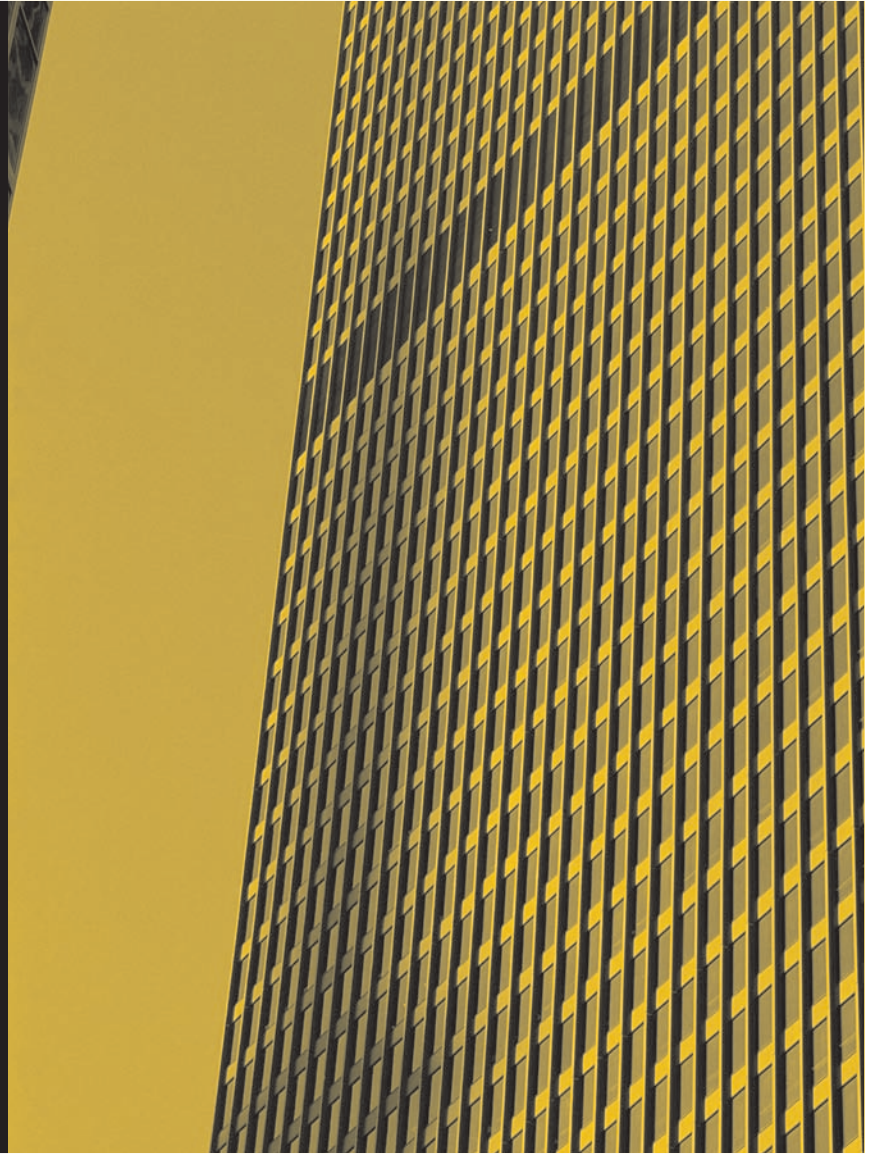


Our Code of Conduct

symantec™

Our Vision

People should be able to work and play freely in a connected world.

Our Mission

To deliver people, products, and processes that help ensure the integrity of information.

Our Promise

You can be confident Symantec will protect the integrity of your information,
helping ensure it is secure and available.

Our Values

Customer-driven, Trust, Innovation, Action.

Customer Experience

Peace of mind.

ABOUT SYMANTEC

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

A Message From the CEO & Chairman

Dear Colleagues,

At Symantec, we have four core values that are the foundation upon which we have built our company. These values are customer-driven, trust, innovation, and action. These values need to be expressed every day in our relationships with our customers and with each other.

To continue to meet this commitment to our customers, partners, and other stakeholders, we must ensure our actions always embody our core values, and that we maintain the highest levels of ethical behavior:

- **Customer-driven.** We make it easy for customers to do business with us. We build Symantec around our customers, not our products.
- **Trust.** We keep our commitments and are 100 percent accountable for delivering what we promise.
- **Innovation.** We anticipate customer needs and continuously develop new ways to add value to our customer relationships.
- **Action.** Our success as the industry leader flows from our ability to move with decisiveness. We respond quickly and continue to develop effective, proactive solutions.

Each of us, regardless of location or role, must build these values into every action we take. Given the unique role we play in our customers' lives, everyone must be committed to the highest degree of integrity and trustworthiness.

This code clarifies the standards of behavior that are expected of us globally, and gives guidance in making personal and ethical decisions. It aligns our values with our business practices and policies and provides a foundation for good governance—which is also a legal requirement. It expands our former Business Conduct Guidelines into the new “Symantec Code of Conduct.”

This Code of Conduct is the way we do business, and it is required reading for everyone at Symantec.

It provides all of us with a clear set of expectations and responsibilities, and highlights the need for each of us to act ethically, to build our company on mutual trust and openness with each other, and to be

forthright about our promises, business behavior, and actions taken in the name of Symantec.

I am asking everyone at Symantec, from the Board of Directors and the company officers, to the most recent new hire, to commit to these guidelines and demonstrate our trustworthy character. Defining the rules and expectations ensures that no matter how dynamic and challenging Symantec becomes, our actions and decisions will fit with our shared values.

Thanks for your commitment,

John W. Thompson

CEO & Chairman of the Board

Contents

Contents

Introduction

Symantec's reputation and credibility result in large part from our collective actions. This means that our work related activities must reflect standards of honesty, loyalty, concern for others, and accountability. We are expected to be sensitive to any situations that can adversely impact Symantec's reputation and are expected to use good judgment and common sense in the way we conduct business.

The Symantec Code of Conduct is designed to help you understand what we mean by good judgement and ethical behavior and outlines how you can align your actions with Symantec's values. It covers many different situations in which you might find yourself during the course of business and outlines principles that help you deal with those situations to avoid running into difficulties.

The policies summarized in this document are part of our corporate governance regulations. We must comply with these regulations and with the laws in every country in which we do business, and it is each employee's responsibility to do the same, and to act in a way that upholds Symantec's values at all times.

Worldwide Application

The Code of Conduct applies to all directors, officers and employees of Symantec and all its subsidiaries wherever located, collectively referred to herein as "employees." In addition, third parties representing Symantec—such as consultants, agents, distributors and independent contractors—will be provided the Code of Conduct and required to comply with applicable terms when performing work for Symantec.

