SUNGARD®

GLOBAL BUSINESS CONDUCT AND COMPLIANCE PROGRAM FOR THE UNITED STATES

(This document is available internally on the Compliance and Business Ethics site on KnowHow or on your SunGard business division intranet).

TO ASK QUESTIONS AND REPORT POSSIBLE VIOLATIONS:

Use any of the following resources at any time to notify SunGard of a possible violation of this Policy, ask questions about this Policy, or discuss any business related concern that you may have.

1. Contact your Supervisor, any leader in your company's management chain, Human Resources or any other Company official including the Chief Compliance Officer, the Chief Legal Officer, the Director of Human Resources or the Chief Financial Officer. You may contact any corporate officer by name or title by calling Company headquarters at 484 582 2000 or by e-mail.* (See EMPLOYEE RESPONSIBILITY below for more detail).

2. Call SunGard's AlertLine toll-free at 800 381 8372. You may remain anonymous when calling the AlertLine.

3. Contact SunGard's AlertLine on-line at www.sungard.alertline.com. You may remain anonymous when contacting the AlertLine.

4. Contact SunGard's Chief Compliance Officer at any time directly by calling 484 582 5576 or by e-mail.*

5. Contact the compliance office through a general e-mail box at compliance@sungard.com.

6. Contact the Chair of the Audit Committee by mailing a confidential letter to the Chair of the Audit Committee at Company headquarters (680 East Swedesford Road, Wayne, PA 19087).

**The names and contact information of the Chief Compliance Officer, other members of the Compliance Program Committee, Chief Legal Officer, Chief Financial Officer and Chair of the Audit Committee are available internally on the Compliance and Business Ethics site on KnowHow or on your SunGard business division intranet.*

SUNGARD®

Honesty–Integrity–Professional Excellence

GLOBAL BUSINESS CONDUCT AND COMPLIANCE PROGRAM

We must guard our hard earned reputation. It is our most valued asset. Our commitment to legal compliance must be unwavering and we should accept nothing less than unrelenting honesty, integrity and professional excellence in everything we do. If we diligently protect our good name, SunGard will always be a company we are proud to support.

The Global Business Conduct and Compliance Program (Compliance Program) is not a contract and is subject to change at any time, without notice, at the sole discretion of the Company.

Except for the promise of protection from retaliation, none of the benefits, policies, programs, procedures or statements in the Compliance Program is intended to confer any rights or privileges upon any Employee or other Company representative or entitle any Employee or Company representative to remain an Employee or representative of the Company.

TABLE OF CONTENTS

INTRODUCTION

The Board of Directors of SunGard Data Systems Inc. has adopted this Global Business Conduct and Compliance Program ("Compliance Program") to provide you with clear guidelines for your conduct as a representative of the Company. This Compliance Program incorporates a code of ethics for all employees, officers, directors and other representatives of the Company and applies to each of those individuals without exception. The terms "Company" or "SunGard" used in this document mean SunGard Data Systems Inc. and all of its consolidated subsidiaries. These definitions and others can be found in Appendix D to this document.

There is no conflict or inconsistency between good business and good ethics. Our most valuable asset, both as individuals and as a Company, is our reputation. We best serve our customers, our investors and ourselves by adhering to the highest standards of ethical behavior and by maintaining an environment that is fair, open and honest.

OUR VALUES

The Global Business Conduct and Compliance Program is a reflection of our values: our uncompromising commitment to the highest standards of ethical behavior, honesty and fair dealing. These values are the foundation for SunGard's Four Pillars which define our strategic agenda and drive SunGard into the future as a successful and innovative company. When you reflect on our Four Pillars -- keeping clients first, creating a great work experience for our employees, focusing on sustainable growth and getting and staying lean -- know that the Four Pillars stand on SunGard's long and proud history of doing business with integrity.

