

FORTINET PARTNER CODE OF CONDUCT

Thank you for your partnership with Fortinet as we work together to provide the best, most innovative security solutions to protect our customers.

Fortinet's mission is to continue to innovate security to be the #1 most well-respected security company worldwide. As part of that mission, compliance and ethical practices are key, and we appreciate our partners ensuring all of their hard work and efforts on behalf of Fortinet and its products are always performed at high ethical and professional standards.

Please take this Partner 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

This Code sets out the expectations of Fortinet Inc. and each of their affiliates and subsidiaries (together "Fortinet") as to how all Fortinet partners, including distributors, resellers, alliance partners, and their employees, independent contractors, and agents ("Partner" or "You") will conduct themselves in a legal and ethical manner. Fortinet expects Partners to comply not only with all applicable laws, but also with this Code and the Fortinet policies identified herein. Similarly, Fortinet expects You to avoid engaging in any activity that involves even the appearance of impropriety. Failure to comply with applicable laws or the Code could subject You to severe civil and/or criminal penalties, along with discipline by Fortinet including but not limited to termination of the relationship.

II. IMPLEMENTATION OF CODE

As a Fortinet partner, you must require full adherence with all applicable laws by all of your employees, agents, suppliers and downstream partners. With regard to anti-bribery or Foreign Corrupt Practices Act (FCPA) provisions, export control laws, and any other laws that should be applicable to downstream partners, you should require full compliance by downstream partners. In addition, by partnering 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 and agents are informed regarding the requirements herein.

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

Fortinet expects You to be knowledgeable about all of the laws and those Fortinet policies that are referenced herein. Some of the more important laws and policies are summarized below.

- A) Anti-Corruption Laws: Fortinet expects its Partners to uphold the highest standards of integrity in all business interactions. Fortinet has a zero tolerance 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. You are responsible to comply in full with Fortinet's Anti-Corruption Policy. Neither You nor any of your agents or employees may offer, pay, promise or authorize any direct or indirect payments or provide anything of value (including, but not 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) Gifts and Courtesies: Gift giving is proper only if reasonable, non-excessive, and done as part of a valid and approved program or promotion when related to Fortinet products and services. 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 to invite customers to reasonable, fully substantive education or training seminars, subject to Fortinet's processes and approval; however, it is inappropriate to offer lavish accommodations and/or sightseeing trips to customers 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 customers

and 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. You are responsible for reading, understanding, and complying with [Fortinet Anti-Corruption Policy](#).

- C) 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 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.
- D) International Trade Laws; Compliance with Export Regulations: Partners must comply with applicable government economic sanctions and trade laws and embargoes when acting in the context of any transaction related to Fortinet products and/or services. 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, and use of U.S.-origin products, services, and technical data, wherever located. Fortinet requires that You comply fully with all U.S. and applicable foreign and multilateral export laws. This means You may not export, re-export or transship Fortinet products, services or technical data (1) to any destinations subject to U.S. embargoes or trade sanctions; (2) to any entity or individual specified on U.S. government-maintained exclusion lists, or (3) for use directly or indirectly in the design, development, or fabrication of nuclear, chemical, or biological weapons or missile technology. When placing orders with Fortinet, always ensure the information on the orders is accurate and complete. For example, always correctly identify the end customer and never identify an order as a stocking order if the end customer is identified. In addition, please always abide by the trade compliance and territory limitations in your partner agreement with Fortinet.

- E) Environmental Laws: Partners must conduct their operations in ways that are environmentally responsible and in compliance with all applicable environmental laws, regulations, and standards. Partners should always ensure full compliance with laws such as RoHS, WEEE and other applicable environmental laws. 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 Fortinet's channel partners are expected to comply with it.
- F) Human Rights, Labor Laws, and Fair Labor Practices: Partners must comply with, and require each of their suppliers to 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](#), partners 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. 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. Partners must never discriminate illegally based on race, color, age, gender, sexual orientation, ethnicity, religion, disability, union membership, marital status, or political affiliation. Partners 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) Data Protection: Fortinet expects that its Partners will understand, track and comply with all laws and regulations relating to data protection that are relevant to their actions as a Fortinet Partner. With respect to any data Partner collects or receives by virtue of its Partner status, Partner shall apply the same level of data protection as set forth in Fortinet's Privacy Policy, as posted online. Partner must also keep confidential any

personal information received from Fortinet, not use such information for any purpose other than as originally intended, and implement the appropriate safeguards to ensure the protection, integrity and security of such personal information. To the extent applicable, Partner must fully comply with all privacy laws, such as the European Union General Data Protection Regulation, or GDPR, and other applicable privacy laws in the relevant regions.