Compliance with Law

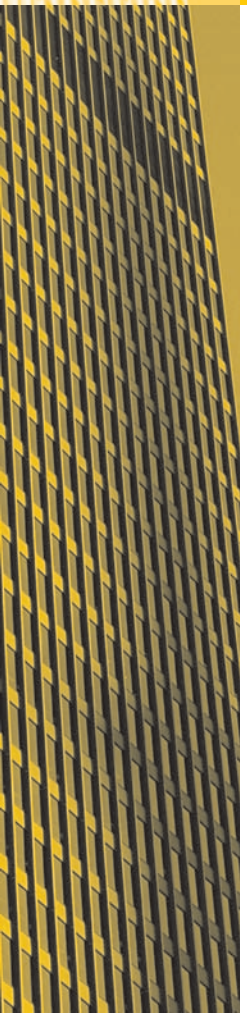
Symantec employees must comply with the laws, rules, and regulations in each country where we conduct business. As Symantec is a public company headquartered in the United States, the Code of Conduct is based primarily on U.S. laws. Local laws may in some cases be less restrictive than the principles discussed here. In those situations, you must comply with the Code of Conduct even if your conduct would otherwise be legal. On the other hand, if local laws are more restrictive than these standards, you must comply with the applicable local laws. Because of the complexity of the laws that apply to our business, the Code of Conduct provides only general guidance. Any questions or comments about the application of these laws should be directed to Symantec Legal.

Additional Information

The Code of Conduct contains policies governing the conduct of all Symantec employees in the course of our business. The Code of Conduct is intended to supplement, not replace, Symantec's employee handbook and other Symantec policies and procedures. This document and the policies described in it are not intended as an employment contract, however it does set forth expectations of behaviors in specific situations. Employees who violate the spirit or letter of the Code of Conduct are subject to disciplinary action up to and including termination of employment.

We may change, suspend or revoke the Code of Conduct at any time, subject to applicable law.

Our Personal Responsibility



Every Symantec employee has a personal responsibility to embody and model behavior that complies with these guidelines and to:

- Learn the details of all policies that affect your job. While no one expects you to know every policy verbatim, you should have a basic understanding of issues covered by each policy, and you should have a detailed understanding of policies that apply to your job.
- Seek assistance from your manager, the Office of Compliance, Legal, HR, or other Symantec resources when you have questions about the application of the policies.
- Know the escalation process and feel empowered to elevate concerns.
- Raise issues and concerns with your manager. If the issue is not resolved, raise it with another manager, the Office of Compliance, Legal, HR, or another Symantec resource.
- Understand the many options you have for raising concerns. Your communication may be written or oral, and it may be anonymous.
- Cooperate in investigations with concerns about a Symantec policy.

The obligations of leaders at Symantec go beyond those required of employees. Leaders at Symantec are expected to build and maintain a culture of compliance by:

- Leading by example, using their own behavior as a model for all employees.
- Personally leading compliance efforts through frequent meetings with direct reports and regular monitoring of compliance matters and programs.
- Making sure that employees understand that business results are never more important than compliance.
- Encouraging employees to raise ethical questions and concerns.
- Using employee actions and judgments in promoting and complying with Symantec policies as considerations when evaluating and rewarding employees.
- Ensuring that compliance risk areas associated with the business process under the leader's management are identified.
- Ensuring that policies and procedures, tailored to particular risk areas, are issued and communicated.
- Providing access to education, training, and legal counseling to ensure that employees, affiliates, and where appropriate, third parties understand the requirements of Symantec policies and applicable laws.
- Implementing appropriate control measures in business process, to detect heightened compliance risks and/or violations.
- Taking prompt corrective action to fix any identified weaknesses in compliance measures.

Everyone has a duty to be vigilant for circumstances that may indicate illegal or unethical behavior and to act appropriately in a timely manner to prevent improper conduct.

1.0 Respect in the Work Environment and in the Community

Symantec is committed to creating and maintaining a work environment based on respect for the individual, and to being a good corporate citizen in every country and community in which we do business. In our relationships with each other, we strive to be open, honest, and respectful in sharing our ideas and thoughts, and in receiving input. Symantec believes that diversity and inclusion are key drivers to creativity, innovation, and invention. We have a duty to embody and promote these values in our daily activities, and to comply with all laws and Symantec policies and guidelines relating to the treatment of all workers.

1.1 Fair Employment Practices

Symantec is an equal opportunity employer and bases employment decisions on merit, experience, and potential, without regard to race, color, gender, sexual orientation, national origin, ancestry, religion, physical or mental disability, age, veteran status, or other characteristics protected by applicable law. Symantec is committed to maintaining a work environment free from discrimination and harassment. Refer to Symantec's Personnel Policies and Guidelines, including the Policy Against Discrimination and Harassment, and the Equal Employment Policy.

1.2 Diversity and Inclusion

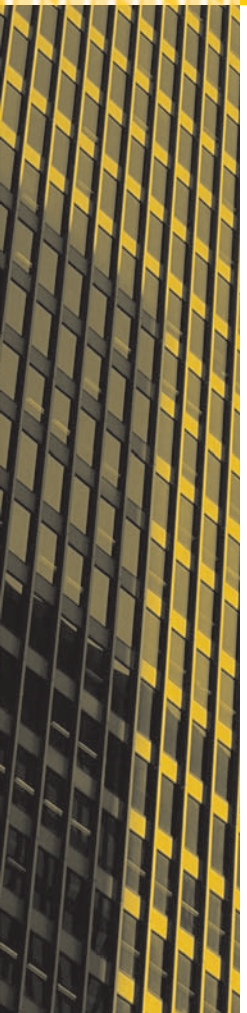
Symantec promotes and supports a diverse workforce at all levels of the Company. It is our belief that creating a work environment that enables us to attract, retain, and fully engage diverse talents leads to enhanced innovation and creativity in our products and services.

1.3 Conduct

Symantec expects every employee to maintain a professional demeanor at all times. This includes observing common courtesy in dealing with other employees, prospective candidates for employment, customers, vendors, or visitors to Symantec. Employees also must ensure that their conduct complies with all company policies and procedures, including this Code of Conduct and Symantec's Personnel Policies and Guidelines.

1.4 Health, Safety, and Security

Each employee is required to comply with all applicable laws and Symantec’s policies to promote an injury-free, safe, and secure workplace. Refer to the Symantec Corporate Security and Safety Policy.



1.5 Global Citizenship

Global citizenship is a commitment made by Symantec to strive to do business in a manner that upholds local and international standards and values everywhere it invests and operates. Global citizenship impacts every business group within Symantec.

Symantec has a responsibility to operate as a good corporate citizen and to make a positive contribution to the customers, communities, shareholders, and stakeholders that we serve.

