EXTREME NETWORKS, INC.

CODE OF BUSINESS CONDUCT AND ETHICS

Amended February 12, 2025

Policy Statement

At Extreme Networks, Inc., we are committed to conducting our business affairs honestly and in an ethical manner. That goal cannot be achieved unless each of us accepts responsibility to promote integrity and demonstrate the highest level of ethical conduct in all of our activities. Activities that may adversely impact our reputation for integrity should be avoided. The key to achieving our business goal and complying with this Code of Business Conduct and Ethics (the "Code") is exercising good judgment. This Code was adopted to encourage:

- Honest and ethical conduct, including fair dealing and the ethical handling of actual or apparent conflicts of interest;
- Full, fair, accurate, timely and understandable disclosure;
- Compliance with applicable governmental laws, rules and regulations;
- Prompt internal reporting of any violations of law or the Code;
- Accountability for adherence to the Code, including fair process by which to determine violations;
- Consistent enforcement of the Code, including clear and objective standards for compliance;
- Protection for persons reporting any such questionable behavior;
- The protection of the Company's legitimate business interests, including its assets and corporate opportunities; and
- Confidentiality of information entrusted to directors, officers and employees by the Company and its customers.

This Code applies to all employees (including those employed by professional employment organizations), officers, and members of the Board of Directors (collectively, the "Directors") of Extreme Networks, Inc. and its subsidiaries and branches in all locations (collectively the "Company" or "Extreme Networks"). The parties to whom the Code applies are collectively referred to as the Covered Parties. The Code is based on the Company's core values, good business practices and compliance with applicable law.

Managers set an example for other employees and are often responsible for directing the actions of others. Each manager and supervisor is expected to take necessary actions to ensure compliance with this Code, to provide guidance and assist employees in resolving questions concerning the Code and to permit employees to express any concerns regarding compliance with this Code. No one has the authority to order another employee to act contrary to this Code.

A key prerequisite to conducting business in an ethical and legal manner is to hire the best employees who share this goal and practice it. To this end, the Company will exercise due diligence when hiring and promoting employees. Where legally permitted, the Company will make reasonable inquiries into the background of each individual who is a candidate for such a position. All such inquiries will be made in accordance with applicable law and good business practice.

Compliance with the Code

All Covered Parties are expected to become familiar with and understand the requirements of the Code. Most importantly, each of us must comply with the Code, and support others in their efforts to comply with it as well.

The Company's Chief Executive Officer ("CEO") is responsible for ensuring that the Code is established and effectively communicated to the Covered Parties. Although the day-to-day compliance issues will be the responsibility of the Company's managers, the CEO has ultimate accountability with respect to the overall implementation of and successful compliance with the Code.

The Company will ensure that the Covered Parties have access to the Code on the Company's website and will provide periodic training on the Code to employees and officers.

Code Requirements

1. Compliance with Laws and Regulations

Extreme Networks is committed to full compliance with the laws and regulations of all jurisdictions in which it operates. Numerous laws and regulations define and establish obligations with which the Company, our employees and agents must comply.

If you violate laws or regulations in performing your duties for the Company, you not only risk individual indictment, prosecution and penalties, in addition to civil actions and penalties from the local authorities, you may also subject the Company to risks and penalties. If you violate laws or regulations in performing your duties for the Company, you may also be subject to immediate disciplinary action, including possible termination of your employment with the Company, as permitted by applicable laws.

2. Import / Export Control

Each of us is responsible for ensuring that Extreme Networks and its agents, channel partners, distributors and resellers (collectively, our “Resellers”) complies with applicable trade regulations, including U.S. export controls, which are intended to control foreign distribution of U.S. origin technology to prevent unauthorized access. Under no circumstance should a Covered Party or Reseller engage in marketing, service or sales of Extreme Networks products or technology to embargoed or prohibited countries, end users or uses, or allow products to be exported without proper export documentation or a license when required.

In addition, when importing products, employees must obey the import requirements of any applicable U.S. or foreign government agencies. All questions and inquiries regarding the identity, value or duty due on imported products must be answered truthfully and completely.

