FORTINET VENDOR/SUPPLIER CODE OF CONDUCT

"At Fortinet, we are focused on ensuring a culture of ethical business practices, and we expect all of our employees, suppliers, and partners to do their part to continue to build an extremely ethical, highly reputable business."

– Ken Xie Founder, Chairman and CEO, Fortinet, Inc.

Fortinet's mission is to continue to innovate security to be the best, most well-respected security company worldwide. As part of that mission, compliance and ethical practices are key, and in order to do business with Fortinet we require that all vendors meet our high ethical and professional standards.

Please take this Vendor/Supplier Code of Conduct ("Code") seriously and always feel free to contact your Fortinet representatives if you have any questions or if anything is unclear.

I. APPLICABILITY & GENERAL SCOPE

A) Scope. This Code sets out the expectations of Fortinet, Inc. and each of its affiliates and subsidiaries (together "Fortinet") as to how all Fortinet vendors and suppliers, and their employees, contractors, agents, and subcontractors ("Vendor" or "You") will conduct themselves in a legal and ethical manner. Fortinet expects Vendors/Suppliers to comply not only with all applicable laws, but also with this Code and the Fortinet policies identified herein. Similarly, Fortinet expects Vendor to avoid engaging in anyactivity that involves even the appearance of impropriety. Failure to comply with applicable laws or the Code could subject Vendor to severe civil and/or criminal penalties, along with discipline by Fortinet including but not limited to termination of the relationship. Vendors/Suppliers should always err on the side of ensuring compliance and ethical business practices. Vendor/Supplier shall cooperate with Fortinet's reasonable request to confirm compliance with this policy and shall provide applicable documentation as requested.

B) Amendments. This policy may be updated from time to time in Fortinet's discretion, and it is the Vendor/Supplier's responsibility. The most updated version of the Code shall apply.

II. IMPLEMENTATION OF CODE

As a Fortinet Vendor/Supplier, you must require full adherence with all applicable laws by all of your employees, contractors, agents, and subcontractors. With regard to anti-bribery, anti- corruption, and Foreign Corrupt Practices Act (FCPA) provisions, export control laws, and any other laws applicable to your own suppliers, you should require full compliance by your own suppliers. Fortinet is a U.S. headquartered company and requires its vendors and suppliers to comply in full with the U.S. FCPA and other applicable laws. In order to do business with Fortinet, and by engaging in business with Fortinet, you contractually agree to this Code and agree to fully enforce it and ensure compliance at all times, and to fully

indemnify Fortinet for any noncompliance of this Code. You should conduct periodic training and implement reasonable internal controls, in order to ensure that all your employees, contractors, agents, and subcontractors are informed regarding the requirements herein.

III. COMPLIANCE WITH LAWS, REGULATIONS, & BUSINESS CONDUCT PRACTICES

Fortinet expects Vendor/Supplier to be knowledgeable about all of the laws and those Fortinetpolicies that are referenced herein. Some of the more important laws and policies aresummarized below.

A) Anti-Corruption Laws and No Improper Advantage: Fortinet expects its Vendors/Suppliers to uphold the highest standards of integrity in all business interactions. Fortinet has a zerotolerance policy and prohibits any and all forms of bribery, corruption, extortion, kickbacks and embezzlements. Anti-bribery laws, such as the U.S. FCPA, the United Kingdom Bribery Act, and other country-specific laws, make it unlawful to bribe any person for the purpose of obtaining or retaining business or obtaining an unfair advantage in any business dealing or transaction. You must comply with these laws. Neither You nor any of your agents, contractors or employees may offer, pay, promise or authorize any direct or indirect payments or provide anything of value (including, butnot limited to, gratuities, gifts, favors, travel, entertainment, loans) to any person, including a public sector or government official or employee, for the purpose of obtaining or maintaining business.

The definition of government official or employee for the purpose of the FCPA includes:

- any person holding an executive, legislative, judicial or administrative office, whether elected or appointed
- any official or employee of any public international organization, such as the United Nations or World Bank
- any person acting in any official capacity for or on behalf of a government office, public enterprise or state-owned business
- any political party or party official, any political candidate or any person or entity whom You know, or have reason to believe, will give part of the payments to any of the previously mentioned categories of people, and
- any employee of a business in which the government asserts any management control over or has an ownership stake (e.g. more than 50%) in the enterprise. Control may be demonstrated by having the ability to hire employees or by appointing Board members and key executives. Additional information regarding the FCPA rules and regulations is set forth at the U.S. Department of Justice's website at http://www.usdoj.gov/criminal/fraud/fcpa/.

