CODE OF CONDUCT FOR DIRECTORS

CyberGuard Corporation ("Company" or "CyberGuard") is committed to compliance with all laws and regulations that apply to it with the spirit and intent of high business ethics, honesty and integrity. As a result, the Company requires all directors ("Directors" or "you") to respect and embrace the principles set forth in this Code of Conduct ("Code").

While this Code imposes requirements that are often more exacting than those mandated by law, the Company believes that it must conduct itself with the highest level of integrity. Therefore, this Code covers many topics, including:

If you have any questions regarding this Code, please contact any member of the Compliance Panel or the Chairperson of the Board of Directors.

Compliance Panel Members in 2004:

Michael Matte, Chief Financial Officer
Adriana Kovalovska, VP, Legal Affairs
Julie Scheer, Manager Human Resources

A. GENERAL CORPORATE GOVERNANCE

I. Honesty & Fairness

The Company is engaged in worldwide business relationships with other organizations and individuals, and is the seller and buyer of goods and services. You may be called upon in the course of your duties to represent the Company in dealings with these individuals or outside organizations. Regardless of the identity of the individuals or the organizations you deal with, you should always adhere to the following standards.

1. Never make misrepresentations or dishonest statements, or statements intended to mislead or misinform. If it appears that anything you have said has been misunderstood, correct it promptly.
2. With the prior approval of the appropriate manager, respond accurately, completely and promptly to all requests for information from government regulatory agencies.
3. Never disparage a competitor, its products or its services. Rather, stress in a fair and accurate manner the advantages of the Company's products and services.

II. Compliance with Applicable Law

The Company is committed to strict compliance with all applicable governmental laws, rules and regulations, including but not limited to laws, rules and regulations related to securities, labor, employment and workplace safety matters. All Directors are expected at all times to comply with all such applicable laws, rules and regulations. Any violation of such laws, rules and regulations should be immediately reported to any member of the Compliance Committee or the Chairperson of the Board of Directors.

III. Confidentiality

While affiliated with the Company, you may obtain "Confidential Information" not known to the public. Some common examples of "Confidential Information" include, but are not limited to, weekly and monthly sales information; new product information, customer information; proposed acquisition plans; information pertaining to vendor products and performance, etc. While affiliated with the Company, or any time thereafter (except as may be expressly authorized by the Company in writing), you should not directly or indirectly, disclose to any person or use any Confidential Information for any purpose whatsoever, or permit any person to examine and/or make copies of any Company property or documents.

IV. Accurate & Complete Records

Accurate records play a vital role in assuring the maintenance of high ethical standards. Accordingly, all Company transactions must be recorded accurately, completely and in a timely manner. Directors must never make false or artificial entries in the Company's records. Directors may never understate or overstate reports of sales or expenses, or alter any documents used to support those reports.

V. Conflicts of Interest

Directors should avoid all Conflicts of Interest. The term "Conflict of Interest" is not easy to define, but it most frequently refers to situations in which decisions are or may be influenced by considerations of personal gain (directly or indirectly), or benefit to a Director's family, relatives or other third parties, which conflict with the Director's obligation to serve the best interest of the Company and its stockholders. Conflicts of Interest arise where a Director's position or responsibilities with the Company present an opportunity for personal gain (directly or indirectly) apart from the normal rewards of employment. The conflicting loyalties that can be created by such opportunities can cause a Director to give preference to personal interest in situations where corporate responsibilities should come first. Any and all possible Conflicts of Interest must be raised with the Chairperson of the Board of Directors.

VI. Improper Payments

No Director is authorized to make contributions of money, property, or services to any political candidate or Political Action Committee, at the expense or on behalf of the Company without prior written permission by the Board of Directors. Directors may, of course, personally participate and contribute to political organizations or campaigns with their own funds and in their own name.

Government Officials:

Directors may not offer gifts or gratuities to any government official, unless the gift is given entirely in the context of a personal friendship, cannot possibly be considered as part of an attempt to influence official behavior, and does not otherwise create an appearance of impropriety.

