

DATASCOPE CORP. - CORPORATE POLICIES AND PROCEDURES

SUBJECT: CORPORATE BUSINESS CONDUCT POLICY GUIDE

1. Code of Ethics

Datascope will manufacture and sell only products that are safe, effective, and of high quality. Datascope will comply fully, in every locale in which it does business, with all laws, regulations, and standards of conduct that apply to it or its products. Datascope employees will conduct themselves with the highest standards of honesty and integrity. Datascope employees will not have any business or other affiliations that create a real or apparent conflict with their loyalty to Datascope and their colleagues at Datascope.

2. Persons Covered

The Policy Guide covers all Datascope employees and those of all subsidiaries of Datascope, as well as all branches. Furthermore, a family member is not permitted to do indirectly what a Datascope employee cannot do directly. Therefore, with regard to securities trading and certain other matters, the Policy Guide also applies to spouses, family members and others who live in their households.

Because this important Policy Guide applies to all employees, each employee must read it carefully. Each Datascope employee will be asked to confirm in writing that the employee will comply with this Policy Guide. Attached to this Policy Guide is the form of acknowledgment each employee will be required to sign. Please also read it carefully. In addition, Datascope will periodically circulate notices reminding all employees of their obligations under the Policy Guide.

Employees should not hesitate to talk to their supervisor or a more senior manager if they have questions concerning this Policy Guide. The President or General Manager of any Datascope division or subsidiary or any corporate officer may be consulted regarding its interpretation.

3. Honesty and Record-Keeping

Datascope employees must conduct Datascope's business to the highest standards of honesty and integrity. Under no circumstances may a Datascope employee prepare a document that includes any untrue, misleading, or confusing statements or representations or make any statements or representations that are not complete, fair, and accurate. Similarly, Datascope employees may not make any untrue, misleading, or confusing statements to other employees, government agencies, customers, suppliers, physicians or the general public, and any statements made to such parties must be complete, fair, and accurate. No employee shall commit or contribute to acts of dishonesty such as fraud, theft, embezzlement or misappropriation of corporate assets.

4. Conflict of Interest

Gifts and Entertainment

No employee may accept a gift, favor or entertainment from a customer, vendor or other person or organization in connection with Datascope business unless all the following criteria are met:

- The item is consistent with the normal and accepted business ethics of the country in which it is provided;
- It does not violate the laws of the United States or the country in which it is provided;
- If a gift, it has only a nominal value (up to about \$100), and if a favor or entertainment, it is reasonable and not excessive;
- It cannot, in the surrounding circumstances, be reasonably construed as a bribe, payoff or kickback; and
- Public disclosure of it would not embarrass Datascope.

In no circumstances may gifts of cash or cash equivalents be accepted.

Acting Against Datascope Interests

No employee may take personal advantage of, or make available to others, any business opportunity in which Datascope is or might be interested, such as a purchase of real estate, a company, a product, a license or other property. In no event may an employee deal for his or her own account in products sold or services performed by Datascope.

Outside Employment

An employee may not also be employed outside Datascope if such employment (1) is with an employer that competes with Datascope or provides services or assistance to a competitor, or (2) interferes with the employee's assigned duties with Datascope. Examples of such interference would be if the outside employment requires the use of Datascope time or facilities, or impairs the employee's ability to give full attention to his or her position with Datascope during normal working hours.

Outside Directorships and Investments

An employee serving as a director of, or having a business or financial interest in, a firm having current or prospective dealings with Datascope, such as a supplier, customer, landlord, tenant or merger/acquisition candidate, or which is a competitor of Datascope, must disclose that fact in writing to the Corporate Secretary so that it may be determined whether the situation

presents a conflict of interest. The business or financial interests of members of an employee's family living with the employee shall also be considered to be the financial interests of the employee. Any subsequent approval to continue or engage in such outside directorship or investment must be in writing. The ownership of not more than one percent of a publicly traded company's securities (other than Datascope) will be presumed not to be a conflict of interest and need not be disclosed.

Government Service

Service by employees in government positions is encouraged but in some cases may present a conflict of interest. If election or appointment to such a position is anticipated, the employee must request the written approval of his or her supervisor. An employee holding a government office should abstain from any vote or decision that involves the interests of Datascope.