B) Antitrust and Competition Laws: Fortinet is committed to observing rigorously the applicable antitrust or competition laws of all countries and expects the same from You. Although these laws vary from country to country, they generally prohibit agreements or actions that reduce competition without benefiting consumers, such as price fixing and other collaboration and collusion around pricing. Violations of antitrust or competition laws may result in severe penalties, including large fines and jail terms. You must not agree with any competitors to fix, adjust, or control prices; structure or orchestrate bids to direct a contract to a certain competitor or reseller (bid rigging); boycott Vendors/Suppliers or customers; divide or allocate markets or customers; or limit the production or sale of products or product lines. In addition, You must refrain from discussions, sales tactics, or other arrangements with customers, suppliers, or competitors that unfairly restrain or limit competition. When in doubt, You should always consult with qualified and competent competition counsel.

C) International Trade Laws; Compliance with Export Regulations: Vendors/Suppliers must comply with applicable government economic sanctions and trade laws and embargoes whenacting in the context of any transaction with Fortinet. You must not participate in any economic boycott not sanctioned by the United States Government. United States export control laws govern all exports, re-export, trade laws such as the Trade Agreements Act, or TAA, and use of U.S.-origin technology products, services, and technical data, wherever located. Fortinet requires that You comply fully with all U.S. and applicable foreign and multilateral export laws.

D) Environmental Laws: Vendors/Suppliers must conduct their operations in ways that are environmentally responsible and in compliance with all applicable environmental laws,regulations, and standards, including those that regulate hazardous materials, air, and water emissions, and wastes. Fortinet demonstrates its commitment to environmentally responsible behavior by reducing the footprint of our products, adhering to compliance and regulations worldwide, and adopting responsible approaches to its daily business operations. Fortinet's Environmental Policy establishes a global standard for Fortinet's approach to managing environmental impacts, and covers its suppliers and vendors.

E) Responsible Sourcing. Vendors/Suppliers are expected to meet applicable laws that require the Vendor/Supplier to reasonably assure that the tantalum, tin, tungsten and gold in the productsthey manufacture does not directly or indirectly finance or benefit armed groups thatare perpetrators of serious human rights abuses in the Democratic Republic of the Congo or an adjoining country. Vendors/Suppliers are expected to exercise due diligence on the source and chain of custody of these minerals and make their due diligence measures available to customers upon customer request. They must be familiar with, understand and comply with the Fortinet Conflict Minerals Policy.

F) Human Rights, Labor Laws, and Fair Labor Practices: Vendors/Suppliers must comply with, and require each of its employees, contractors, agents, and subcontractors comply with, all health and safety regulations, laws upholding the rights of persons with disabilities, domestic and international labor laws, and fair labor practices. Per Fortinet's Global Human Rights Policy, Vendors/Suppliers must observe and comply with international principles relating to human rights, including but not limited to the ones expressed in the International Bill of Human Rights, the Trafficking Victims Protection Act and the UK Modern Slavery Act of 2015 (please refer to Fortinet's statement on modern slavery). Violations of local minimum wage and maximum working hour requirements are unacceptable, as are forced labor scenarios and labor contracts that impose unreasonable legal or practical limitations on the workers' ability to leave their employment. Child labor is not to be used. Vendors/Suppliers must never discriminate illegally based on race, color, age, gender, sexual orientation, ethnicity, religion, disability, union membership, marital status, or political affiliation. Vendors/Suppliers shall respect the right of freedom of association in conformance with local law and allow all their workers to form and join trade unions of their own choosing, to bargain collectively, and to engage in peaceful assembly as well as respect the right of workers to refrain from such activities. Workers and/or their representatives shall be able to openly communicate and share ideas and concerns with management regarding working conditions and management practices without fear of discrimination, reprisal, intimidation, or harassment.

G) Securities and Insider Trading Laws: If You possess material, non-public information about Fortinet (also called "inside information"), You may not trade in Fortinet securities or the securities of another company to which the information pertains. You may not engage in any other action to take advantage of or pass on to others (i.e., "tip") material information gained through your relationship with Fortinet until it has been disclosed to the general public. These restrictions also apply to spouses and family members. You should familiarize yourself with these laws and consult qualified counsel for related advice.