Our values and the Compliance Program reflect our Four Pillars in a number of ways:

- We **keep clients first** when we protect our reputation for doing the right thing and our clients can count on us to be an ethical business worthy of their trust;
- We **create a great working experience** for our employees when we treat each other with respect, provide a workplace where great performance is measured by achievements and ethical behavior, and where our performance drives success;
- We **focus on sustainable growth** when we expand our markets without compromising compliance with the law or accepting shortcuts that violate global principles of integrity in business; and
- We **get and stay lean** when we use and protect SunGard's resources properly and avoid costly compliance risks.

Whatever your role, your conduct and judgment reflect on our reputation and are critical to supporting the Four Pillars with our values.

GENERAL PRINCIPLES

In our complex global business environment, we recognize that Employees will encounter situations that pose ethical, policy, legal and regulatory issues in connection with the Company's business activities. The Company expects and requires that you will resolve these issues by complying with all applicable laws and regulations and by acting ethically and in accordance with the Company's standards of professional excellence. The Compliance Program is a tool to help you meet this SunGard objective.

You are required to adhere to this Compliance Program. You are encouraged to talk to your Supervisor or other Company officials about any question of proper business conduct, even if it does not seem important at the time. You must avoid any activities that could involve the Company in unethical or unlawful conduct. If you fail to adhere to this Compliance Program, then you are acting outside the scope of the authority given to you by the Company, and you will be held personally responsible for the consequences of your unauthorized conduct.

Adherence to this Compliance Program is a condition of employment. Failure to adhere to this Compliance Program could result in very serious consequences to both the individuals involved and the Company. If you violate this Compliance Program, then you will be subject to appropriate disciplinary and remedial sanctions up to and including immediate discharge and possible legal action by the Company.

Except for the promise of protection from retaliation made in the paragraph below, none of the policies, procedures or statements in this Compliance Program is intended to confer any rights or privileges upon any Employee or entitle any Employee to be or remain an Employee of the Company. This Compliance Program is not a contract and is subject to change at any time, without notice, at the sole discretion of the Board of Directors.

Protection from Retaliation

An individual, who reports incidents that he or she believes to be violations of this Policy, or who is involved in an investigation under this Policy, will not be subject to reprisal or retaliation as a result of such reporting or involvement. Retaliation is a serious violation of this Policy and should be reported immediately. The report and investigation of allegations of retaliation will follow the procedures set forth in this Compliance Program. Any person found to have retaliated against an individual for reporting or for participating in an investigation of allegations will be subject to appropriate disciplinary action.

Reporting Possible or Suspected Violations

Each Employee has an obligation to alert the Company to any situation in which the Compliance Program is being violated or is about to be violated. You should make a report if you are concerned that a Company practice or operation or an Employee action violates a law, rule or regulation, Company policy, or accounting or auditing principle or practice. Report your concerns if the activity in question has not yet occurred, but is being planned or considered. Furthermore, you must make a report if you have been asked by a Supervisor or another Employee to do something that you believe will result in a violation of a law, rule or regulation, Company policy, or accounting or auditing principle or practice. You do not need to be certain that a violation has occurred or is about to occur. Nor do you need proof before you report. You are protected from retaliation for reporting regardless of the outcome of the investigation. You may make a report in any of the following ways:

- Contact your Supervisor, any other Supervisor or any other Company official including the Chief Compliance Officer, any other member of the Compliance Program Committee, the Chief Legal Officer or the Chief Financial Officer. You may contact any corporate officer by name or title by calling Company headquarters at 484 582 2000 or by e-mail.*

- Contact SunGard's AlertLine on-line at www.sungard.alertline.com. By using this system, you may remain anonymous. (See COMPLIANCE ALERTLINE below.)

- Call SunGard's AlertLine toll-free at 1 800 381 8372 from anywhere in the world. These calls are taken by employees of Global Compliance Services, a company specializing in compliance reporting. By calling the AlertLine, you may remain anonymous if you wish. (See COMPLIANCE ALERTLINE below.)