5. Confidentiality of Inside Information

Datascope employees must maintain the confidentiality of information belonging to Datascope or belonging to others and obtained through a relationship with Datascope.

Section 6 of this Policy Guide contains a discussion of "material information" in the context of the "insider trading" and "tipping" provisions of the securities laws. However, the information that must be kept confidential by Datascope employees is much broader. Confidential information also includes any information not generally known about Datascope's business such as, but not limited to, unpublished financial data, marketing, financial or other plans, customer or vendor lists, sales reports, price lists, blueprints, formulas, manufacturing processes, inventions, product development information or other proprietary data. Misuse of such information is inappropriate as a business practice and could lead to civil and criminal prosecution. If you have any questions regarding this, you should contact Corporate Counsel.

In addition to using your own judgment, you should take the following actions to preserve the confidentiality of Datascope information:

- Do not discuss or disclose confidential information in public places where you can be overheard, such as elevators, hallways, restaurants, airplanes or taxicabs. Discussions of confidential information with persons entitled to that information should be confined to closed offices or other secure locations.
- Do not read confidential documents in public places or discard them where others can retrieve them. Do not leave confidential documents in unattended conference rooms or where visitors can see them. Confidential information sent to others within or outside Datascope should be placed in sealed envelopes.
- Be aware that voices carry and that conversations conducted on speaker telephones in offices and on car or airplane telephones may be overheard easily.
- Be aware that conversations about where Datascope personnel are traveling or the presence of certain visitors in the office may reveal confidential information.

- Whenever possible, avoid sending or receiving confidential information by fax machines located in hotels, airport lounges, or the offices of third persons.
- Under no circumstances are employees to provide confidential Datascope documents or information to third parties unless an executed confidentiality agreement is in place.

The above list gives examples of steps designed to insure confidentiality. In some situations, other steps may be necessary. Each employee is responsible for taking whatever practical steps are appropriate to preserve the confidentiality of information.

6. Improper Trading in Securities

The “insider trading” provisions of the securities laws prohibit the trading of securities (such as stocks and bonds) based upon “material” (that is, significant), non-public information. Because of the severity of the penalties provided by law and the potential for damage to the good name and reputation of Datascope as a result of such unlawful trading, these legal prohibitions are summarized below.

General prohibitions

U.S. and foreign securities laws, as well as Datascope policy, prohibit employees from trading securities -- whether Datascope’s or those of other companies (for example, a supplier, a customer, or the subject of a possible acquisition) -- on the basis of material, non-public information, or providing such information to others who trade.

The law prohibits an insider, who is anyone with a special relationship to a company, from trading in any securities of that company on the basis of material, non-public information or directly or indirectly disclosing such information to another person -- a “tippee” -- who uses it for trading purposes, regardless of whether the “tippee” is related to the insider, or is an entity (such as a trust) in which the insider has an interest, or is merely a friend or acquaintance, unless and until such information has been disclosed to and absorbed by the investing public.

For purposes of this Policy Guide, the term “material information” should be broadly interpreted to include any information -- whether positive or negative -- that, if publicly disclosed, might have an effect on the market for a company’s securities generally, or any information that an investor might consider important in deciding whether to buy, sell, or hold securities. Examples of such information about Datascope include: financial results, especially earnings estimates, or operating results; internal financial projections, especially those that vary from previously issued, publicly stated financial projections; important new contracts or changes in contractual relationships or loss of business; an important new product or service or disappointing results concerning a new product or service; an important development related to a pending application for regulatory approval to market a new product; significant shifts in operating or financial circumstances; significant changes in the business prospects of counterparts, customers or suppliers; actual or proposed capital expenditures that vary substantially from those included in public projections for the relevant period; a proposal, negotiation or agreement for a joint venture or the termination thereof; proposals, negotiations or

agreements for corporate acquisitions or the sale of existing operations; the initiation or resolution of significant litigation or a significant litigation development; a change or important development in company management; a government investigation; a significant contingent liability; or any other event that would be expected to affect the market value of Datascope's stock.

A person with material, non-public information may trade only when he or she is certain that official announcements of the material information have been sufficiently publicized (for example, through issuance of company press releases or through public filings) so that the public has had the opportunity to evaluate the information.