IV. FINANCIAL INTEGRITY AND ACCURATE RECORD KEEPING

You must maintain accurate and complete books and records regarding sales of Fortinet products and services and all related transactions, such as for 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 retained in 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 agreement permits 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 the 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 derived from 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. Prohibition on Returns; Prohibition on “Side Agreements”

You understand and agree that Fortinet Sales representatives and executives are not authorized to bind Fortinet, and that, in the event any sales agreement is not signed by Fortinet’s General Counsel, Fortinet is entitled to declare such agreement invalid. No partner is entitled to return any products except in limited circumstances pursuant to a formal agreement signed by Fortinet’s General Counsel. Partners are fully responsible if they place any order with Fortinet without the existence of a corresponding end user agreement or order for such product, and the partner will not be entitled to return the products and services even if the end customer deal never materializes and Fortinet shall not be obligated to assist with selling such product through.

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

- A) Marketing and Sales Practices: Partners must not engage in any misleading or deceptive practices. 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. Partners 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 ability to act with total objectivity with regard to the distribution of Fortinet products and services. Fortinet wants its Partners’ loyalty to be free from any conflicts of interest. If You believe that You have an actual or potential conflict with Fortinet or any of its employees, then You must report all pertinent details to Fortinet. You must not ask or encourage Fortinet employees to violate Fortinet’s Business Conduct Guidelines, and you should help ensure Fortinet employees do not have conflicts of interest, such as any ownership interest in a partner or end customer.
- C) Compliance with Contractual Obligations: Partners must comply with their obligations under all agreements in place with Fortinet and others. Partners 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. Partners must not infringe on Fortinet’s copyrights, patents, trademarks, trade secrets, and other intellectual property rights. Partners 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 other materials 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 with a need to know for proper and authorized purposes, and not misused or disclosed to unauthorized third parties.
- E) Government Sector Sales Rules: Partners must become familiar with, track, understand,

and comply with all laws and regulations relating to sales to government entities and government sector customers that are relevant to their Partner status. Partners shall strictly observe the laws, rules, and regulations that govern the acquisition of products and services by any governmental entity of any country and the performance of government contracts.

VII. COMPLIANCE; ENFORCEMENT & REPORTING

- A) Business Controls: Partners must maintain effective policies, documentation and business controls that are capable of preventing and detecting unlawful conduct by their employees, agents and business partners. Partners 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 Partners' commitment to, and states objectives for, their compliance and ethics programs; (iii) designated company representatives responsible for overseeing and implementing such compliance and ethics programs; and (iv) clearly communicated mechanisms for employees to report misconduct or seek guidance without fear of retaliation. In addition, all Partners accept that Fortinet will, and authorizes Fortinet to, conduct due diligence screenings, including, but not limited to, export compliance screening and others, and Partner hereby certifies it has completed (or for new Partner applicants, it will complete promptly upon becoming a Partner), and will continue to complete, the required partner ethics and compliance training on an ongoing basis. Partners agree to, and must provide reasonable assistance with respect to, any investigation, 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 their sale and distribution of Fortinet products and services. Partners should contact their Fortinet Partner manager if they have any questions regarding Fortinet's policies or this Partner Code of Conduct. You also may report any conduct by Your employees, independent contractors and agents, and representatives that You have reason to believe constitutes an actual, apparent, or potential violation of this Code, Fortinet's Business Conduct Guidelines, or applicable laws relating to the sale or distribution of Fortinet products/services. Reports should be made pursuant to Fortinet'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 at legal@fortinet.com.