3. Compliance with Anti-Corruption Laws

Extreme Networks requires its employees to fully comply with the U.S. Foreign Corrupt Practices Act ("FCPA"), the U.K. Bribery Act, as well as all other applicable anti-corruption laws everywhere we do business. Covered Parties, as well as our Resellers, are prohibited from making, offering, authorizing or promising any payment of any money, or offer, gift, promise to give, or authorize the giving of anything of value to any Public Official for the purpose of influencing or inducing that official to affect any government act or decision or to assist the Company in obtaining or retaining business or any other unfair or improper advantage. For the purposes of this Code, "Public Official" includes anyone with any affiliation to a government department, agency, or instrumentality, at any level, including:

- Government employees (at any level, whether national, provincial or local);
- Directors, officers and employees (regardless of position or level) of entities owned or controlled by, or affiliated with, a foreign government (*e.g.*, state owned enterprises, public universities, public hospitals);
- Members of public international organizations;
- Members of the military or royal families;
- Candidates for political office;
- Political party officials;
- Anyone acting on behalf of any of the above, such as lobbyists or advisors; and
- Journalists of state-owned or controlled media.

The anti-corruption laws prohibit not only improper payments of money (for example, a payment to a Public Official to obtain an operating license, a tax incentive or exemption, or a regulatory change), but also excessive hospitality in the form of lavish gifts, entertainment, travel, accommodations or dining for the purpose of influencing or inducing a benefit from a Public Official. This policy extends to indirect payments made through agents and includes the use of personal funds. Company Directors, officers, and employees are prohibited from doing through a third-party intermediary that which they are prohibited from doing directly. The FCPA prohibits giving anything of value, directly or indirectly, to officials of foreign governments or foreign political candidates to obtain or retain business. It is strictly prohibited to make illegal payments to government officials of any country.

Extreme Networks also requires that books and records accurately report all payments made by or on behalf of the Company.

The FCPA and other similar laws carry both civil and criminal penalties for noncompliance. Additional guidance regarding compliance with anti-corruption laws is set forth in Extreme Networks' Global Anti-Corruption Compliance Policy.

4. Gifts, Entertainment, Travel, and Hospitality for Public Officials and Commercial Parties

You may not give or offer or promise to give any excessive entertainment or gifts other than of nominal value to any person or organization to attract or retain business. All decisions

regarding the investing of our assets or the purchasing of goods and services must be made on the basis of applicable investment or acquisition criteria, and in a way that preserves Extreme Networks' integrity. Business-connected gifts, entertainment, meals, hospitality, travel, or other favors may not be extended to any party, including intermediaries, clients or suppliers (current or prospective), unless they:

- have a lawful business purpose;
- are kept to a reasonable value;
- are not intended to improperly influence acts or decisions;
- are appropriate to the business relationship and local custom;
- are legal in both your country and the country of the recipient;
- do not violate the standards of conduct of the recipient's organization or any contractual agreement with a customer;
- are properly documented; and
- where necessary, proper approval is obtained prior to giving any gift, entertainment, or hospitality.

For any gifts, entertainment, or hospitality for Public Officials or commercial customers with whom Extreme Networks does business under U.S. federally funded contracts, you must obtain advance written approval by Extreme Networks' Legal Department and your manager if the value of such payment, gift, entertainment, or hospitality exceeds USD$20 for a single gift or USD$50 per year (or less, if applicable law has a lower limit). For more information and further details regarding permissible gifts, entertainment and hospitality, please see Extreme Networks' Global Anti-Corruption Compliance Policy.

To avoid even the implication of impropriety, you should also decline any gift, favor, entertainment or anything else of value from current or prospective intermediaries, clients, suppliers or contractors or their representatives except for:

- Gifts that do not have substantial monetary value given at holidays or other special occasions.
- Covered Parties may not accept any gifts, entertainment, or hospitality with a fair market value in excess of USD$20 per gift or USD$50 per year from suppliers with whom the Company does business under U.S. federally funded contracts, unless the Company's Legal Department has given advance written approval.
- Employees who receive gifts, entertainment, or hospitality with a fair market value in excess of USD$200 must report it to their manager promptly. Executive officers or Directors who receive such gifts must promptly report them to the Chief Legal, Administrative & Sustainability Officer (or the Chief Financial Officer, if the executive officer in question is the Chief Legal, Administrative & Sustainability Officer).
- Reasonable entertainment at lunch, dinner or business meetings where the return of the expenditure on a reciprocal basis is likely to occur and would be properly chargeable as a business expense.