B. FEDERAL LAWS GOVERNING THE COMPANY

I. Compliance with Antitrust Laws

The U.S. federal government and most state governments, as well as the European Union and many foreign governments, have enacted antitrust or similar laws designed to ensure that the market for goods and services operates competitively and efficiently and to protect trade and commerce from unlawful restraints, price discriminations, price fixing and monopolies.

Violations of the antitrust laws can lead not only to substantial civil liability, but are often deemed to be criminal acts that can result in felony convictions.

The following are examples of activities that are prohibited under the U.S. antitrust laws:

(1) Agreements with competitors:
   - (i) to control or to fix prices or conditions of sale;
   - (ii) to allocate products, markets or territories or not to solicit business from each other's customers;
   - (iii) to boycott certain customers or suppliers; or
   - (iv) to refrain from the sale or marketing of, or limit the supply of, particular products;

(2) Reciprocal purchase agreements between buyer and seller, where the purchase of a product is conditioned on the seller's agreement to buy products from the other party; or tie-ins, whereby the seller requires a buyer to purchase one product to obtain the product it wants; and

(3) Discriminating among purchasers of products without any valid business justification.

Participation in trade associations and professional organizations, as well as informal contacts with competitors may serve useful and have legitimate purpose. To the extent that you have occasion to speak with competitors in any area of the Company's business, you must be certain never to discuss confidential matters as previously described in this Code. If a competitor begins to talk about these matters, you should respectfully remove yourself from the conversation.

II. Compliance with Export Laws – Export Licensing

(a) Export Policy. It is the policy of this Company that each and every export shipment or transmission of CyberGuard products (and third party products exported by the Company) must comply with all applicable U.S. export regulations.

(b) Export Regulations. The Bureau of Industry and Security ("BIS") of the U.S. Department of Commerce has recently amended the law governing export of

encryption software. The new law allows the export of software products with any encryption strength to (1) all end users in "EU+9 countries": European Union, Australia, Canada, Czech Republic, Hungary, Japan, New Zealand, Norway, Poland and Switzerland, and (2) all non-government end-users in all other countries (except T-7); provided that the BIS has reviewed and classified the software product for export. Any export or re-export to a government end-user in any non-EU+9 country requires an export license.

(c) CyberGuard's Products. CyberGuard products have been reviewed and classified by BIS which allows the Company to export these products to all non-governmental end users and to governmental end users in EU+9 countries. In the event that the Company plans to export its products to a government end user in a non-EU+9 country, the Company must obtain an export license to ship to that specific government end user, irrespective of the level of encryption. Therefore, each order must identify the intended end-user.

(d) Prohibited Exports: CyberGuard products can be exported and re-exported world-wide, EXCEPT to the 7 terrorist countries (currently: Cuba, Libya, Sudan, Syria, Iran, Iraq, North Korea) and EXCEPT to government end-users in non-EU+9 countries. Any planned export or re-export to any of these T-7 countries or to a government end-user in non-EU+9 country requires a prior export license from the BIS.

(e) Violation Consequences. In the event of a violation of the export regulations, the BIS can impose several sanctions on the Company, its officers and directors, and/or the individual person violating the export regulations:

(1) Administrative

- Denial of export privileges
- Revocation or suspension of export license
- Exclusion from practice in front of BIS (attorneys, accountants, freight forwarder, etc.)
- Civil penalty not to exceed $10,000 for each violation, except that any violation involving national security controls (includes CyberGuard products) shall not to exceed a fine of $100,000 for each violation

(2) Criminal

- Fine: not more than 5 times the value of the exports or re-exports, or $50,000, whichever is greater; and/or
- Imprisonment: not more than 5 years

or

- For willful violation:
    - ***Company:*** fine of not more than 5 times the value of exports or re-exports or $1 million, whichever is greater
    - ***Individual:*** not more than $250,000, or imprisonment for not more than 10 years, or both.

and/or

- Prosecution under provisions of law other than export regulations, for example: conspiracy, mail and wire fraud, false statements and money laundering.