- Contact the Chief Compliance Officer at 1 484 582 5576 or via email (this should not be used for anonymous reports).*

- Send an e-mail to compliance@sungard.com (you may remain anonymous if you send your e-mail using a personal e-mail service that does not identify you).

- Contact the Chair of the Audit Committee. You may mail a confidential letter to the Chair of the Audit Committee at Company headquarters (680 East Swedesford Road, Wayne, PA 19087).* You may remain anonymous.

* *The names and contact information of the Chief Compliance Officer, other members of the Compliance Program Committee, Chief Legal Officer, Chief Financial Officer and Chair of the Audit Committee are available internally on the Compliance and Business Ethics site on KnowHow or on your SunGard business division intranet.*

If the situation involves accounting or auditing principles or practices, internal accounting controls, a violation of law, or another serious matter, or you are concerned that your report is not being addressed in an appropriate and timely manner, then you are encouraged to quickly escalate your concern to higher levels of management including contacting the Chair of the Audit Committee directly.

All reports and investigations will be handled confidentially to the extent possible. Everyone involved in an investigation will use their best efforts to remain impartial and objective, and, to the extent possible, will observe basic principles of due process. No Employee will be judged to have behaved unethically or illegally before he or she has had a reasonable opportunity to explain the circumstances.

COMPLIANCE ALERTLINE

The purpose of SunGard's Compliance AlertLine ("AlertLine") is to help you get your questions about the Compliance Program answered, to receive your reports of possible or suspected violations of the Compliance Program and to facilitate anonymous communications regarding open reports. The AlertLine is available to all Employees and company representatives, twenty-four (24) hours a day, seven (7) days a week including weekends and holidays. You may contact the AlertLine to ask questions or make reports via telephone or on-line in several languages.

Compliance AlertLine reports are handled by trained specialists employed by Global Compliance Services, a third-party vendor, so you may remain anonymous if you wish. When you contact the AlertLine, you will be assigned a report number for future reference. If you wish to check the status of your report or provide additional information, you may call the AlertLine or access your report on-line at any time using your assigned report number.

EMPLOYEE RESPONSIBILITY

Each Employee is responsible for understanding the Compliance Program, the Company's Policies, and the laws, rules and regulations that apply to his or her work. You can familiarize yourself with applicable laws, rules and regulations by receiving on-the-job training, attending Company and outside courses and presentations, reviewing Company Policies, asking questions of your Supervisors, the Chief Compliance Officer and the Legal Department, and calling the AlertLine. You are responsible for being well informed and up-to-date as to your legal and ethical responsibilities.

If you have a concern regarding compliance or you suspect a violation of the Compliance Program, then in most cases, you should discuss this with your Supervisor. Discussions with Supervisors resolve or clarify most issues. However, if for any reason you are uncomfortable discussing your concern or reporting a suspected violation to your Supervisor, then you can and should use any of the other reporting options described under INTRODUCTION above.

The Company also encourages Employees to report their own violations. The Company cannot promise in advance that a self-reporting Employee will not be disciplined or reported to law enforcement authorities, but cooperation will be taken into consideration. You are encouraged to use the AlertLine to seek guidance as to self-reporting a violation.

You may ask questions, address concerns and report possible and suspected violations of the Compliance Program without fear of retribution. All Supervisors and other Company officials are required to maintain an "open door" policy with respect to compliance matters. Under no circumstances will you be subjected to discipline or retaliation as a result of asking a question, expressing a concern or reporting a violation. Any suggestion to the contrary is itself a violation of the Compliance Program. However, an Employee who participates in a violation or knowingly submits a false or malicious report may be disciplined for that conduct.

Employees violating the Compliance Program or Policies will be subject to disciplinary actions. In some cases, this may include immediate discharge and possible legal action against the individuals involved. The Company also may have an obligation to report the matter to appropriate law enforcement or regulatory authorities when the violation of the Compliance Program or Company Policies also is a violation of a law, rule or regulation.