Ultimately, you must exercise good business judgment in deciding which situations are unacceptable. If you ever have any doubt as to the acceptability of any entertainment activity, consult with the Extreme Networks' Legal Department or Extreme Networks' Chief Legal, Administrative & Sustainability Officer by sending an email to LegalCompliance@Extremeneworks.com.

5. Political and Charitable Activities and Contributions

You should not use the Company's funds for political contributions of any kind to any political candidate or person who holds any government office without prior written approval from the Extreme Networks' Legal Department. "Political contributions" include direct and indirect payments, loans, advances, deposits, or gifts of money, or any service. It also includes subscriptions, memberships, tickets, and the purchase of advertising space, payment of expenses, or compensation of employees for a political organization, candidate, or public official. You may participate in trade associations on behalf of the Company that support our industry through lobbying efforts and politically related activities.

The Company strives to make positive contributions in the communities in which it operates and encourages its employees to do the same. The Company's corporate philanthropy is principally directed to educational, scientific and humanitarian endeavors across the globe. Employees wishing to make contributions in the name of Extreme Networks – whether by financial contributions or volunteer activities – must receive prior written approval from the Extreme Networks' Legal Department. Sometimes, customers or suppliers ask that we make a contribution to a charity or nonprofit organization. Charitable contributions may not be given by the Company or requested by an employee, customer, supplier, Public Official, or other business partner as a condition of or to influence a business decision (no "quid pro quo") or be made for the benefit of any one individual.

6. Full, Fair, Accurate, Timely and Understandable Disclosure

All Company disclosures in reports and documents that the Company submits to any government authority, and other public communications made by the Company, must be full, fair, accurate, timely and understandable. You must take all steps available to assist Extreme Networks in its disclosure responsibilities, consistent with your role within the Company. In particular, you are required to provide prompt and accurate answers to all inquiries made to you in connection with the Company's preparation of its public reports and disclosures. The Company's CEO and Chief Financial Officer ("CFO") are responsible for designing, establishing, maintaining, reviewing and evaluating the effectiveness of the Company's disclosure controls and procedures (as such term is defined by applicable SEC rules) on a quarterly basis.

The Company's CEO, CFO, and Corporate Controllers (and such other Company officers designated from time to time by the Audit Committee, collectively, the "Senior Officers") will take all steps necessary or advisable to ensure that all Company disclosures in reports and documents filed with or submitted to the SEC, and all disclosures in other public communication made by the Company, are full, fair, accurate, timely and understandable.

Senior Officers are also responsible for establishing and maintaining adequate internal control over financial reporting to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes, in accordance with generally accepted accounting principles ("GAAP"). The Senior Officers will take all necessary steps to ensure compliance with our system of internal controls and GAAP. For example, Senior Officers will ensure that Extreme Networks makes and keeps books, records, and accounts which accurately and fairly reflect the transactions and dispositions of our assets in reasonable

detail. Senior Officers will also ensure that we devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that:

- transactions are executed in accordance with management's general or specific authorization;
- transactions are recorded as necessary to: (i) permit preparation of financial statements in conformity with GAAP or any other criteria applicable to such statements, and (ii) maintain accountability for assets;
- access to assets is permitted, and receipts and expenditures are made, only in accordance with management's general or specific authorization;
- the method that the Company uses to record its assets is consistent with existing assets at reasonable intervals, and appropriate action is taken with respect to any differences; and
- all to permit prevention or timely detection of unauthorized acquisition, use or disposition of assets that could have a material effect on our financial statements.

Any attempt to enter inaccurate or fraudulent information into the Company's accounting system will not be tolerated and may result in disciplinary action, up to and including termination of employment, as permitted by applicable laws.