H) Information Security and Data Protection: Fortinet expects that its Vendors/Suppliers will understand, track, and fully comply with all laws, rules, standards, and regulations relating to privacy, data protection, security, breach notification, and consumer protection that are relevant to the products and services that Vendor/Supplier supplies or performs as a Fortinet Vendor/Supplier. With respect to any data that Vendor/Supplier collects or processes, or Vendor/Supplier systems that support Fortinet, by virtue of its Vendor/Supplier status, Vendor/Supplier shall meet its obligations as set forth in the Fortinet policies, terms and conditions, and agreements, including without limitation, the Fortinet Information Security Policy Addendum, the Trusted Supplier Program Agreement, and the Fortinet Data Processing Addendum, as

applicable to the Vendor/Supplier. Vendor/Supplier must also keep confidential any information received from or on behalf of Fortinet, not use, collect, disclose, or transfer such information for any purpose other than as originally intended,and implement the appropriate safeguards to ensure the protection, confidentiality, integrity, availability and security of such data. Fortinet's Vendors/Suppliers must all ensure proper processes and controls that ensure in no event does Vendor/Supplier and its Vendors/Suppliers andsuppliers allow any security vulnerabilities, including but not limited to viruses, malware, worms, contaminants, time bombs, time locks, or drop dead devices, traps, trap doors, Trojan Horses, or back doors to be included in any Fortinet component, product or service.

IV. FINANCIAL INTEGRITY AND ACCURATE RECORD KEEPING; DISCLOSURE OF INFORMATION

You must maintain accurate and complete books and records regarding transactions with Fortinet, including but not limited to marketing programs and events. False and misleading accounting practices, slush funds and similar financial practices are prohibited by Fortinet and may violate applicable laws. You must accurately document all transactions related to your contract for Fortinet products or services, and your business records must be retainedin accordance with record retention policies and all applicable laws and regulations. Documents must not be inappropriately altered or signed by your representatives lacking proper authority. To the extent that you sell goods or services to Fortinet, you must invoice Fortinet for goods and services only after they are delivered, except to the extent that the related purchase agreement expressly permits advance invoicing. If the purchase agreementpermits invoicing or payment in advance of delivery, such items will be clearly identified in the invoice line item description using such terms as "deposit," "prepayment," or "advance billing." You may not act as a "pass through" party where the only "service" provided by theVendor/Supplier is to be an intermediary between Fortinet and a third party. All requests for non- standard discounts must be accurate and for legitimate business purposes. Margins derivedfrom misleading and/or unjustified non-standard discounts are inappropriate, and may not be used to pay or otherwise reward a customer, employee, or other third party.

V. FAIR MARKETING/SALES PRACTICES; COMPLIANCE WITH CONTRACTUAL OBLIGATIONS

A) Marketing and Sales Practices: Vendors/Suppliers must not engage in any misleading or deceptivepractices. All advertising, marketing, or promotional activities that reference or implicate Fortinet, its logo, or products and services in any manner, must comply with all laws, rules, and regulations, as well as all related Fortinet policies, and must be truthful and accurate. Advertising must clearly disclose the material terms and limitations of advertised offers and any pass-through terms if mandated by Fortinet. Vendors/Suppliers should not misrepresent products, services, and prices, or make unfair, misleading, inaccurate, exaggerated or false claims about, or comparisons with, competitor offerings.

B) Conflicts of Interest: The term "conflict of interest" describes any circumstance that could cast doubt on your or a Fortinet representative's ability to act with total objectivity, and, with respect to Fortinet representatives, their ability to act in the best interests of Fortinet. Fortinet wants its Vendors/Suppliers' loyalty to be free from any conflicts ofinterest. If You believe that You have an actual or potential conflict with Fortinet or anyof its employees, then You must report all pertinent details to Fortinet. You must not ask, encourage, or participate in any violation by Fortinet employees or other representatives of Fortinet's Code of Business Conduct and Ethics or of Fortinet's applicable travel and expense policies, and you should help ensure Fortinet employees do not have conflicts of interest, such as any ownership interest in a Vendor/Supplier.