(3) Other Sanctions by BIS

- Seizure and forfeiture of the exported items
- Suspension of the right of any person (including the Company) to contract with the U.S. government based on export violations.

III. The Foreign Corrupt Practices Act

The U. S. Foreign Corrupt Practices Act prohibits giving anything of value, directly or indirectly, to foreign government officials or foreign political candidates in order to obtain or retain business. It is strictly prohibited to make illegal payments to government officials of any country. It is in violation of federal law and Company policy to promise, offer or deliver to an official or employee of a foreign government a gift, favor or other gratuity. Violation of this law may lead to substantial fines, possible imprisonment, and disciplinary action by the Company.

C. CYBERGUARD - A PUBLIC COMPANY

I. Securities Law

As a public company, with the Company's shares being traded on the Nasdaq Stock Market, the Company is subject to regulation by the SEC and Nasdaq, and federal securities laws and regulations, as well as state and local laws. The Company requires strict compliance with these laws, rules and regulations.

In connection with its publicly traded shares, each public company has periodic reporting responsibilities to its shareholders and the Securities and Exchange Commission ("SEC") by filing annual reports (10-K), quarterly reports (10-Q), current reports on material events (8-K), proxy statements, and other reports. It is the policy of the Company to ensure full, fair, accurate, timely, and understandable disclosure in reports and documents that it files with, or submits to, the SEC and in other public communications made by the Company. In order to ensure adherence to this policy, all Directors are expected to keep accurate and complete business records as described above in this Code. These reports are prepared primarily by the Company's management and approved by the Board of Directors, to which the management reports. All financial reports prepared by the management are also independently reviewed by the Company's outside auditors and the Audit Committee of the Board of Directors.

II. Insider Trading

Federal securities laws and regulations govern transactions in the public companies' securities, such as the Company's common stock. Violations of federal securities laws can lead to civil and criminal actions against both the individual and the Company.

The securities laws and regulations prohibit, among other things, "insider trading," which means the use of confidential inside information which is material to the price of a publicly traded security in connection with the purchase or sale of the security.

During the course of your affiliation with the Company, you may come into possession of material non-public information either with respect to the Company's activities or business, or with respect to another company, such as the Company's customers or suppliers. It is the Company's policy that Directors who have such material non-public information may not engage in any transaction in the Company's securities or such other company's securities, and may not pass on to others that information, until such information has been disclosed to the public by the respective company.

Material Information: **"**Material Information" is any information that a reasonable investor would consider important in a decision to buy, hold or sell stock. In short, any information that could reasonably affect the price of the stock.

Common examples of information that will frequently be regarded as material are projections of future earnings or losses, news of a pending or proposed merger, acquisitions or tender offer; news of a significant sale of assets or the disposition of a subsidiary, changes in dividend policies or the declaration of a stock split or the offering of additional securities, changes in management, significant new product or discoveries; impending bankruptcy or financial liquidity problems; and the gain or loss of a substantial customer or supplier. Either positive or negative information may be material.

When information is "Public": The Company's shareholders and the investing public should be afforded enough time to receive publicly-released information and act upon it. As a general rule you should not engage in any transactions until the third business day after the information has been publicly released.

Transactions By Family Members: The very same restrictions that apply to you also apply to your family members and others living in your household. Directors are expected to be responsible for the compliance of their immediate family and personal household.

Tipping Information To Others: Whether the information is proprietary information about the Company or information that could have an impact on the Company's stock price, Directors must not pass the information on to others. The below-mentioned penalties apply, whether or not you derive any benefit from another's actions.

(a) **The Company's Insider Trading Policy:** Below is a summary of the Company's Insider Trading Policy.