The most dangerous time to engage in a purchase or sale of a company's securities would be shortly in advance of the public release by it of important information, such as quarterly or year-end results or other important news, while the safest time would be the period shortly following the release and publication of such information (always assuming that the employee is not aware of other undisclosed material information). However, even after a company has released such information, it is important to be sure that sufficient time has elapsed to enable the information to be disseminated to and considered by investors. If there is any question about the propriety of an employee's proposed trading, that employee must consult Datascope's Corporate Secretary before trading.

Penalties for Insider Trading

The seriousness of insider trading is reflected in the penalties it carries. Both a company itself and individual directors, officers or employees may be held liable. Insider trading may result in serious criminal penalties of up to \$1,000,000 or more in fines and imprisonment, or both, if the trading is found to be a willful violation of the law.

The Securities and Exchange Commission ("SEC") also has the authority to seek from the violator forfeiture of profits, a civil money penalty of up to three times the amount of profit gained or loss avoided by insider trading, and an injunction against future violations. The SEC also may impose liability on a company and any "controlling person" of an insider trading violator for up to the greater of \$1,000,000 or three times the amount of profit gained or loss avoided by insider trading if the company or a "controlling person" is found to have recklessly disregarded the likelihood that a controlled person would engage in a violation and failed to take steps to prevent the action before it occurred. The SEC is authorized to pay rewards of up to ten percent of a penalty recovered to persons providing information leading to the imposition of a penalty. Finally, private parties also may bring actions against any person purchasing or selling a security while in the possession of material, non-public information.

7. Responding to Inquiries From the Press, Regulatory Bodies and Others

If someone outside Datascope, such as a member of the news media or a securities analyst or investor, asks you questions about the business of the Company, do not answer them. You should obtain the name of the person making the inquiry and immediately notify the Corporate Secretary. Questions pertaining to products and services being sold by the Company

may be answered as you would answer a customer. If you have any questions regarding this policy, you should contact the Corporate Secretary for clarification.

Do not discuss confidential information even with persons from governmental bodies unless there is a legal obligation to do so. Simply and politely inform the inquirer that Datascope policy requires that he or she be referred to the Corporate Secretary.

8. Payment of Corporate Funds

Payments to Customers, Suppliers or Others

No effort may be made, directly or indirectly, to influence improperly a Datascope customer, supplier, or anyone doing business with or associated with Datascope. The payment of bribes, payoffs, kickbacks or other benefits that may improperly influence business relationships between Datascope and its customers or suppliers is prohibited. Such conduct is illegal and may violate state and federal criminal laws, including the Medicare/Medicaid anti-kickback statute discussed in Section 9.

Payments to Government Officials or Employees

Company funds or other assets may not be paid, directly or indirectly, to a government official, employee or politician for the purpose of obtaining or maintaining business. Such conduct is illegal and may violate state and federal criminal laws, including the Foreign Corrupt Practices Act discussed in Section 10.

Political Contributions

No Company funds or other assets may be paid, directly or indirectly, to a political party or political candidate or incumbent, except if legally permissible and if approved in advance by the Corporate Secretary. All requests must be presented in writing to the Corporate Secretary. No political contributions by individual employees may be made in the name of Datascope or be reimbursed by Datascope, directly or indirectly.

Gifts and Entertainment

Gifts, favors or entertainment may not be provided to a customer, supplier, government employee or other person or organization, unless all the following criteria are met:

- The item is consistent with the normal and accepted business ethics of the country in which it is provided and with the applicable industry association (e.g., Advamed or Eucomed) guidelines;
- It does not violate the laws of the United States or the country in which it is provided (see discussions of Medicare/Medicaid anti-kickback statute and Foreign Corrupt Practices Act below);

- It cannot, considering all circumstances, be reasonably construed as a bribe, payoff or kickback;
- Public disclosure of it would not embarrass Datascope;
- Modest gifts may be occasionally provided to health care professionals, but only if the gifts benefit patients or serve a genuine educational function. Other than the gift of medical textbooks, or anatomical models used for educational purposes, any gift should have a fair market value of less than \$100. Branded promotional items (e.g., pens, pencils, or post-it notes with the Company logo) of minimal value are acceptable.
- **Gifts may NOT be given in the form of cash or cash equivalents, such as gift certificates, under any circumstances.**

