any person who has in good faith made a complaint or reported a good faith concern, or against any person who assists in any investigation or process with respect to such a complaint or concern, is prohibited. Employees who believe that they have been subjected to any discrimination, retaliation or harassment for having submitted a complaint regarding questionable accounting, internal accounting controls or auditing matters, or the reporting of fraudulent financial information under this policy, or participating in an investigation relating to such a complaint, should immediately report the concern to either the General Counsel, Audit Committee or to any of their supervisors. Any complaint that such discrimination, retaliation or harassment has occurred will be promptly and thoroughly investigated. If such a complaint is substantiated, appropriate disciplinary action will be taken, up to and including termination.

7. To the extent practical and determined appropriate, the General Counsel, Audit Committee or other Fortinet representative will report the consummation of any investigation and any additional information deemed appropriate in the discretion of the team leading the investigation, to the person making the complaint.

8. Nothing in this Policy (nor any other Fortinet policy or agreement) limits, impedes, or restricts your ability to contact, report to, or file a charge or complaint with, the Securities and Exchange Commission (the "SEC"), or, to the extent applicable law prohibits such limitation, impediment, or restriction, any other federal, state, or local government agency or commission (together with the SEC, the "Government Agencies"). This Policy also does not limit your ability to participate and/or assist in any investigation or proceeding that may be conducted by any Government Agencies, including providing information without notice to Fortinet, to the extent applicable law prohibits such limitation. Nothing in this Policy limits your right to seek and/or receive an award for information provided to any Government Agencies or prohibits you from providing truthful information in response to a subpoena or other legal

process, to the extent applicable law prohibits such limitation or prohibition.

Modification

The Audit Committee or the Board of Directors can modify this Policy unilaterally at any time without notice. Modification may be necessary, among other reasons, to maintain compliance with state and federal regulations and/or accommodate organizational changes within Fortinet.

Publication of the Policy

Fortinet shall place this Policy in the Employee Handbook distributed to new employees and shall place a copy of this Policy on Fortinet's Intranet site or equivalent.