- All Directors (and all family members living in their respective households), without exception, are prohibited from trading in the Company's securities while in possession of material non-public information.

- All Directors, officers, certain key employees with access to proprietary business and financial information, as identified by the Company, may trade in the Company's securities only:

  (1) during the "Trading Window Period" as indicated on the Company's Securities Trading Restriction Calendar; and
  (2) if not in possession of any material non-public information; and

(3) after obtaining clearance from the Company's CFO prior to making any trade, on the "Form for Securities Transactions" (which is attached to the Insider Trading Policy).

All other employees can trade at any time provided they do not possess any material non-public information, provided they obtain prior clearance from the Company's CFO prior to making any trade.

- Stock option sales (not exercises) are governed by the Company's Insider Trading Policy.

See attached CyberGuard's Insider Trading Policy and the Securities Trading Restriction Calendar for additional information.

(b) **Violation Consequences:** The consequences of insider trading violations can be staggering:

(1) For the **individuals** who trade on inside information or tip information to others:

- Disgorge all profits
- Civil penalty of up to three times the profit gained or loss avoided
- Criminal fine (no matter how small the profit) of up to $5 million
- Prison term of up to twenty years.

(2) For the **Company** and any **person in supervisory position** that fails to take appropriate steps to prevent illegal trading:

- Civil penalty of the greater of: $1 million or three times the profit gained or loss avoided as a result of the Director's violation; and
- Criminal penalty of up to $25 million.

(3) Moreover, if a Director violates the Company's Insider Trading Policy, the Company will impose sanctions, including dismissal for cause.

(c) **Company Assistance:** Any concerns or questions regarding this policy should be cleared with the Chief Financial Officer. Remember, however, the ultimate responsibility for adhering to the Insider Trading Policy and avoiding improper transactions rests with you. In this regard, it is imperative that you use your best judgment. If your securities transactions become the subject of scrutiny, they will be viewed after the fact with the benefit of hindsight. As a result, before engaging in any transaction you should carefully consider how regulators and others might view your transaction then.

III. No Personal Loans

Federal securities laws prohibit public companies from directly or indirectly extending or maintaining credit, from arranging from the extension of credit, or to renew an extension of credit, in the form of a personal loan to or for any Director or Executive Officer of the public company. Therefore, it is the policy of the Company to prohibit any personal loans directly or indirectly to any Director or Executive Officer.

D. ADHERENCE TO THIS POLICY

I. Reporting Violations of this Code

All Directors are expected to adhere, embrace, and promote this Code. If a Director becomes aware of any violation, or possible violation of this Code, the Director is required to report it to the Compliance Panel. A Director who reports a violation or possible violation of this Code should do so without fear of reprisal or retaliation, unless the Director knowingly makes a false report. All reports will be kept confidential.

II. Investigation of Violations

The Compliance Panel shall investigate any report it receives of a violation or possible violation of this Code.

III. Discipline for Violations

If the Compliance Panel concludes, after appropriate investigation, that this Code has been violated - whether by unlawful actions, condoning or failing to report information as to wrongdoing by others, retaliation against those who report suspected wrongdoing, or otherwise - the Compliance Panel is authorized to recommend disciplinary action up to and including termination as a Director's responsibilities to the Board of Directors.

IV. Waiver of the Code

The Board of Directors may waive the application of this Code to Directors under exceptional circumstances, provided that a request by a Director is made in writing to the Board of Directors in advance of any activities requiring waiver. Every waiver along with the reasons for the waiver will promptly be disclosed to shareholders in accordance with applicable law, SEC requirements and Nasdaq requirements.

Corporate Governance

ACKNOWLEDGEMENT

By signing below I hereby represent that:

1. I received a copy of the Code; and
2. I had ample time and opportunity to ask the Company's management and counsel to clarify anything that I did not understand; and
3. I read and understand the Code; and
4. I agree to comply with the Code at all times.

Signature: _____

Print Name: _____

Date: _____