ETHICAL BEHAVIOR

Ethical behavior means more than complying with the law. It means honesty and integrity in every aspect of the Company's activities. Every Employee should be guided by the following general principles:

- Honesty and integrity mean truthfulness and the absence of fraud or deception of any kind. You must act with honesty and integrity in every aspect of your dealings with the Company, other Employees, the public, the business community, investors, customers, suppliers, auditors and governmental and regulatory authorities.

- The Company's books, records, documents, financial statements and public reports and other disclosures must be accurate and complete. A fundamental tenet of this Policy is openness. Every transaction we engage in must be correctly recorded. The Company should have no fear of inspection.

- Employees must accept responsibility for their actions. You have a responsibility to acquire sufficient information to make informed decisions, to deal with others fairly and honestly, and to use the authority given to you by the Company in the best interest of the Company.

- The Company cannot hope to spell out Policies or correct ethical behavior for every situation. Ultimately, we must rely on our own good judgment. When you face difficult decisions, you should seek advice from your Supervisors or any other Company officials including the Chief Compliance Officer, the Chief Legal Officer, the Chief Financial Officer or the Audit Committee Chair.

Integrity, honesty and professional excellence are defining traits of SunGard Employees.

RELATIONSHIPS

Relationships with Employees

SunGard endeavors to deal fairly and equitably with Employees and affirms the principle of equal opportunities within the Company. We will timely inform Employees about Company Policies and plans that may affect them. We encourage feedback from Employees about their work and about the Company.

Our intention is to compensate Employees in relation to their responsibilities and performance and in accordance with the prevailing standards of the communities and markets in which they work.

Relationships with Customers

SunGard prospers only to the degree that we serve our customers honestly and competently. Our competitive appeal must be based upon the quality of our products and services, the prices that we charge for them, the integrity of our sales and marketing efforts, and the reliability of our customer support. The Company will continue to treat all customers, regardless of size, fairly. We will continue to be responsive and courteous to all customers. We will not forget that, without customers, we would not have jobs.

We regularly receive confidential information as part of meeting our contractual obligations. To breach a confidence or to use confidential information improperly or carelessly would be unthinkable. We protect each of our customer's confidential information and use it solely on behalf of that customer and for no other purpose, including trading of securities.

Relationships with Suppliers

Our choice of suppliers is based only upon the quality, price and service offered, giving due consideration, when applicable, to the need for multiple sources of supply. We will conduct open and frank business dealings with our suppliers and will strive to develop mutually advantageous relationships, but will not do so on the basis of reciprocity. We will only purchase goods and services from our suppliers when the combination of quality, price and service are competitive with that of other suppliers.

Relationships with Investors

Our investors have entrusted us with their invested dollars. Our responsibility to them is to do our best to keep our investors' equity secure and to produce a fair return on that equity. By finding the right balance

between short-term profits and long-term goals, we manage our businesses to keep SunGard growing and prospering. In each of our transactions, we will endeavor to promote the interests of our investors.

Relationships with the Public

SunGard recognizes that a corporation has more than an economic existence. SunGard is a part of many communities and must behave as a good citizen. We live in a world that sometimes looks with suspicion upon big business, its motives and its behavior. SunGard will conduct itself so as to reflect well upon the business community as a whole. We also will conduct our business with due concern for our physical environment. We will strive to conserve energy and protect our natural resources.

CONFLICTS OF INTEREST

We all have a duty of loyalty to the Company to further its goals and to work on behalf of its best interests. In establishing and achieving its goals, the Company intends not only to comply with legal requirements, but also to conduct its business affairs with the highest level of integrity. This means that you must use your best care, skill and judgment for the sole benefit of the Company, and that you must not take improper personal advantage of your position with the Company. In dealings with and on behalf of the Company, you should apply strict standards of good faith, loyalty, honesty and fair dealing. In order to honor this standard of behavior, we must do our best to avoid any conflict of interest between our personal interests and those of SunGard. In this context, any interest or involvement of an Employee's immediate family, close friend, or relative is considered an interest or involvement of the Employee.