1.6 Respect for the Environment

Symantec respects the environment and protects our natural resources. We strive to comply with applicable laws and regulations regarding the use and preservation of our land, air, and water.

What To Watch Out For:

- Allowing race, color, gender, sexual orientation, national origin, ancestry, religion, physical or mental disability, age, veteran status, or other characteristic protected by law, to be a factor in hiring, promotion, compensation, or other employment-related decision.
- Harassing others based on any of the above characteristics, for example, telling jokes or displaying materials that ridicule or offend a member of any race or ethnic group.
- Making or threatening retaliation against anyone who files a complaint of discrimination or harassment.
- Making unwelcome sexual advances to another employee or person with whom you work.
- Violating local labor laws (for example, hiring a child who is under the legal minimum working age).
- Refusing to work, or otherwise cooperate with certain individuals because of their race, religion, sex, etc.
- Failing to comply with health, safety, or environmental regulations.
- Failing to report environmental, health, safety hazards, or accidents.
- Failing to respond promptly to concerns about possible safety issues.

2.0 Conducting Business In Compliance With Applicable Laws And Regulatory Requirements

Symantec conducts its business fairly, legally, and with integrity. While working for the best interests of Symantec, we have a duty to be ethical and lawful in our dealings with customers, channel partners, suppliers, other business partners, and competitors, as well as our Symantec colleagues. Although laws and customs vary from country to country, Symantec expects that all employees comply with local laws, regulations, and standards of honesty and fairness in carrying out their duties on behalf of Symantec.

2.1 Contracting Practices

When Symantec is selling or buying products and services, or entering into other commitments, Symantec must embody the rights and obligations of each party in appropriate written contracts. Properly written contracts document the use of Symantec funds and assets, define the rights and obligations of Symantec and other parties, establish protections against liability, and provide tools for handling disputes. If you are involved in negotiating with Symantec customers, channel partners, suppliers, other business partners, or outside parties, you are required to understand basic principles of business transactions and to abide by Symantec contracting policies and guidelines.

You may not commit Symantec to undertake any performance, payment, or other obligation unless you are authorized under the appropriate Symantec delegation of authority policies.

You may not enter into any agreement or engage in any activity that may violate applicable law. You may not enter into any transaction that facilitates improper revenue recognition, expense treatment, or other accounting improprieties on the part of either Symantec or the business partner.

2.2 Antitrust and Competition

As a global business, we conduct our business in compliance with laws and regulations designed to promote fair competition and encourage ethical and legal behavior among competitors. Antitrust laws and fair competition laws generally prohibit any activity that restrains free trade and limits competition. (Refer to Section 6.0 Relating to Competitors.)

While basic antitrust and competition law principles apply worldwide, there are significant country and regional differences. If you are engaged in multinational business activities, you are required to be aware of, and abide by, all the laws that apply. Contact the Office of Compliance or Symantec Legal for further assistance.

2.3 Anti-Corruption

No one acting on Symantec's behalf may directly or indirectly use bribes or other corrupt practices in conducting Symantec business to influence any federal, state, or local government employee in any country. You are required to comply strictly with all ethical standards and applicable laws in every country in which Symantec does business. As a Symantec employee

wherever located in the world, you must comply with all elements of the U.S. Foreign Corrupt Practices Act (FCPA). The FCPA prohibits giving or offering to give anything of value, any payment, gift, entertainment, or service to foreign government officials, their employees, foreign political parties or public international organizations such as the UN, or the Red Cross, for the purpose of obtaining or retaining business.

2.4 International Trade

It is the policy of Symantec and its subsidiaries, including all employees and contractors, to comply with all applicable export control laws and regulations. Each Symantec business location is responsible for maintaining import, export, and customs records in accordance with the policies and guidelines provided by the Legal and Trade Compliance teams.

U.S. trade regulations apply to many activities involving non-U.S. citizens, including site visits, training, employment, and transmission of products, software, or technical data. U.S. law forbids doing business with certain countries and their nationals without obtaining prior U.S. government approval. U.S. law also prohibits accepting contract clauses that obligate a party to boycott any country. These U.S. controls apply to Symantec and its subsidiaries worldwide. You are responsible for consulting with the Symantec Legal and Trade Compliance departments to determine whether your activities are subject to special controls, and if so, to comply with them.

What To Watch Out For:

- Using side letters, “off-the-book” arrangements, letters of intent, memoranda of understanding, or other express or implied agreements without prior review and approval by Symantec Legal.
- Giving, offering, or authorizing to offer anything of value, such as money, goods, or services, to a customer or government official to obtain any improper advantage. A business courtesy, such as a gift, contribution or entertainment, should never be offered under circumstances that might create the appearance of impropriety.
- Discussing or agreeing with competitors on pricing, terms, conditions of sale, costs, profits or profit margins, product or service offerings, production or sales volume, market share, coordination of bidding activities, dividing sales territories, or allocation of customers or product lines.
- Making contact with competitors that could create the appearance of improper agreements or understandings, whether the contact is in person, in writing, by telephone, through email, or through other means of communication.
- Requesting that a commission or other payment be made in a third country or to another name.
- Receiving a commission that seems large in relation to the services provided.

3.0 Protecting and Safeguarding Symantec's Assets

Protecting and safeguarding Symantec's assets – including tangible and intangible property, business, and technical information – is critical to Symantec's business success. We have a duty to use those assets for legitimate business purposes only, to protect them from loss or unauthorized use, and to keep them confidential as appropriate. In no event may Symantec assets be used for unlawful or improper purposes.

3.1 Finance and Accounting Practices

It is a legal requirement that, as a public company, Symantec adheres to strict accounting principles and standards of reporting. Financial information must be accurate and complete, and there must be internal controls and processes to comply with these accounting and financial reporting laws.

These laws require the proper recording of, and accounting for, revenues and expenses. If an employee has responsibility for or any involvement in these areas, they must understand and adhere to these rules. Also, these rules prohibit anyone from assisting others to engage in improper accounting practices or make false or misleading financial reports. Employees must never provide advice to anyone outside of Symantec, including clients, suppliers, and business partners, about how they should be recording or reporting their own revenues and expenses.