Entertainment: It is appropriate for employees to provide *occasional* hospitality for health care professional attendees *only* in the form of *modest* meals or receptions that are conducive to the exchange of information. Such hospitality events must be attended by at least one Datascope employee. Modest is defined as moderate or low value and in no event is to exceed \$100 per person including tax and tip. It is *not* appropriate to pay for meals, hospitality, travel, or lodging of guests of health care professionals or any other person who does *not* have a *bona fide* professional interest in the information being shared at the meeting (such as physician's spouse or companion who is not a health care professional).

Payments Outside Recipient's Domicile Or Resident Country

Datascope's Corporate Counsel must review and the Vice President of Finance must approve in advance any salary payment or any payment for goods or services that is to be made outside the domicile or resident country of the recipient.

Agents, Brokers and Consultants

Payments to agents, brokers, consultants, professionals or other parties representing Datascope must be limited to commercially reasonable compensation for services rendered plus reimbursement for reasonable expenses incurred. Contracts entered into with such parties must fully disclose the fees to be paid and the services to be rendered and must be reviewed and approved by Corporate Counsel. No such party may be engaged by Datascope to make payments or take action that would be in conflict with any provisions of this Code of Conduct.

Accounting Procedures

All transactions, Company funds, and assets must be properly and accurately recorded on Datascope's books and records in accordance with Datascope policies and procedures.

Documentation

Company funds may not be paid for a purpose other than that described by the documents supporting such payment. All Corporate payments must be made in accordance with established approval procedures.

9. Medicare/Medicaid Anti-Kickback Statute

According to federal law, anyone who knowingly and willfully offers or makes any payment, directly or indirectly, in cash or in kind, in order to induce a referral or purchase of an item or service for which payment may be made in whole or in part under Medicare or Medicaid, is guilty of a felony and, if convicted, may be fined up to \$25,000 or more, and imprisoned for up to five years, or both.

In order to avoid violating the provisions of the anti-kickback statute, employees should ensure that any questionable promotional or other offers made to prospective customers are reviewed by the Corporate Counsel.

10. International Business Conduct

International Boycotts

Several United States laws prohibit the observance or cooperation with boycotts of certain countries. Penalties apply even for failure to report promptly any requests for boycott-related information or action. The boycott laws are extremely complex, and any request received by Datascope that could possibly fall within the context of a boycott law should immediately be brought to the attention of the Corporate Counsel before any response is made to the request.

Foreign Corrupt Practices Act

The federal Foreign Corrupt Practices Act (“FCPA”) prohibits any employee of Datascope from, directly or indirectly, paying or giving, or offering or promising to pay or give, any funds or anything of value to any foreign official or other “Covered Person” (as defined below), for the purpose of (a) influencing any act or decision of the Covered Person in his or its official capacity, (b) inducing the Covered Person to do or omit to do any act in violation of his or its lawful duty, or (c) inducing the Covered Person to use his or its influence with a foreign government or instrumentality to affect or influence any act or decision of that government or instrumentality. The FCPA also prohibits paying or giving funds or anything of value to any person while knowing that all or a portion will be forwarded to a Covered Person for a purpose proscribed by the FCPA.

For purposes of the FCPA, “foreign” means outside of the United States. “Covered Person” includes any foreign official (which includes, without limitation, an officer or employee of any foreign government or any governmental department, agency or instrumentality or any government owned or controlled enterprise or any person acting in an official capacity for or on behalf of such government, department, agency, instrumentality or enterprise), foreign political party, foreign party official or candidate for foreign political office.

Government employees outside the United States have been known to request small payments in return for their performing routine services which are part of their jobs but which they may delay or refuse to perform unless compensated. Examples of such services would be the issuing of visas or customs documents. Such payments are discouraged but, if absolutely necessary, may be made only after consultation with the head of a division and Corporate Counsel. Any such payments must be accounted for properly in the corporate books and records.

11. Antitrust Laws

The discussion that follows is designed to familiarize you with the United States antitrust laws. You should be aware that many foreign countries (including the European Community and most of its member countries, Canada, Japan, and others) have their own antitrust laws which must be complied with when their markets would be affected. This presentation is, of necessity, only a general guide.