Gifts and Courtesies: Gift giving is proper only if reasonable, non-excessive, and done aspart of a valid and approved program or promotion. You shall not seek special favors, such as favorable treatment in connection with a deal, by offering or providing lavish gifts, kickbacks or things of value which are out of proportion given the situation at hand. Always use common sense and good judgment. It is appropriate for Fortinet to accept an invitation from a Vendor/Supplier to reasonable, fully substantive education or training seminars that legitimately and properly contribute to Fortinet's business, subject to Fortinet's processes and approval; however, it is inappropriate to offer lavish accommodations and/or sightseeing trips to Fortinet employees attending such training. As always, consider the frequency and timing of any such gift to prevent any perceived impropriety. You must ensure that expenditures on Fortinet personnel or representatives are reasonable and in the ordinary and proper course of business. A general guideline for evaluating whether a gift or other business courtesy is appropriate is whether public disclosure would be embarrassing to You, to Fortinet, or to the recipient. You must not exceed local gift giving customs and practices, nor violate related laws that may vary in different countries. Regardless of local practice, any payment or gift to a person acting in an official capacity and/or on behalf of the government, where designed to influence that individual's acts or decisions, is improper. Vendors/Suppliers are responsible for reading, understanding, and complying with Fortinet Anti-Corruption Policy.

C) Compliance with Contractual Obligations: Vendors/Suppliers must comply with their obligations underall agreements in place with Fortinet and others. Vendors/Suppliers should contact their Fortinet representative if they have specific questions about the various provisions in their agreements with Fortinet.

D) Intellectual Property Laws; Confidentiality: Notwithstanding anything to the contrary, Fortinet retains all intellectual property and ownership rights related to its products and technology. Vendors/Suppliers must not infringe on Fortinet's copyrights, patents, trademarks, tradesecrets, and other intellectual property rights. Vendors/Suppliers are also prohibited from infringing on the intellectual property rights of third parties in any manner. You must not use Fortinet's patented technology or reproduce copyrighted software, documentation, or othermaterials without appropriate written permission. You must

safeguard confidential information by not transferring, publishing, using, or disclosing it except as in accordance with applicable regulations, contractual requirements, or this Code. You should safeguard and protect confidential or personal information or information that is protected by privacy standards, and you should share internally this information only with those employees or agents with a need to know for proper and authorized purposes, and not misused or disclosed to unauthorized third parties.

VI. COMPLIANCE; ENFORCEMENT & REPORTING

Business Controls; Audits: Vendors/Suppliers must maintain effective policies, documentation, training, and business controls that are effectively designed to prevent and detect unlawful conduct, or conduct that violates the policies discussed herein, by their employees, contractors, agents and subcontractors. Vendors/Suppliers shall ensure that their business controls contain the following components: (i) periodic risk assessments that lead to adjustments to existing policies and practices, when necessary; (ii) a written code of conduct or similar policy that expressly confirms Vendors/Suppliers' commitment to, andstates objectives for, their compliance and ethics programs; (iii) designated company representatives responsible for overseeing and implementing such compliance and ethics programs; (iv) compliance and ethical business practices training, and (v) clearly communicated mechanisms for employees, contractors, agents, or subcontractors to report misconduct or seek guidance without fear of retaliation. In addition, all Vendors/Suppliers accept that Fortinet will, and authorizes Fortinet to, conduct due diligence screenings, reviews and audits, including, but not limited to, export compliance screening and others. Vendors/Suppliers agrees to, and must provide reasonable assistance with respect to, anyinvestigation, audit or review by Fortinet of any suspected violation of this Code or applicable laws, and will allow Fortinet reasonable access to all facilities, records and documentation concerning their compliance with this Code and laws applicable to theirsale and distribution of Fortinet products and services. Vendors/Suppliers should contact their Fortinet Vendor/Supplier manager if they have any questions regarding Fortinet's policies or thisVendor/Supplier Code of Conduct.

A) Reporting Violations: Vendors/Suppliers are expected to promptly report any conduct by You, Your employees, contractors, agents, subcontractors and other representatives that Youhave reason to believe constitutes, or may constitute, an actual, apparent, or potential violation of this Code, Fortinet's Code of Business Conduct and Ethics, Fortinet's Anti- Corruption Policy, or applicable laws. Reports should be made promptly and pursuant toFortinet's on-line reporting tool managed by an independent third party, **NAVEX**, **at the following link: http://www.ethicspoint.com/, or directly to Fortinet's legal team atlegal@fortinet.com**.