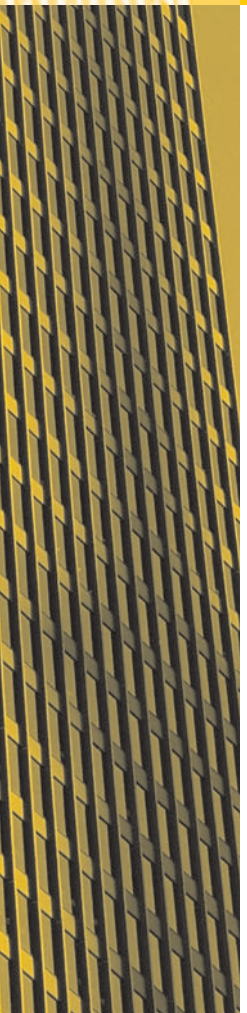
Violations of laws associated with accounting and financial reporting can result in fines, penalties, and even imprisonment, and can lead to loss of public faith in a company. If you become aware of any action related to accounting or financial reporting that you believe may be improper, you should immediately report it. This may be done through your management, the Office of Compliance, Symantec Legal, Symantec Internal Audit, or by informing Symantec management using any other communications channels, including anonymous email and/or contacting AlertLine.

3.2 Political Contributions and Activities

Symantec's public policy agenda includes the support of legislation that protects and promotes the business interests of the Company. However, Symantec's funds and other assets may be used as political contributions only as allowed by law and in accordance with Symantec policies set forth by Symantec Government Relations.

Federal Politics. Symantec may not use its corporate funds or assets for contributions to candidates for U.S. federal political office. An independent entity, the Symantec Political Action Committee, may solicit individual contributions from Symantec managers to support selected candidates in federal campaigns.

State and Local Politics. In the U.S., where legally permitted, Symantec may make contributions to state candidates, and to state and local ballot measures, provided such contributions have been authorized by the Director of Symantec Government



Relations as part of programs approved by the Senior Vice President, Communications and Brand Management.

Non-US Politics. Symantec funds or other assets may not be used for political contributions outside the U.S., even where permitted by local law, without written clearance from Symantec Legal, the Director of Government Relations, and the Senior Vice President, Communications and Brand Management.

Personal Activities. While you are encouraged to participate in your community and the political process, you may not create the impression that you are speaking or acting for or on behalf of Symantec. You may make personal contributions to political candidates of your choice, however, Symantec will not reimburse you for personal contributions.

Lobbying Activities. In the course of your employment, you may not engage in any activity on behalf of Symantec with the intention to influence legislation or rulemaking, or engage lobbyists or others to do so, without the express written authorization from the Director of Government Relations.

3.3 Intellectual Property

Symantec's intellectual property portfolio is vital to its business success. Intellectual property includes patents, trademarks, copyrights, trade secrets, source and object code, marketing plans, contact lists, employee phone lists, or other confidential or proprietary information. Symantec invests substantial amounts of money in you as an employee, in the development of products, services, and business processes, and in the protection of related intellectual property. The intellectual property that you generate while doing your job contributes to Symantec's strength and you have a duty to protect these valuable assets from misuse and unauthorized disclosure.

Just as we expect others to honor our intellectual property rights, we must honor the intellectual property rights of others. You have a duty to protect any confidential information you receive from others from misuse and unauthorized disclosure.

When you joined Symantec, you were required to sign an agreement under which you assumed specific obligations relating to intellectual property, as well as the treatment of confidential information. Any questions about this agreement should be directed to the Symantec Legal department.

3.4 Personal Use of Company Resources

Symantec provides a wide variety of assets for its employees in conducting company business, including computers, communications systems, and other equipment and materials. Although you may occasionally use some of these resources for incidental personal activities, it is your duty to keep this usage to a minimum and to comply with all Symantec policies and guidelines

3.0 Protecting and Safeguarding Symantec's Assets

on Internet usage. Excessive personal use of Symantec resources increases Symantec's costs and expenses, reduces availability of the resources for Symantec's business needs, and may adversely affect your job performance and the performance of Symantec.

You may not use any Symantec resource in violation of the law. You may not allow other people, including your friends and family, to use Symantec resources for any purpose. You may not use any Symantec resources to visit Internet sites that contain sexually explicit content, or visit sites for the purpose of gambling, or visit sites that advocate intolerance of others. Such misuse of Symantec assets is misconduct and may lead to immediate termination of employment. Refer to the Symantec Internet/ Intranet Usage Policy.

3.5 Protecting, Disclosing, and Receiving Confidential Information

You have a duty to protect Symantec information. Symantec confidential information includes a wide range of non-public information including but not limited to financial and cost data, business plans and strategies, operating reports, pricing information, marketing and sales data, business partner information, research and development (R&D), trade secrets, proprietary information, technical information and source code, personnel records, and organization charts. Appropriate security measures to protect Symantec information from improper disclosure should be taken in accordance with applicable Symantec IT, Security, Public Relations, Investor Relations, and Legal policies and guidelines.

Disclosure of Symantec information may be made only by those authorized to do so and in compliance with Symantec policies. Acceptance of confidential information from others must also be handled with care and in compliance with Symantec policies. Inappropriate disclosure of Symantec confidential information or receipt of non-public information from others can weaken our competitive position, jeopardize our R&D, and squander our investments in the processes and resources we have developed for conducting our business.

Before sharing any Symantec confidential information with an outside party, in writing or orally, an appropriate Symantec Non Disclosure Agreement (NDA), available from Symantec Legal, should be properly completed and executed.

Although Symantec sometimes has a business need to receive confidential information from a company or individual outside Symantec, you should be cautious when anyone wishes to share information based on an expectation that Symantec will hold it in confidence. Casual acceptance of confidential information creates a risk that Symantec will be accused of misusing it.

Symantec does not accept unsolicited suggestions that the submitter may consider confidential, such as unsolicited ideas for future products. This policy is intended to prevent Symantec's own R&D and other business activities from becoming encumbered by unintended obligations to outsiders. Any recipient of an unsolicited suggestion should promptly contact Symantec

Legal. Refer to the Symantec Legal Web site for policies related to intellectual property.

3.6 Communicating With The Public

Your duty is to maintain as confidential all non-public information of Symantec and to refer all requests by representatives from the media, financial analysts, investors, industry analysts, or legislative entities, to the appropriate communications department - Public Relations, Investor Relations, Analyst Relations, or Government Relations. Only designated Symantec representatives are authorized to make public any news and information about Symantec that may be significant to the financial markets. News that can be expected to influence investors or have an impact on the market for Symantec stock, including forward-looking information such as projections of orders, revenue, or earnings, may be released only through designated representatives in the Symantec Corporate Public Relations or Investor Relations department.

Press releases are to be made only through designated Public Relations representatives assigned to your business, operation, or function, in compliance with Symantec policies. All media contact is initiated and managed only by the Symantec Public Relations department. You may not grant interviews or provide comments to the press without prior approval from the Symantec Public Relations department. Unless you receive other guidance from Public Relations, you are expected to decline the opportunity to respond to any inquiries for news or information about Symantec and refer the request to the appropriate Symantec spokesperson. You may not create any impression that you are speaking on behalf of Symantec in any personal communications such as blogs, user forums, chat rooms, and bulletin boards.