It is important to be sensitive to the type of issues that may be violations of the antitrust laws. Should you become aware of any situation that may raise questions under the antitrust laws, contact Datascope's Corporate Counsel immediately.

Overview

Among other things, the antitrust laws prohibit contracts or agreements that unreasonably restrain trade. Agreements among competitors with respect to prices and other terms and conditions of sale may be automatically considered to be illegal without regard to the business purpose for that agreement. To be unlawful, there does not necessarily have to be a formal agreement. Informal, oral agreements and understandings have been found to be agreements prohibited by the antitrust laws.

Specific Practices Prohibited by the Antitrust Laws

Price-fixing. Agreements between competitors to raise, lower or stabilize prices, or to set maximum or minimum prices, or agreements concerning terms and conditions of sale that affect price, may be automatically unlawful. Negotiations and agreements between buyer and seller or between supplier and customer that are part of a bona fide transaction do not violate the antitrust laws. Agreements setting or restricting the prices at which a purchaser may resell can be a violation of the prohibition against price fixing.

Market Allocations. Agreements among competitors to allocate markets, customers or business opportunities will likely violate the antitrust laws.

Group Boycotts/Concerted Refusals to Deal. The antitrust laws permit a company, acting alone, to select the persons with whom it will and will not do business. However, when two or more companies agree not to do business with another person, that agreement may often violate the antitrust laws.

Monopolization and Attempts and Conspiracies to Monopolize. The antitrust laws prohibit monopolizing, or attempting or conspiring to monopolize, the market for a particular product. Defining a product market (a market applicable to a particular product or group of

products) for purposes of the antitrust laws is a complex issue. Merely possessing significant market power or market share is not illegal. However, a violation may occur when a person with monopoly or near-monopoly power engages in unfair or predatory conduct with the purpose or effect of maintaining or increasing that market power.

Tying. A tying arrangement is an agreement by a party to sell one product or service but only on the condition that the buyer also purchases a different product or service. Such an arrangement may violate the antitrust laws, and may be automatically unlawful.

Reciprocity. It may also violate the antitrust laws for a buyer to condition his purchases from another person on that person making purchases from the buyer. It is not unlawful, however, for a person to transact business with a present or potential customer, even if done for the purpose of inducing that customer to transact other business. What can make the conduct unlawful is to attempt to coerce the customer to engage in reciprocal business.

Restrictions on resale. Restrictions on resale of Company products by our customers raise antitrust concerns. Restrictions, particularly those that relate to price terms, may be illegal.

Enforcement of the Antitrust Laws

In the United States, the antitrust laws are both civil and criminal laws. Their violation could expose you, and perhaps Datascope, to criminal penalties. Furthermore, any person or class of persons injured because of a violation of the antitrust laws may recover three times the amount of their actual damages, plus costs and attorneys' fees. Antitrust suits have often resulted in multimillion-dollar judgments or settlements.

Violations may also result in court orders that will restrict the way Datascope can do business. Violations may also cause agreements entered into unlawfully to be unenforceable.

12. Competition and Competitive Products

It is Datascope's policy to sell our products on their merits. Datascope employees, representatives and agents should not disparage or make unfair negative comments about our competitors or their products and services.

13. Compliance with Food and Drug Administration (FDA) Laws, Regulations and Requirements

As a company that pioneers medical and technological change, Datascope remains fully committed to fulfilling its duties under the food and drug laws. Accordingly, Datascope wishes to instill in every employee an understanding of the importance of dealing honestly with the FDA and other government agencies in the conduct of all Datascope business. Employees with Regulatory responsibility should refer to Datascope's Corporate Regulatory Policy Manual for a more detailed discussion of the duties and responsibilities imposed on medical device manufacturers by the FDA. What follows is an overview of relevant legal provisions and should be read in conjunction with the more detailed procedures set forth in the Corporate Regulatory Policy Manual and in each division's regulatory policies. If you have any questions, you should contact Corporate Counsel.