An actual conflict of interest exists when you have divided loyalty between a personal interest and the interests of the Company. An apparent conflict of interest exists when it reasonably appears to others (who may not know all the facts) that an actual conflict of interest exists, even if you are sure that there is no actual conflict. Whether the conflict of interest is apparent or actual, it can be damaging to our personal and corporate reputation.

It is each Employee's responsibility and obligation to avoid apparent and actual conflicts between personal interests and those of the Company. However, we understand that, even using our best efforts, apparent or actual conflicts of interest will inevitably arise from time to time. So it is critical that we remain sensitive to situations that give rise to conflicts and that we act expeditiously to disclose the conflict by reporting it and assisting in eliminating or mitigating the conflict properly.

Examples of Conflicts of Interest

It is impossible to list every circumstance that might give rise to an apparent or actual conflict of interest. Employees are strongly encouraged to contact the Chief Compliance Officer with questions about any activities that may create a conflict of interest. The following examples will serve as a guide to the types of situations which might involve conflicts and, therefore, should be avoided:

- **Gratuities and Entertainment.** Accepting anything more than nominal inexpensive trinkets from suppliers or companies seeking to do business with SunGard creates the appearance of a conflict of interest even if no actual conflict exists. Please see *Accepting Entertainment, Gifts, or Gratuities from Others* in the section on ENTERTAINMENT, GIFTS AND GRATUITIES below.

- **Conflicting Financial Interests.** Employees and members of their immediate families should not have undisclosed financial interests, such as stock ownership, partnership participation, management, employment, consulting agreements or any other contractual arrangements, with other entities where such involvement is or may appear to cause a conflict of interest situation. Examples of such situations include, but are not limited to:

    1. Direct or indirect material financial interests (including employment or consultant agreements) in any outside company that does business with or competes with the Company.

    2. Direct or indirect competition with the Company in the purchase or sale of technology, property rights or other assets.

    3. Representation of the Company in any transaction in which the Employee has a material financial interest.

    4. Disclosure or use of an Employee's knowledge or information about the Company for the personal profit or advantage of the Employee or anyone else.

    5. Taking personal advantage of an opportunity which the Employee learned of in the course of his or her employment with the Company, such as competing or interfering with the Company in the purchase or sale of property by acquiring property or leases in which the Company may be interested.

    6. Direct supervision of or responsibility for the performance evaluations, pay or benefits of a close relative or other person with whom you have a close personal relationship. See *Family and Personal Relationships* below.

    7. Selling anything to the Company or buying anything from the Company (except in connection with any normal disposal of surplus property by the Company or in connection with the exercise of stock options or similar rights) unless prior approval of Company management is obtained.

    8. Any outside activity that is substantial enough to interfere with the Employee's ability to devote appropriate time and attention to his or her job responsibilities with the Company.

- **Family and Personal Relationships.** Questions concerning confidentiality and objectivity arise when family or close personal relationships combine with workplace relationships. To prevent an actual conflict of interest or the appearance of one, SunGard requires that you disclose any family or close personal relationship among Employees or with customers or suppliers. You do not have to disclose every work-related friendship in order to comply with this section, but you are expected to disclose close personal relationships that could reasonably appear to impair or that in fact impair your objectivity. Disclosure in accordance with this Policy will allow for a practical and appropriate adjustment in job requirements to protect the parties, their colleagues and the Company. The roles and duties of at least one of the parties may be changed in order to remedy the actual or apparent conflict. Examples of conflicts of interest arising out of family and personal relationships include, but are not limited to:

1. Remaining silent about a personal relationship with an applicant, vendor, or candidate for promotion when the Employee has any role in the selection process or is consulted for a recommendation.