7. Insider Trading

You should never trade securities on the basis of confidential information acquired through your employment or fiduciary relationship with the Company. You are prohibited under applicable law and Company policy from purchasing or selling Company securities, directly or indirectly, on the basis of material non-public information concerning the Company Any person possessing material non-public information about Extreme Networks must not engage in transactions involving Company securities until this information has been released to the public. Generally, material information is that which would be expected to affect (i) the investment decisions of a reasonable investor, or (ii) the market price of the stock. You must also refrain from trading in the stock of other publicly held companies, such as existing or potential customers or suppliers, on the basis of material confidential information obtained in the course of your employment or service as an officer or Director. It is also illegal to recommend a stock to someone else (*i.e.*, "tip") on the basis of such information. If you have a question concerning appropriateness or legality of a particular securities transaction, consult with the Company's Legal Department. Covered Parties are subject to Extreme Networks' Insider Trading Policy, a copy of which has been made available to each such Covered Party.

8. Conflicts of Interest and Corporate Opportunities

Covered Parties must avoid any situation in which your personal interests conflict or even appear to conflict with the Company's interests.

You owe a duty to the Company not to compromise the Company's legitimate interests and to advance such interests when the opportunity to do so arises in the course of your employment. You must perform your duties to the Company in an honest and ethical manner. You must handle all actual or apparent conflicts of interest between your personal and professional relationships in an ethical manner. You should avoid situations in which your personal or financial interests conflict, or even appear to conflict, with those of the Company. You may not engage in activities that compete with the Company or compromise its interests. You should not take for your own benefit

opportunities discovered in the course of employment that you have reason to know would benefit the Company. The following are examples of actual or potential conflicts:

- you, directly or indirectly through someone else, receive improper personal benefits as a result of your position in the Company;
- you use Company's property for your personal benefit;
- you engage in activities that interfere with your loyalty to the Company or your ability to perform Company duties or responsibilities effectively;
- you work simultaneously (whether as an employee or a consultant) for a competitor, customer or supplier;
- you, directly or indirectly, have a financial interest in a customer, supplier, or competitor which is significant enough to cause divided loyalty with the Company, or the appearance of divided loyalty. (The significance of a financial interest depends on many factors, such as size of investment in relation to your income, net worth and/or financial needs, your potential to influence decisions that could impact your interests, and the nature of the business or level of competition between the Company and the supplier, customer or competitor);
- you, directly or indirectly, acquire an interest in property (such as real estate, patent or other intellectual property rights or securities) in which you have reason to know the Company has, or might have, a legitimate interest;
- you, directly or indirectly, receive a loan or a guarantee of a loan or the benefits thereof from a customer, supplier or competitor (other than a loan from a financial institution made in the ordinary course of business and on an arm's-length basis);
- you divulge or use the Company's confidential information, such as financial data, customer information, or computer programs, for your own purpose;
- you make gifts or payments, or provide special favors, to customers, suppliers or competitors (or their immediate family members) with a value significant enough to cause the customer, supplier or competitor to make a purchase, or take or forego other action, which is beneficial to the Company and which the customer, supplier or competitor would not otherwise have taken; or
- you are given the right to buy stock in other companies or you receive cash or other payments in return for promoting the services of an advisor, such as an investment banker, to the Company.

The Company and Covered Parties may not do indirectly through third parties what the Company or Covered Parties could not do directly under this Code or applicable law, rules and regulations.

Neither you, nor members of your immediate family on your behalf or with your knowledge, are permitted to solicit or accept valuable gifts, payments, special favors or other consideration from customers, suppliers, or competitors. Any exchange of gifts must be conducted so that there is no appearance of impropriety. Gifts may be given only in compliance with anti-corruption and other applicable laws.

Conflicts are not always clear-cut. If you become aware of a conflict described above or any other conflict, potential conflict, or have a question as to a potential conflict, you should contact the Company's Legal Department and follow the procedures described in this Code. You should act only after the conflict has been reviewed and you have received prior written approval from the Extreme Networks' Legal Department. By fully disclosing the potential conflict before you act, you help ensure that business is done objectively, fairly, and in line with Company policy.