Federal Food, Drug, and Cosmetic Act -- General Overview

The primary enforcement mission of the Federal Food, Drug, and Cosmetic Act (“FDC Act”) is the prohibition against the introduction of “adulterated” or “misbranded” devices into interstate commerce. For purposes of the FDC Act, a device is “adulterated” if it does not have the product characteristics that it claims to possess, whereas it is “misbranded” if its labeling is false or misleading in any way. A device is also considered to be adulterated if it is not manufactured in compliance with the FDA’s Good Manufacturing Practices regulations, which describe the methods that must be used to manufacture medical devices and to document the manufacturing process. Anyone who violates this prohibition is guilty of a misdemeanor.

Submissions to FDA and Regulatory Agencies Worldwide

Datascope employees are expected to provide only truthful and accurate information in any correspondence or communication with the FDA or other government agency, and in any internal document that may be reviewed by any such agency. Section 1001 of the Federal Criminal Code provides that anyone who knowingly makes any false statements or representations to a federal agency with knowledge of their falsity, shall be fined up to \$10,000 (or more under legislation enacted subsequently) or imprisoned for up to five years, or both. An example of an offense punishable under this section would be the making of a false statement, either orally or in writing, in any document provided to the FDA.

Datascope emphasizes that any submission to the FDA or other regulatory agency must be produced in accordance with the policies articulated in Datascope’s Corporate Regulatory Policy Manual, Policies Numbers 1 and 6.

MDR Reporting Requirements

Datascope employees are expected to comply fully with the FDA’s Medical Device Reporting (MDR) rule. Under the regulation, each death or serious injury, and certain malfunctions, must be reported to the FDA within the time specified, regardless of the status of any investigation. Moreover, additional reporting requirements apply with respect to devices distributed under an Investigational Device Exemption (IDE). See Corporate Regulatory Policy Manual, Policy Number 2.

Government Inspections

Under the FDC Act, government inspectors are allowed to inspect device establishments and copy records. Records that are specifically required for devices under the Act may be copied by the inspector. Datascope employees are expected to cooperate fully with inspections conducted by the FDA and in a manner consistent with the guidelines articulated in Corporate Regulatory Policy Number 3.

Labeling and Advertising

All product labels, labeling and advertisements for any Datascope product must provide accurate and comprehensive information for the safe and effective use of the product and must comply with all relevant legal and regulatory requirements. Under the FDC Act, a product may be deemed misbranded or adulterated if, for example, it fails to provide information or provides incorrect, misleading, or only partially correct information to the user. Penalties for misbranding or adulteration are severe and may include recall, corrective advertising, product seizure, withdrawal of premarket approval, injunction, criminal indictment, significant product liability verdicts, and other such measures. Employees should refer to Corporate Regulatory Policy Manual, Policy Number 5, for Datascope's requirements for the labeling and promotion of medical devices and drugs subject to the FDC Act.

Distribution of Investigational Devices

Any and all shipments or deliveries of Datascope investigational products must be made in accordance with all applicable laws and regulations. Datascope's requirements for distribution of investigational devices are set forth in Corporate Regulatory Policy Number 7.

Remedial Actions on Distributed Products

Datascope's employees must take all appropriate steps to ensure that all products distributed by Datascope are safe, effective, and meet their specifications. However, in the event that, despite Datascope's best efforts, products not in compliance with these requirements are distributed, appropriate remedial action must be promptly taken. Appropriate actions include, but are not limited to, product recalls, safety alerts, inventory retrieval programs, and letters to doctors or customers conveying information about potential product and/or labeling problems. See Corporate Regulatory Policy Manual, Policy Number 8.

Criminal Prosecution for Regulatory Violations

Regulatory violations carry the risk of enormous harm to both the offending individual and to Datascope. A person who is convicted of violating the FDC Act for the first time is guilty of a misdemeanor and is subject to the penalties of imprisonment for up to one year or a fine of up to \$1,000 or both. Once a person has been convicted under the Act, any subsequent conviction may result in imprisonment for up to three years and/or a fine of up to \$10,000. If a first offense is committed with the intent to defraud or mislead, the stricter penalties apply. Under legislation enacted in 1986, an alternative schedule of far higher fines may be imposed for violations of the Act.