2. Employees involved in an undisclosed family or personal relationship and who are working in the same office, product group, or operating entity.

3. Employees involved in an undisclosed family or personal relationship and supervise or otherwise have any ability to affect the work assignments, compensation, performance review or promotion of the other person.

- **Consensual Relationships.** Romantic or sexual relationships among Employees may create especially difficult conflicts of interest and raise unique concerns. Other members of the work group often reasonably perceive a conflict of interest regardless of facts. In addition, not all romantic or sexual relationships end well. Employees in a romantic or sexual relationship must follow Company policy as outlined in the section titled SEXUAL AND OTHER DISCRIMINATORY HARASSMENT and specifically in the paragraph called *Reporting Consensual Relationships*.

Disclosing Conflicts of Interest

Any Supervisor, Executive Officer, or Director who becomes involved in an apparent or actual conflict of interest, should promptly and fully disclose all relevant facts to SunGard's Chief Compliance Officer or another member of the Compliance Program Committee. A Director who becomes involved in a conflict of interest should also report the matter to the Chair of the Audit Committee, in addition to any other reporting deemed appropriate under the circumstances. All other individuals who become involved in an apparent or actual conflict of interest should promptly and fully disclose all relevant facts to his or her Supervisor or Human Resources representative.

Review and Resolution of Conflicts of Interest

When an apparent or actual conflict of interest occurs, the affected individual must abstain from acting on behalf of the Company in connection with the conflict situation. The individuals involved in the apparent or actual conflict of interest are disqualified from determining the resolution of the conflict of interest and must not attempt to improperly influence the decision. The full cooperation of all those affected by the conflict is required to adequately resolve or mitigate the conflict.

If a conflict of interest involves a Director or Executive Officer, or if it is considered material to the Company by SunGard's Chief Compliance Officer or another member of the Compliance Program Committee, the conflict of interest situation will be reviewed by the Compliance Program Committee at its next regularly scheduled meeting or, when the Chief Compliance Officer deems it necessary or desirable, at a special meeting called for that purpose, and the report forwarded to the Audit Committee. SunGard's Compliance Program Committee, in consultation with the Audit Committee, will determine whether an actual or apparent (or potential) conflict of interest exists or will exist, and, if so, what corrective or preemptive action should be taken to resolve the conflict or potential conflict.

In all other cases, conflict of interest situations will be reviewed and resolved by the individual to whom the conflict was properly disclosed as outlined above. The management organization and the Chief Compliance Officer may be consulted for assistance in resolving any such conflict.

Divided Loyalty and Conflicts of Duty for Management Employees

Supervisors and Executive Officers may not engage in any outside employment, whether as an employee, director, executive officer, partner, consultant, trustee or proprietor, with any company or firm, without first obtaining the approval of the Employee's Supervisor **and** SunGard's Chief Compliance Officer or another member of the Compliance Program Committee. Approval will be given if the outside employment will not interfere with the individual's performance of his or her regular duties for the Company and will not create an actual or apparent conflict of interest situation. This Policy applies only to outside employment with business enterprises and not to associations with charitable, religious, civic, educational purposes or other non-profit organizations.

Prohibition on Extending or Maintaining Credit

The Company is prohibited from extending or maintaining credit or arranging for the extension of credit in the form of a personal loan to or for any Director or Executive Officer of the Company.

GLOBAL OPERATIONS

As a global company, SunGard must comply with the laws of the countries in which it operates or does business. These laws usually differ and sometimes are inconsistent. It is the Company's policy to comply, wherever possible, not only with the laws of the United States, but also with the laws of all countries in which the Company operates. Employees involved in the Company's non-United States operations should be aware of their legal responsibilities in the countries in which they conduct business. Where there appears to be a conflict between the laws of the United States and the local law, you should seek the assistance of the Legal Department.