3.7 Insider Trading

Insider trading, insider dealing, and stock tipping are criminal offenses in most countries where Symantec does business. Our policy requires that any employee or director who has material, non-public information about the Company may not buy or sell securities of the Company or engage in any other action to take advantage of or to pass on to others, that information. Symantec has also implemented a trading window whereby employees who are likely to have access to inside information may not engage in any transactions in the Company's securities until the third business day after the information has been released to the public and must get pre approval for all trades.

If you are considering a stock transaction, and you believe you may have inside information, consult with Symantec Legal. Refer to Symantec's Policy on Securities Trades by Company Personnel for details on what constitutes material non-public information.

3.0 Protecting and Safeguarding Symantec's Assets

3.8 Privacy and Personal Data Protection

Symantec is committed to protecting the personal information of its customers, channel partners, suppliers, and other business partners and employees. Personal information includes data related to a person who can be identified or located by that data. In order to create an environment of trust and to comply with applicable local laws, employees are required to follow Symantec privacy policies and data protection practices in using online and offline systems, processes, products, and services that involve the use, storage, or transmission of any personal information.

Symantec is also committed to protect the privacy interests of employees in their personal data. While seeking to maintain employee privacy, however, Symantec reserves the right to monitor use of company property (for example, computers, email, phones, proprietary information, etc.) in accordance with applicable laws.

3.9 Records Management

For business, accounting, and legal reasons, our company records must be properly managed. We create, retain, and dispose of our business records and information assets, both written and electronic, as part of our normal course of business in compliance with Symantec policies and applicable regulatory and legal requirements. Information defined as essential must be retained in a recoverable format for as long as it remains essential. Information that is no longer essential should be disposed of as soon as possible, unless it is subject to a hold order issued by Symantec Legal. For questions regarding what is essential information, contact Symantec Legal.

3.10 Lawsuits, Legal Proceedings, and Investigations

Lawsuits, legal proceedings, and investigations concerning Symantec must be handled promptly and properly in order to protect and defend Symantec. You are required to contact Symantec Legal immediately in the event you receive a court order or a court issued document, or learn of a threatened lawsuit, legal proceeding, or investigation brought by private parties or by any government agency. Records relevant to a lawsuit, legal proceeding, or investigation must not be altered or destroyed, and must be promptly produced and turned over to Symantec Legal upon request.

Under U.S. law, attorney-client privilege applies only to communication in confidence to Symantec attorneys to obtain legal advice, as well as communication from Symantec attorneys applying their advice to Symantec activities. These communications should not be copied or distributed except under the direction of a Symantec attorney, and should be given only to the narrowest possible set of Symantec people on a need-to-know basis. If you are involved on Symantec's behalf in a lawsuit or other legal dispute, you must avoid discussing it with anyone inside or outside of Symantec without prior approval of Symantec Legal. You are required to cooperate fully with Symantec Legal in the course of the lawsuit, legal proceeding, or investigation.

What To Watch Out For:

- Reporting financial results that seem inconsistent with underlying performance.
- Inaccurately stating financial records, such as overstating travel and entertainment expenses, or submitting erroneous time sheets or invoices.
- Releasing confidential information to unauthorized third parties.
- Having lack of controls in place to protect assets from risk or loss.
- Making personal contributions to candidates for office that are then expensed back to Symantec.
- Discussing Symantec proprietary or confidential information with customers or suppliers.
- Receiving, from an employee, proprietary or confidential information about his or her prior employer.
- Passing on or divulging proprietary or confidential information to outsiders, for example on Internet message boards.
- Speaking to a member of the press without prior approval.
- Using company computers to visit Web sites that contain inappropriate or unprofessional content.

4.0 Avoiding Conflicts of Interest

Symantec recognizes and respects that employees may take part in legitimate financial, business, and other activities outside of their jobs. However, we all have a duty of loyalty to Symantec. Symantec employees are expected to act in Symantec's best interests and to exercise sound judgment unclouded by personal interests or divided loyalties. We seek to avoid the appearance of, as well as an actual, conflict of interest both in the performance of our duties for Symantec and our outside activities.

4.1 Outside Employment and Other Volunteer or Charitable Activities

Symantec policy does not prohibit all outside employment, but your duty to Symantec is to ensure that outside employment and other activities do not negatively impact your work at Symantec, cause you to misuse Symantec information or assets, or result in consequences unfair to Symantec.

You may not engage in any outside employment or activities that may improperly influence, or appear to improperly influence, your judgment, decisions, or actions with respect to your role at Symantec. To assess whether a potential conflict of interest may exist, you need to consider the activities in which you may be engaging, regardless of whether you may be called an "employee," "consultant," "contractor," "owner," "investor," or "volunteer."

Symantec encourages your personal involvement in charitable, professional, and other community organizations. Except as part of a Symantec-sponsored event, your volunteer service must be performed on your own time, at your own risk, away from Symantec premises, and without the use of any Symantec resources.

You may not solicit donations from Symantec business partners where an appearance of conflict of interest may arise due to your status as a Symantec employee.

4.2 Personal Benefit or Gain from Business

Receiving personal benefits from others because of your status as a Symantec employee may lead to divided loyalties. You may not receive any personal profit or advantage other than your compensation from Symantec in connection with any transaction involving Symantec, or your status as a Symantec employee.

You must disclose to your manager, and your appropriate HR contact, all situations where you or your Symantec group may be conducting Symantec business with members of your family, your friends, or others with whom you have a close personal relationship. Upon disclosure, Symantec may under certain circumstances allow you or your Symantec group to do business with your family members or friends, or entities they own or control. However, you will be required to remove yourself from Symantec's decisions relating to such transactions. In no event are you permitted to provide your services to Symantec outside your role as a Symantec employee.

4.3 Outside Directorships

Participating on the board of directors of other companies or non-profit groups may enhance your business and leadership skills, but may also lead to conflicts of interest. Prior to service on an outside board, you must seek prior approval from Symantec Legal or the Senior Vice President of Human Resources. If you are serving as a director of a company or other organization, and you encounter any situation where your role as a director may be in conflict with Symantec's interests, you must either withdraw from that situation or resign as a director.

You may not be a director of a Symantec competitor, customer, channel partner, supplier, Symantec subsidiary, or joint venture without approval from the Symantec General Counsel and a member of the Symantec Executive Staff.

If you serve as a director of another company at the request of Symantec, or in connection with a Symantec equity investment in the Company, you may not receive compensation from that company, such as fees, stock options, or other perks for your service. You may not accept outside directorships if the resulting time demands interfere with your ability to perform your job at Symantec. You must remove yourself from any Symantec decision-making with respect to the company or organization on whose board you serve.