9. Confidentiality

All confidential information concerning the Company is the property of the Company and must be protected. Confidential information includes all non-public information relating to the Company, or other companies, that might be of use to competitors, or harmful to the relevant company or its customers if disclosed. You must maintain the confidentiality of such information entrusted to you by Extreme Networks, its customers and its suppliers, except when disclosure is authorized by the Company or required by law. If you believe you are required by law to disclose confidential information, you must notify the Legal Department prior to disclosure. If you plan to disclose confidential information to a third party, you must first ensure that a non-disclosure agreement exists between Extreme Networks and the third party.

Examples of confidential information not only include trade secrets, but also include without limitation non-public: personal data (data that could identify an individual or as otherwise defined under applicable law); business trends and projections; information about financial performance; new product or marketing plans; research and development ideas or information; manufacturing processes; information about potential acquisitions, divestitures and investments; stock splits, public or private securities offerings or changes in dividend policies or amounts; significant personnel changes; and existing or potential major contracts, orders, suppliers, customers or finance sources or the loss thereof. Your obligation with respect to confidential information extends beyond the workplace. In that respect, it applies to communications with your family members and continues to apply even after your relationship with the Company terminates.

10. Fair Dealing, Antitrust, Procurement Integrity and Competition

Our goal is to conduct our business with integrity. You should endeavor to deal honestly with the Company's customers, suppliers, competitors, and employees. Under applicable laws, the Company is prohibited from engaging in unfair methods of competition, and unfair or deceptive acts and practices. You should not take unfair advantage of anyone through manipulation, concealment, abuse of privileged information, misrepresentation of material facts, or any other unfair dealing. Examples of prohibited conduct include, but are not limited to:

- bribery or payoffs to induce business or breaches of contracts by others (see Sections 4 and 5 above);
- acquiring a competitor's trade secrets;
- making false, disparaging, or deceptive claims or comparisons about competitors or their products or services; or
- price-fixing or other pricing arrangements which unfairly restrict competition.

In addition, most countries have well developed bodies of law designed to encourage and protect free and fair competition. The Company is committed to obeying both the letter and spirit of these laws.

These laws often regulate the Company's relationships with its sales representatives, resellers, and customers. Antitrust and competition laws generally address the following areas: pricing practices (including price discrimination); discounting; terms of sale; credit terms; promotional allowances; secret rebates; product bundling; restrictions on carrying competing products; termination; and many other practices.

Antitrust and competition laws also strictly govern relationships between the Company and its competitors. Although the spirit of these laws, known as "antitrust," "competition," "consumer protection" or unfair competition laws, is straightforward, their application to particular situations can be quite complex. To ensure that the Company complies fully with these laws, each of us should have a basic knowledge of them and should involve the Legal Department early on when questionable situations arise.

Special rules apply for U.S. government contracts. “Bid or proposal information” is information submitted to a federal agency in connection with a bid or proposal, including cost or pricing data, indirect costs and direct labor rates, proprietary information, and other information marked by a contractor as “contractor bid or proposal information.” “Source selection information” is information not previously made available to the public that is prepared for use by a federal agency in evaluating a bid or proposal, such as bid or proposal prices, source selection plans, technical evaluation plans and the results of technical evaluations or proposals, cost or price evaluations of proposals, competitive range determinations, rankings of bids or proposals, and reports and evaluations of source selection panels, boards, or advisory councils.

You must not accept or solicit competitor bid or proposal information, or source selection information pertaining to the Company’s own or others’ bids or proposals, before the award of a federal agency procurement contract to which the information relates. After the contract is awarded, requests for source selection information or bid or proposal information must only be submitted through proper channels to persons with proper authority to consider and grant such requests.

11. Protection and Proper Use of Company Assets

You should protect the Company's assets and ensure their proper use. Company assets, both tangible and intangible, are to be used only for legitimate business purposes of the Company and only by authorized employees, officers, Directors, or consultants. Intangible assets include, but are not limited to: intellectual property such as trade secrets; patents, trademarks and copyrights; business, marketing and service plans; engineering and manufacturing ideas; designs; databases; proprietary Company records; organizational data; and any unpublished financial data and reports. Unauthorized alteration, destruction, use, disclosure or distribution of Company assets violates Company policy and this Code. Theft, waste of, or carelessness in using any company assets or funds have an adverse impact on the Company's operations and profitability and will not be tolerated.

