EXTREME NETWORKS, INC. CODE OF BUSINESS CONDUCT AND ETHICS

Policy Statement

At Extreme Networks, we are committed to conducting our business affairs honestly and in an ethical manner. That goal cannot be achieved unless each individual 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 or integrity should be avoided. The key to achieving our business goal and complying with this Code is exercising good judgment. This means following the law, doing the "right" thing, and acting ethically even when the law or internal policy is not specific.

This Code applies to all employees, officers and Directors of Extreme Networks, Inc. and its subsidiaries and branches in all locations (collectively the “Company” or “Extreme Networks”). It 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. Every 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. 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

Each employee, officer and Director is expected to become familiar with and understand the requirements of the Code. Most importantly, you must comply with it, and support others in their efforts to comply with it as well.

The Company's CEO will be responsible for ensuring that the Code is established and effectively communicated to all employees, officers and directors. 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 employees, officers and Directors have access to the Code on the Company's website and will provide periodic training on the Code to employees, officers, and Directors.

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 Extreme Networks, 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 Company employee, officer, Director and reseller is responsible for ensuring that Extreme complies with US export controls which are intended to control foreign distribution of US origin technology to prevent unauthorized access. Under no circumstance should a Company employee, officer, Director 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 various 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 around the globe. Directors, officers, and employees of the Company, as well as our agents, channel partners, and other third-party representatives, are prohibited from making, offering, authorizing or promising any payment of any money, or offer, gift, promise to give, or authorization of 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, etc.)
- 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.

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's 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, you must obtain advanced, written approval by Extreme's Legal Department and your manager if the value of such payment, gift, entertainment, or hospitality exceeds US $50. For more information and further details regarding permissible gifts, entertainment and hospitality, please see Extreme's 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. In the event that you receive any gift with a fair market value in excess of $75, you must report it to your Supervisor promptly. Executive Officers must report such gifts in writing, on a periodic basis, to the Audit Committee of the Board of Directors.

- 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 there is ever any doubt as to the acceptability of any entertainment activity, consult with the Legal Department or Extreme's Chief Compliance Officer by sending an email to Compliance@Extremeneworks.com.

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

All Company disclosures in reports and documents that the Company submits to the applicable 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 Chief Executive Officer ("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 WW Corporate Controller (and such other Company officers designated from time to time by the Audit Committee of the Board of Directors) will be deemed the Senior Officers of the Company. 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 (a) permit preparation of financial statements in conformity with GAAP or any other criteria applicable to such statements, and (b) 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; and

- 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; 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.

6. 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 stock, 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 a 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. Officers, directors and employees of the Company are subject to Extreme Network's Insider Trading Policy, a copy of which has been made available to each such officer, director and employee,

7. Conflicts of Interest and Corporate Opportunities

Employees, officers, and Directors 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 its employees, officers and Directors may not do indirectly through third parties what the Company employees, officers, and Directors 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 consult with your manager, the Company's Legal Department, or follow the procedures described in this Code. If you become involved in a situation that gives rise to an actual conflict, you should inform your manager or the Company's Legal Department of the conflict.

8. Confidentiality

All confidential information concerning the Company obtained by you is the property of the Company and must be protected. Confidential information includes all non-public information that might be of use to competitors, or harmful to the 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 and the third party.

Examples of confidential information not only include trade secrets, but also include without limitation non-public: 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.

9. Fair Dealing, Antitrust 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 government and non-government bribery sections 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.

10. 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 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, voice mail, and electronic mail (e-mail), and Internet access to certain employees for the purpose of achieving the Company's business objectives. These resources and assets are provided only for employees' use in doing their job for Extreme, and not for any other personal or business reason of the employee. Extreme Network 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 electronic communications 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 property or systems, or place or retain anything on Company computers 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 any electronic communications device owned, leased or operated in whole or in part by or on behalf of Extreme.

The Company has the right to access, reprint, publish, or retain any information created, sent or contained in any of the Company's computers or e-mail systems of any Company machine, to the extent permitted by applicable laws. You may not use e-mail, the Internet or voice mail 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 computer, any software, third party content or database without the proper license to do so.

You may use a handheld computing device or mobile phone in connection with your work for the Company, but must not use such device or phone to access, load or transfer content, software or data in violation of any applicable law or regulation or without the permission of the owner of such content, software or data. If you should 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 electronic communications, may result in disciplinary action, up to and including termination of employment as permitted by local laws.

11. Reporting Violations of the Code

You should report any violation or suspected violation of this Code to the appropriate Company personnel or via the Company's anonymous and confidential reporting procedures.

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, or the Legal Department, or the Chairman 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 EVP General Counsel, or the Chairman 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:

        EVP General Counsel, or Audit Committee Chairman,
        145 Rio Robles, San Jose, CA 95134 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

U.S./Canada: 1-855-227-0662
Online: www.ExtremeHelpline.EthicsPoint.com
International: Click here for the number

*** Global * Toll-Free**
*** 24 Hours a Day * 7 Days A Week**
*** Confidential * Choice to Remain Anonymous**
*** Interpreter Available in 175 Languages**

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.

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 Compliance@Extremeneworks.com.

No fear of Retaliation. It is Company policy that there be no 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. In cases in which 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.

12. 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 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, 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.

13. Government Reporting

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.