4.4 Financial Interests in Other Businesses

You may not have a personal or family financial interest in a Symantec customer, channel partner, supplier, other business partner, or competitor that could improperly influence your judgment, has the potential to cause the appearance of divided loyalty, or might result in personal benefit because of your role at Symantec. Financial interests include investment, ownership, or creditor interests.

You should not have financial interests in Symantec customers, channel partners, suppliers, other business partners, or competitors if (a) you are in a position to influence Symantec decisions relating to them and those decisions could affect your financial interests, and (b) your financial interests represent such a percentage of yours or your family's net worth that an actual or apparent conflict of interest exists.

4.0 Avoiding Conflicts of Interest

4.5 Business Gifts and Entertainment

Symantec policy and practice requires the use of good judgment, discretion, and moderation when giving or accepting gifts or entertainment in business settings. Any gifts and entertainment given or received must be in compliance with the law in that country and the U.S. Foreign Corrupt Practices Act, and must not violate the giver's and/or receiver's company policies on the matter. Extending or receiving common courtesies such as business meals, usually associated with accepted business practice, in dealings with a customer, supplier or other non-governmental person or entity is acceptable. However, in any such dealings, employees of Symantec should not request, accept, offer to give, or give anything of significant value that would give the appearance of impropriety, or that the gift or entertainment was intended in any way to influence a business relationship. Extending or receiving occasional gifts having a maximum retail value of $250 over the course of any one calendar year as a gesture of goodwill is acceptable. Gifts in the form of cash payments are not allowed, regardless of amount. Gifts in the form of tickets to sporting events and other forms of entertainment may not be subject to the $250 limit. However, all entertainment with a value in excess of $250 requires notification to and consent of the Executive Management member in charge of the relevant operating unit. See also the Symantec Global Expense Reimbursement Policy, and Customers from the Public Sector (Section 5.8).

4.6 Disclosing Conflicts

The effectiveness of this policy depends in large part on the cooperation of all employees in disclosing situations that may be contrary to the intent of the policy and the ethical standards that it expresses. Your responsibility is to use your best judgment to evaluate objectively whether your outside activity, financial interest, or receipt of business gifts and entertainment may lead to divided loyalties. You must promptly disclose in writing to your manager, and your appropriate HR contact, any situation that could present a conflict of interest with your role at Symantec. Your disclosure will then be submitted to the Office of Compliance for consideration. Copies of your disclosure and Symantec’s response will be kept in your personnel file. You will have a continuing obligation to disclose any change in circumstances that could affect Symantec’s interests.

What To Watch Out For:

- Holding a financial interest in a company where you could personally affect Symantec's business with that company.
- Taking a part-time job where you may be tempted to spend time on that job during your normal Symantec working hours or to use Symantec equipment or materials.
- Receiving gifts of greater than nominal value from suppliers, customers, or competitors while you are in a position to influence Symantec decisions that might affect or appear to affect the outside concern.
- Receiving personal discounts or other benefits from suppliers, service providers, or customers not available to the general public or similarly situated Symantec employees.
- Accepting an offer to purchase "friends and family stock" in a company issuing shares through an initial public offering (IPO) if you interface with that company in your Symantec business activities.
- Directing business to a supplier that is owned or managed by a relative or close friend.
- Misusing Symantec resources, or your position or influence, to promote or assist an outside business, or not-for-profit activity.
- Preferentially hiring, directly supervising, or making a promotional decision about a spouse, relative, or close personal friend.
- Participating in a romantic or other personal relationship that may create a conflict of interest with the employee's responsibilities or compromise company interests.
- Borrowing money, goods, or services from the Company or lending to employees, customers, or suppliers.

5.0 Working With Customers, Partners, Suppliers, and Government Business

We must maintain the confidence, respect, and trust of our customers, partners, suppliers, and government organizations by conducting business responsibly. We must be committed to acting ethically, lawfully, truthfully, and with integrity in all business dealings whether selling or buying, or representing Symantec in any other capacity.

5.1 Advertising, Marketing, and Sales Practices

Generally, statements in Symantec advertising, promotional materials, and product packaging must be fair, factual, complete, capable of being substantiated, and may not deceive or mislead current or potential customers. Symantec's marketing and sales practices reflect Symantec's commitment to honest and fair dealings with its current or potential customers. You may not make false or misleading statements about Symantec's products or services, or those of competitors, in marketing or sales activities.

5.2 Selecting and Managing Channel Partners

Symantec resellers, distributors, and other channel partners are important to Symantec's sales and marketing strategies. Channel partners, however, are independent businesses, and Symantec's relationships with them are subject to antitrust, competition, and other laws. If you work with Symantec channel partners, you have a duty to manage channel programs in compliance with local laws and Symantec channel policies of your respective region. You are required to document properly all channel partner relationships. If Symantec is also a competitor of a channel partner, some otherwise permitted activities may be restricted by law.

5.3 Channel Pricing and Programs

Symantec may establish channel pricing and programs to help channel partners in selling Symantec products and services. However, there are legal limitations on the influence that Symantec may exert over channel partners. You are required to comply with the law and Symantec policies when developing and implementing Symantec channel pricing and promotional programs.

5.4 Choosing Suppliers

Symantec suppliers are of great strategic importance. Suppliers include component and material vendors, indirect goods and service providers, consultants, contract manufacturers, and anyone else who provides a product or service to Symantec. Symantec selects suppliers based on the merits of their products, services, prices, and business practices. You are required to follow Symantec policies in choosing suppliers on a basis that serves Symantec's interests and protects Symantec's reputation.

You must engage the assistance of Symantec Procurement in dealing with suppliers throughout the purchasing lifecycle. Symantec purchasing decisions will be made jointly between Symantec Procurement and the Symantec business owner and will reflect our best judgment about a supplier's technology,

quality, responsiveness, delivery capabilities, cost, environmental performance, and financial stability. You may not establish a business relationship with a supplier if its business practices violate local laws or basic international principles relating to labor standards or environmental protection.

5.5 Managing Suppliers

Properly managing relationships with suppliers is vital to the success of Symantec's worldwide operations. We are required to deal with suppliers in a professional and fair manner, to document properly all transactions, and to manage supplier relationships in accordance with the best interests of Symantec and in accordance with applicable internal policies and procedures. Symantec is required to document all supplier relationships in appropriate written contracts where applicable.

You may not establish exclusive arrangements or reciprocal purchase obligations in any supplier relationship without prior approval from Symantec Legal and Procurement. You may not enter into or request Procurement to enter into any false transactions or arrangements that assist a supplier in manipulating revenue or expense recognition. The existence and the terms of contracts between Symantec and its suppliers are considered confidential and are not to be disclosed to any other party. If a dispute with a supplier may lead to its termination, you must consult with Symantec Procurement and Legal departments.