The Company provides computers and other information technology devices (each a “Device” or collectively, “Devices”), as well as voice mail, electronic mail (e-mail), chat applications, Internet access, and various information and management systems (“Business Systems”) to certain employees for the purpose of achieving the Company's business objectives. These Business Systems are provided only for employees’ use in doing their job for Extreme Networks, and not for any other personal or business reason of the employee. Extreme Networks reserves the right to access and review electronic files, messages, mail, etc., including, but not limited to, personal, password protected email, and to monitor the use of Business Systems as is necessary to ensure that there is no misuse or violation of Company policy or any law. For these reasons, employees should not use, send, receive or sync any personal communications through Company Devices or Business Systems, or place or retain anything on Company Devices or

Business Systems that the employee considers to be personal or private or otherwise would not want the Company to see. Therefore, to the extent permitted by law, employees should not have an expectation of privacy related to the information transmitted over, received by or stored in or on any Device or Business Systems owned, leased or operated in whole or in part by or on behalf of Extreme Networks.

The Company has the right to access, reprint, publish, or retain any information created, sent or contained in any of the Company's Devices or Business Systems, to the extent permitted by applicable laws. You may not use any Device or Business System for any offensive or illegal purpose or in any manner that is contrary to the Company's policies or the standards embodied in this Code. You must at all times use good judgment regarding electronic communications.

You should not make copies of, or resell or transfer (externally or internally), copyrighted publications, including software, manuals, articles, books, and databases being used in the Company, that were created by another entity and licensed to the Company, unless you are authorized to do so under the applicable license agreement. In no event should you load or use, on any Company Device, any content, software, or data without the proper license to do so. If you have any question as to what is permitted in this regard, please consult with your manager or the Company's Information Technology Department.

Failure to comply with the asset protection and use provisions of this Code or to use good judgment regarding use of Devices and Business Systems may result in disciplinary action, up to and including termination of employment, as permitted by local laws.

12. Government Contracts

The Company is fully committed to the establishment and maintenance of compliance and business ethics standards with respect to transactions with the U.S. government and with prime contractors and subcontractors on government programs. The Company will strictly observe laws, rules, and regulations fairly and ethically for all such business opportunities. The Company is committed to full and timely disclosure of any violation that governs the acquisition of goods and services by the U.S. government and will compete fairly and ethically for all such business opportunities. In furtherance of that objective, no employee shall, in connection with any transaction with the U.S. government, engage in any conduct in violation of such laws, rules, and regulations or act in a manner which is otherwise inconsistent with the Company's high standards of honesty and integrity. The company is committed to full and timely disclosure of any violation of federal criminal law involving the following topics:

- Procurement or Contract Fraud
- Personal and Organizational Conflicts of Interest
- Bribery/Kickbacks
- Gratuities
- False Statements or Claims to the Government
- Inaccurate Recordkeeping
- Human Trafficking
- Contract Overpayments by the Government

Any of the above matters should be immediately brought to the attention of the Chief Legal, Administrative & Sustainability Officer for assessment to determine if credible evidence exists necessitating disclosure to the Government. The Company is fully committed to support any inquiries from U.S. government authorities related to any and all disclosures of violations that may be made. Such support will entail full cooperation with Government authorities to provide timely and complete responses to auditors' and investigators' requests for documents and access to company employees with information.

In addition, we expect that all employees will comply fully with all applicable security procedures pertaining to any Government contracts. Company personnel are specifically expected to exercise the appropriate standard of care with respect to the handling of classified information. It is important, both from the standpoint of national security and that of assuring compliance with applicable laws, regulations and U.S. government contractual requirements, that all employees handle U.S. government classified material in the proper manner. Unauthorized access, dissemination, acceptance, or handling of that material is strictly prohibited. Company personnel with proper security clearances who may have access to classified information must be aware of and observe the specific requirements of the rules and regulations associated with the use, control, retention, and disposition of classified materials. The Company has agreed to adhere to these requirements as a condition to be eligible for the receipt of classified information. All of the Company's personnel with security clearances will receive regular training in the proper handling of classified information.