On the corporate level, violations can result in criminal fines of up to twice the company's "gross gain" (which may be equal to net sales, with no deduction for cost of goods sold or overhead); where a violation affects an entire product line (for example, due to a false statement in a PMA, PMA supplement, or a Section 510(k) filing), the fine can be many millions of dollars. Criminal charges can lead to suspension, and convictions can lead to debarment of companies and individuals from the federal procurement process. A debarred individual may find it hard to obtain or keep a job. In addition, regulatory violations, when disclosed, can lead

to severe drops in the prices of publicly traded shares, and to negative publicity, which can adversely affect relations with customers, suppliers, joint venture partners, investors, and others.

Civil Penalties for Regulatory Violations

Under the Safe Medical Devices Act of 1990, persons violating the medical device provisions of the FDC Act face civil penalties in addition to criminal penalties. Any person who violates a requirement that relates to devices shall be liable for a civil penalty of up to \$15,000 per violation.

14. Implementation

All U.S. and international managers shall, within their areas of responsibility, be responsible for explanation of this Policy Guide so as to assure employee understanding and compliance. Managers are also responsible for enforcement of this policy within their areas of responsibility.

Any actual or contemplated conduct that an employee discovers and which he or she reasonably believes may constitute a violation of this Policy Guide must be promptly reported to the company. Reports may be made:

- in person to a division head, a corporate officer or the Director of Internal Audit;
- by telephone using the dedicated Confidential Business Conduct Hot-lines
 - The U.S. telephone number is 800-500-0333 and the fax number is 800-500-0993
 - The Belgium telephone number is 0800-79906 and the fax number is 0800-79900
 - The France telephone number is 0800-910123 and the fax number is 0800-910241
 - The Germany telephone number is 0800-1326233 and the fax number is 0800-0326233
 - The Netherlands telephone number is 08000-232384 and the fax number is 08000-233841
 - The Hong Kong fax number is 800-968671;
 - The Italy telephone number is 800-786685 and the fax number is 800-786686
 - The United Kingdom number is 08-000324462 and the fax number is 08-000324461

- by mail to Datascope Corp., P.O. Box 61, Montvale, New Jersey 07645.

Employees reporting such violations will be protected against retaliation.

15. Enforcement

Violation of this Policy Guide may result in disciplinary action, including termination of employment. Legal proceedings may also be commenced, if necessary, to recover the amount of any improper expenditures, any profits realized by the offending employee, and any financial detriment sustained by Datascope Corp. In appropriate circumstances, violations of this Policy Guide will be reported to the applicable criminal authority.

16. Waivers and Amendments

Any request for a waiver of any provision of this Code shall be communicated immediately to the Chief Executive Officer, or in the case where the waiver relates to the Chief Executive Officer, the Chairman of the Audit Committee. Any waiver of this Code with respect to directors or officers may be made only by a majority of the Board of Directors and shall be promptly disclosed (along with the reason(s) for the waiver) as required by law and NASDAQ regulation.

This Code may be modified, amended or supplemented from time to time. Any amendment of this Code shall be approved by a majority of the Board of Directors and shall be promptly disclosed as required by law and NASDAQ regulation.

17. Conflicts of Laws

If any provision of this policy or its application to any employee or circumstance is held invalid, illegal, or unenforceable to any extent, the remainder of this policy and the application of that provision to the other employees or to other circumstances is not affected and is to be enforced to the fullest extent permitted by law. This policy represents the minimum standard for acceptable business conduct by Datascope employees, and any local law that is more restrictive or sets a higher standard shall be followed.

**ACKNOWLEDGMENT OF COMPLIANCE WITH
POLICY GUIDE**

I have read the Business Conduct Policy Guide of Datascope Corp. dated April 22, 2004, which, among other things, sets forth the obligations of Datascope personnel to (1) conduct the business of Datascope in accordance with the highest standards of honesty and integrity, (2) comply fully with the rules and regulations of the Food and Drug Administration and other government agencies, (3) maintain the confidentiality of information, (4) refrain from trading securities on the basis of material, non-public information or from “tipping” others concerning such information, and (5) comply with the Foreign Corrupt Practices Act, the antitrust laws and other state and federal laws.

I will adhere to the policies set forth in the Policy Guide for the duration of my employment with Datascope.

[Signature]

[Print Name]

[Date]