5.6 Supplier Pricing

You are responsible for working with Procurement, in the best interest of Symantec and in compliance with Symantec policies and applicable law, to negotiate and obtain the best possible pricing.

While Symantec may have no legal obligation to protect price information unless required by contractual terms, negotiated price information is usually competitively significant and must be handled as Symantec confidential information. In general, we will not disclose the non-public prices of one supplier to another, or to anyone else within or outside of Symantec who does not have a legitimate business reason to know. If disclosure of negotiated pricing information or other terms is required for Symantec contract manufacturers or service providers, you must abide by Symantec policies on handling Symantec confidential information.

5.0 Working With Customers, Partners, Suppliers, and Government Business

5.7 Symantec as a Company Reference

The Symantec brand is a valuable asset that other companies may want to exploit. We are responsible for protecting the Symantec brand from unauthorized and inappropriate use. You may not permit any supplier or other party to use the Symantec name, logo, or other branding in its advertising, promotional materials, customer references, or the like, without approval from Symantec Corporate Public Relations or Brand Management. You may not permit any supplier to mention Symantec as a customer or disclose the terms of any contract with Symantec in an offering document such as a prospectus or a securities registration statement without prior approval from Symantec Corporate Public Relations or Brand Management.

5.8 Customers from the Public Sector

When Symantec sells products or services to any government entity, state-owned enterprise or public international organization, on a country, state, or local level, Symantec must abide by all applicable laws and regulations. In dealing with public sector customers in the U.S. or other countries you are required to understand the special rules that may apply. These rules also may apply to companies that bid or work on government contracts.

You must not give a U.S. government employee anything of value, including gifts, meals, entertainment, awards, or travel, for any reason, unless you have consulted with Symantec Legal to determine if an exception applies. U.S. Government employees are not allowed to receive gifts or entertainment of more than $25 in value. You must receive prior approval, in writing, from the Symantec Chief Financial Officer before providing any gifts, meals, or entertainment to any foreign entity covered by the U.S. Foreign Corrupt Practices Act (FCPA).

You must always exercise greater restraint in dealing with a representative of a government or government-owned entity than with someone from a private enterprise. Gifts, meals, and entertainment provided by any Symantec employee located anywhere in the world to foreign government officials, their employees, foreign political parties, foreign state-owned enterprises, and public international organizations are governed by the FCPA. In all cases, you are required to comply with the U.S. Foreign Corrupt Practices Act, and to adhere to the entity's published Code of Conduct. You are also required to abide by policies prohibiting any use of Symantec assets that can be construed to be a bribe.

You may not seek or obtain “source-selection information” or “contractor bid and proposal information” from government employees or employees of prime contractors in the course of a U.S. federal procurement. Doing so is a violation of the U.S. Procurement Integrity Act. Similar restrictions may apply in procurements conducted by state and local governments, and governments outside the U.S.

What To Watch Out For:

- Making untrue, inaccurate, or misleading statements to current or potential customers regarding our products and services.
- Establishing supplier relationships without engaging the assistance of Procurement personnel.
- Choosing a supplier on any basis other than open and competitive bidding.
- Accepting gifts or other items of value which could lead to a potential conflict of interest when selecting a supplier.
- Directing business to a supplier owned or managed by a relative or close friend.
- Establishing “quid pro quo” relationships with customers or suppliers.
- Using the Symantec name and/or logo in any supplier advertising or promotional material.
- Giving, offering, or authorizing to give anything of value (money, goods, or services) to a customer or government official to obtain an improper advantage.
- Accepting business courtesies, such as a gifts, contributions, or entertainment, under circumstances that might create the appearance of an impropriety.
- Giving a gratuity or other payment to a government official or employee to expedite routine administrative actions without consulting the Symantec Chief Financial Officer.

6.0 Relating To Competitors

As a global business, Symantec succeeds by competing vigorously and fairly in the marketplace in full compliance with applicable antitrust, competition, and other laws. These laws and regulations were designed to promote fair competition, free trade, and encourage ethical and legal behavior among competitors. Each employee must conduct business in compliance with these laws.

6.1 Dealing With Competitors

You may not make agreements, expressly or implied, with any Symantec competitor to set pricing, limit output, divide territories, or allocate customers for competing products or services. You may not discuss with competitors any proprietary and/or confidential information such as non-public or future pricing information, terms of sale, costs, margins, inventories, marketing plans, or similar confidential information.

When representing Symantec in trade associations, standard setting bodies, consortia, and other industry organizations, you need to be aware of the risk that participating companies may be perceived as using the meetings to reach anti-competitive agreements. You may not participate in groups engaging in activities that violate antitrust and competition laws. If a competitor uses a legitimate forum to discuss subjects that are prohibited, you must refuse to participate.

6.2 Competitive Information

We must have timely and complete information about industry developments in order to stay competitive. We only obtain competitive information by fair and legal methods.

You may review any public information, such as published specifications, trade journal articles, and other materials that a competitor has released to other companies, without restrictions. You may not obtain non-public information by illegal activities involving industrial espionage, or by asking a competitor's employees or contractors, or former employees or contractors. You may not examine information about competitive proposals or products that are submitted to customers, channel partners, suppliers, other business partners, or anyone else with the understanding they would treat it as confidential.

You may not misrepresent who you are or for whom you work when you ask for competitive information. You may not use or engage consultants, agents, friends, or others to undertake activities to obtain competitive information that would be unacceptable if pursued by you.

6.3 Competitive Practices

Symantec competes based on the quality and value of its products and services, not by disparaging the competition. Your statements about competitors need to be fair, factual, complete, and capable of being substantiated. While forceful marketing messages may be appropriate, you may not make false, misleading, unfair, or unprofessional comments about competitors or others outside Symantec, or internally at Symantec in company messages, presentations, and other materials.

You need to be aware that, where Symantec may have significant market share, its business practices in maintaining that success will be closely scrutinized. Activities that in some circumstances may be considered misuse of market power include refusing to provide a product or service that is essential to a competitor, exclusive relationships with customers or suppliers, and pricing below cost with the intent to drive competitors from the market. Once a customer has placed a firm order with a competitor, you may not engage in activities to interfere with the performance of that contract.

What To Watch Out For:

- Discussing with competitors non-public information, such as pricing.
- Obtaining non-public information by illegal means.
- Requesting that a competitor's current or former employees provide confidential information.
- Misrepresenting yourself or who you work for when seeking competitive information.
- Engaging others to obtain non-public information through illegal means.
- Interfering in the fulfillment of an order to a competitor.