13. Employment Practices

Extreme Networks is fully committed to complying with all applicable labor laws and regulations. As an employer, the Company shall provide a fair, professional and mutually respectful work environment for all. As an equal opportunity employer, the Company will provide equal employment opportunity to qualified individuals regardless of race, color, religion, sex, sexual orientation, gender identity, national origin, age, ethnicity, or physical or mental handicap, and in compliance with all applicable employment laws and regulations. The Company will also provide employees a workplace free from any form of sexual or other types of harassment.

Extreme Networks is further committed to complying with all applicable immigration laws and regulations concerning verification of employment eligibility for all. The Company will not tolerate the employment of individuals who are not legally authorized to work in their work location.

The rules relating to recruiting and hiring current or former U.S. government employees are complex, and therefore you may not initiate negotiations with or extend any offers of employment to any current or former Government employee without first obtaining the review and written approval of the Company's Legal Department.

14. Reporting Violations of the Code

You should promptly report any violation or suspected violation of this Code to the appropriate Company personnel or via the Company's anonymous and confidential reporting procedures. However, nothing in this Code prevents you from communicating directly with relevant government authorities about potential violations of law.

The Company's efforts to ensure observance of, and adherence to, the goals and policies outlined in this Code mandate that you should promptly bring to the attention of the Company any material transaction, relationship, act, failure to act, occurrence or practice that you believe, in good faith, is inconsistent with, in violation of, or reasonably could be expected to give rise to a

violation of, this Code. You should report any suspected violations of the Company's financial reporting obligations or any complaints or concerns about questionable accounting or auditing practices.

Here are some approaches to handling your reporting obligations:

- In the event you believe a violation of the Code or a violation of applicable laws and/or governmental regulations has occurred, or you have observed or become aware of conduct which appears to be contrary to the Code, you should immediately report the situation to your supervisor, the Legal Department, or the Chair of the Audit Committee.

- If you have or receive notice of a complaint or concern regarding the Company's financial disclosure, accounting practices, internal accounting controls, auditing, or questionable accounting or auditing matters, you should immediately advise your supervisor, the CFO, the Chief Legal, Administrative & Sustainability Officer, or the Chair of the Audit Committee.

- If you wish to report any such matters anonymously or confidentially, then you may do so as follows:

    - Mail a description of the suspected violation or other complaint or concern to:

      Chief Legal, Administrative & Sustainability Officer, or Audit Committee Chair,
      6480 Via Del Oro, San Jose, CA 95119

      or

    - Submit the information online through the Company's third party administered help line

Raising a Concern or Asking a Question Related to Our Code

USA/Canada (English): **1-833-961-3663**
USA/Canada (Spanish): **1-800-216-1288**
Canada (French): **1-855-725-0002**
Mexico (Spanish): **01-800-681-5340**
All other countries: **800-603-2869** (must dial country access code first; click here for access codes and dialing instructions)

Online: report.syntrio.com/ExtremeNetworks

Global * Toll-Free * 24 Hours a Day * 7 Days A Week
Confidential * Choice to Remain Anonymous
Interpreter Available in many Languages

Confidentiality Obligations and Rights. Note that certain countries where the Company does business may not allow certain concerns to be reported at all or to be reported anonymously via the Company's provided hotline. Further, certain local regulations may require the Company to inform the person who is identified as a subject of a reported concern or violation that the report was submitted and that such person may exercise his or her right to access and respond to such

reported concern. As such, reports may be made anonymously and confidentiality will be maintained subject to applicable law, regulations and legal proceedings.

If you become aware of a suspected violation, don't try to investigate it or resolve it on your own. Prompt disclosure to the appropriate parties is vital to ensuring a thorough and timely investigation and resolution. The circumstances should be reviewed by appropriate personnel as promptly as possible, and delay may affect the results of any investigation.