Administrative Matters

Office of Compliance

Symantec has instituted an Office of Compliance under the direction of Thomas G. Aurelio, Vice President, Global HR Operations. The Office of Compliance reports to Rebecca Ranninger, Senior Vice President, Human Resources. The Office of Compliance will have direct access to Symantec's Chief Executive Officer and Symantec's Audit Committee. The Office of Compliance has been assigned overall responsibility to oversee compliance with the Code of Conduct, and will be supported by Symantec's Finance, Human Resources, Internal Audit, Information Systems and Technology, Legal, and other functional departments as needed. Depending on the nature of the compliance issue, the Office of Compliance will delegate authority to other departments and/or persons when appropriate

Changes and Communication

The Code of Conduct may be changed from time to time in response to employee feedback, changes in industry practices, changes in applicable laws, or past violations of these standards.

While the Office of Compliance has the authority to interpret and make administrative changes to the Code of Conduct, only Symantec's Board of Directors can approve a substantive change.

The Code of Conduct has been posted to our external Web site at www.symantec.com and to our company intranet. Changes to the Code of Conduct will be made to these online versions, and you will be advised of important changes by email.

Acknowledgment

Symantec asks employees to annually acknowledge their commitment to the Code of Conduct. Your signature acknowledges that you have read and understand the Code of Conduct. Symantec may require you to sign additional acknowledgement from time to time indicating that you have read and understand the Code of Conduct and that you are not aware of any violations. Newly hired employees must sign the acknowledgment prior to commencing their employment with Symantec.

Training

You may be required to take a training course covering the Code of Conduct and may be required to take refresher courses from time to time. You may also be required to attend additional training courses if that is appropriate for your job responsibilities. Further guidance and compliance information on the Code of Conduct are available from your local HR contact or the Symantec Legal department.

Monitoring and Auditing Compliance

The Office of Compliance will determine methods to monitor and audit employees' compliance with the Code of Conduct. You must cooperate fully and truthfully in any compliance efforts.

Penalties For Violations

Your compliance with the Code of Conduct is very important to Symantec. Your failure to comply with these standards or with applicable laws is subject to disciplinary action by Symantec, ranging from a reprimand to immediate termination of employment. Symantec may take disciplinary action against:

- Any employee who violates the Code of Conduct or applicable law, or requests that others violate the Code of Conduct or applicable law.
- Any employee who deliberately withholds relevant information concerning a violation of the Code of Conduct or applicable law.
- Any manager who participates in a violation of the Code of Conduct or applicable law, who fails to act diligently in responding to issues raised by employees or who fails to report any possible violations to the Office of Compliance.
- Any manager or employee who retaliates against any employee who reports a possible violation of the Code of Conduct or applicable law or who cooperates in any investigation regarding such possible violations.
- Any employee who knowingly falsely or maliciously accuses another employee of a violation of the Code of Conduct or applicable law.

Waivers of Compliance

The Office of Compliance has the authority to grant waivers of compliance with the Code of Conduct, either proactively or retroactively, except when the waiver involves a director, executive officer, or financial officer.

How to Raise a Concern

Often, the choices we face are difficult to make, and the decisions we make can fall into grey areas. Situations where integrity is questioned are usually emotional and personal, and remaining objective can be difficult. In addition, laws and regulations concerning ethical issues are often complex and subject to interpretation. This is why it's important to speak up, and to ask questions.

Ask yourself:

- Is this legal?
- Does it follow Symantec company policy?
- How will the decision affect others, including consumers, shareholders, suppliers, partners, competitors, the community, and other employees?
- How will the decision look in the eyes of others?
- How would you feel if the decision was made public?
- Have you fully explored the implications of this decision?
- Would additional advice be helpful?

Generally, your immediate manager will be in the best position to understand the situation and resolve the issue. Managers at Symantec are expected to maintain an "open door" policy with respect to your questions and concerns, and to be diligent in responding to issues raised promptly. Managers must report any possible violations of the Code of Conduct to the Office of Compliance. You should also feel free to contact the Office of Compliance directly. You may raise your concern orally or in writing, and if you prefer, you may do it anonymously. The goal is to bring concerns into the open so that any problems can be resolved quickly, preventing any further harm.

Beyond your manager, Symantec offers you several ways to get answers to your questions about ethics issues and to raise any concerns about possible violations of the Code of Conduct or applicable law. You may contact your local human resources representative. You may contact the Office of Compliance, at ethics@symantec.com. If your local management team is unable to help, or you are uncomfortable discussing your concern with them, a toll-free telephone line, called AlertLine, is available to assist you. AlertLine is provided by Global Compliance Services, an independent third party staffed with trained communication specialists who will gather the pertinent information related to your concern. If you choose, you may remain anonymous when you call AlertLine. Reports from AlertLine are provided to the Symantec HR department, which ensures concerns are reviewed and addressed as quickly as possible. All inquiries or reports will be handled as confidentially as possible, although confidentiality may not be appropriate in some circumstances.

You may also contact AlertLine if you believe there has been any violation of Symantec's accounting practices, securities laws or legal requirements, or if there are any issues that you believe should be brought to the attention of the Audit Committee of the Board of Directors.

Our intent is to ensure that Symantec employees have open access to a number of different channels to get answers to ques-

tions, and to raise any potential concerns. If you still believe your concern or question has not been adequately addressed, please contact a member of the Symantec leadership team, including Rebecca Ranninger, Senior Vice President, Human Resources, Art Courville, Senior Vice President, Corporate Legal Affairs & Secretary, or James Beer, Chief Financial Officer. If, however, you prefer to make a report anonymously, the AlertLine service is available.

The obligation to raise a concern about a possible violation of the Code of Conduct, Symantec policy, or the law is one of the most important responsibilities each of us has as a Symantec employee. Failure to raise a concern can cause significant harm to the health and safety of yourself, your fellow employees, the Company, customers, and the communities in which we operate. Failure to raise a concern could also result in the loss of confidence in Symantec by our customers and shareholders. These are just some of the reasons Symantec requires that employees immediately raise a concern.

Non-Retaliation

Under no circumstances will you be subject to any disciplinary or retaliatory action for reporting a possible violation of the Code of Conduct or applicable law or for cooperating in any investigation of a possible violation. However, knowingly false or malicious reports will not be tolerated, and anyone filing such reports will be subject to appropriate disciplinary action.

At Symantec, we want to encourage employees to do the right thing. This includes reporting all violations of the law or company policies, including incidents of harassment or discrimination. Symantec will take appropriate steps to investigate all such reports and will take appropriate action.

AlertLine

To report a concern:

Within U.S./Canada: 1 877 231 0837
International Access: +704 556 7046
Email: symantec@alertline.com

If you need an interpreter to assist you during your call, please inform the AlertLine specialist.

Global • Toll-Free • 24 Hours a Day • 7 Days A Week • Confidential

 P/N 10432999 July 2005


symantec™