Special Rules for U.S. Government Contracts. If you become aware of evidence of gross mismanagement of a U.S. government contract, a gross waste of Government funds, an abuse of authority relating to a Government contract, a substantial and specific danger to public health or safety, or a violation of law, rule, or regulation related to a Government contract (including the competition for or negotiation of a contract), you should report it to the Company via one of the above methods. If you wish to report such matters directly to one of the U.S. government entities designated in 48 C.F.R. § 3.908-3(b), you may do so instead of, or in addition to, reporting it to the Company. A violation of the Code, or of applicable laws and/or governmental regulations is a serious matter and could have legal implications. Allegations of such behavior are not taken lightly and should not be made to embarrass someone or put him or her in a false light. Reports of suspected violations should always be made in good faith.

If you have any questions regarding the Code, you should reach out to the Legal Department for guidance by sending an email to LegalCompliance@Extremeneworks.com.

The Company will not permit intentional retaliation against any person who, in good faith, provides truthful information to a Company or law enforcement official concerning a possible violation of any law, regulation or Company policy, including this Code. Persons who retaliate may be subject to civil, criminal and administrative penalties, as well as disciplinary action, up to and including termination of employment as permitted by applicable laws. If you report a suspected violation in good faith and you are not engaged in the questionable conduct, the Company will attempt to keep its discussions with you confidential to the extent reasonably possible. In the course of its investigation, the Company may find it necessary to share information with others on a "need to know" basis.

15. Internal Investigation

When an alleged violation of the Code is reported, prompt and appropriate action will be taken in accordance with the law and regulations and otherwise consistent with good business practice to investigate the matter either internally or with outside assistance.

At a point in the process consistent with the need not to compromise the investigation, a person who is suspected of a violation will be apprised of the alleged violation and will have an opportunity to provide a response to the investigator.

Based on the outcome of the investigation, the following actions may be taken, as appropriate:

- Implement Disciplinary Action. Disciplinary actions may be implemented in accordance with the Company's policies and procedures for any employee who is found to have violated the Code, as permitted by applicable laws. Any violation of applicable law or any deviation from the standards embodied in this Code may result in disciplinary action, up to and potentially including termination of employment, as permitted by applicable laws. Any employee engaged in the exercise of substantial discretionary authority who is found to have engaged in a violation of law in contravention of this Code or unethical conduct in

connection with the performance of his or her duties for the Company, may be removed from his or her position and not assigned to any other position involving the exercise of substantial discretionary authority, as permitted by applicable laws. In addition to imposing discipline upon employees involved in non-compliant conduct, the Company also may to the extent permitted by applicable laws, impose discipline, as appropriate, upon an employee's supervisor, if any, who directs or approves such employees' improper actions, or is aware of those actions but does not act appropriately to correct them, and upon other individuals who fail to report known non-compliant conduct.

- Implement Corrective Actions. The appropriate level of management will assess the situation to determine whether the violation demonstrates a problem that requires remedial action as to Company policies and procedures. If a violation has been reported to the Audit Committee or another committee of the Board of Directors, that committee will be responsible for determining appropriate remedial or corrective actions. Such corrective action may include providing revised public disclosure, retraining Company employees, modifying Company policies and procedures, improving monitoring of compliance under existing procedures and other action necessary to detect similar non-compliant conduct and prevent it from occurring in the future. Such corrective action will be documented, as appropriate.

16. Government Reporting

In addition to the reporting requirements in the section "Government Contracts" above, appropriate law enforcement personnel may be notified of potential violations of law in addition to any discipline imposed by the Company. Whenever conduct occurs that requires a report to the government, the Company will comply with such reporting requirements.

17. Waivers

Before a Director or officer (as defined under in Rule 16a-1(f) of the Securities Exchange Act of 1934), or an immediate family member of such person, engages in any activity that would be otherwise prohibited by the Code, he or she must obtain a written waiver from the disinterested directors of the Board. Such waiver must then be disclosed to the Company's shareholders, along with the reasons for granting the waiver.

18. No Rights Created

This Code is a statement of certain fundamental principles, policies and procedures that govern the Company's Covered Parties in the conduct of the Company's business. It is not intended to and does not create any rights in any employee, customer, client, visitor, supplier, competitor, shareholder or any other person or entity.