As a United States company, SunGard is obligated to follow the law of the United States wherever it does business. Even if activities are conducted outside the United States, they may be within the reach of United States criminal law, particularly where the activity could have an impact in the United States. Accordingly, unless specifically advised to the contrary by the Legal Department, Employees involved in operations outside the United States must at all times conduct themselves in a manner that is consistent with United States law.

A SAFE AND HEALTHY WORKPLACE

SunGard is committed to providing a safe and healthy working environment, and we will maintain and improve our facilities, equipment and methods to that end. If you observe any unsafe conditions in your work place or in any work place where Employees are working, you are asked to report the condition as soon as possible.

In an effort to maintain the safety and well-being of every employee of SunGard and its business units, SunGard maintains a zero-tolerance policy that strictly prohibits workplace violence. Violent acts or threats of violence against a person, his or her family or property will not be tolerated. Anyone who carries out or threatens violence either directly or indirectly through gestures, innuendo or symbols is in violation of this Policy.

Handguns, other firearms, and other weapons are strictly prohibited on Company premises (including company-owned, -leased, or -controlled buildings and all sidewalks, walkways, driveways and parking lots adjacent to such buildings), as permitted by law. Handguns, other firearms, and other weapons are strictly

prohibited in Company owned or leased vehicles, unless expressly authorized by the Company and in strict compliance with state law regulating the carrying or possession of such weapons. Please consult with Human Resources as to the restrictions and conditions of state law.

Anyone violating this Policy will be subject to disciplinary and remedial sanctions up to and including immediate discharge and possible legal action by the Company.

REGULATED ENTITIES

SunGard has various subsidiaries ("Regulated Entities") that are regulated by governmental agencies and self-regulatory organizations such as the United States Securities and Exchange Commission, the Financial Industry Regulating Authority (FINRA), and the U.K. Financial Conduct Authority. As a result, these subsidiaries are subject to various regulatory requirements and have their own compliance officers and written policies requiring adherence to applicable regulations. The Regulated Entities' compliance officers have a dotted-line reporting relationship to the Chief Compliance Officer. Employees of Regulated Entities must abide by their compliance policies as well as this Compliance Program. Those policies will be consistent with this Compliance Program to the fullest extent possible. To the extent they are inconsistent or broader than this Compliance Program, Employees should adhere to the policies of the Regulated Entity.

The Supervisors over each Regulated Entity must take steps to promote regulatory compliance and cooperation with the applicable regulating agencies such as:

- Establishing written policies and procedures to govern the conduct of employees.
- Conducting periodic operational audits to assess compliance with policies and procedures.
- Cooperating fully and appropriately with regulators.
- Retaining and supporting a qualified compliance officer and other specialized employees to promote compliance with industry specific compliance requirements.

ACCURATE DISCLOSURES, BOOKS AND RECORDS

The laws of countries where SunGard conducts business, including the law in the United States, require that SunGard maintain books and records that are accurate and fairly stated. It is SunGard's policy that all books and records of the Company comply with SunGard's Financial Policy Manual, which is distributed to all SunGard financial professionals, and with generally accepted accounting principles as applied in the United States. In addition, entities located outside the United States may be required to maintain books and records in accordance with local rules and regulations. Not only is keeping accurate records required by law, it is good business practice. Books and records include invoices, timecards, expense reports, internal or external memoranda, correspondence or other communications, including telephone, e-mail or wire communications.

Falsifying internal or external documents, or in any other way causing books and records or financial statements or reports to be inaccurate or misleading, is against this Policy and also may be illegal and subject the violator and the Company to significant penalties. No unrecorded funds or assets may be created or maintained for any purpose. In addition, payments on behalf of the Company may be made

only after appropriate supporting documentation is provided and after obtaining appropriate authorizations. The purpose of the payment must be stated in the supporting documentation.

Examples of violations of this Policy include the following:

- Recording a payment as though it was made to one person, when it was actually made to another.
- Submitting expense reports that do not reflect the true nature, purpose or amount of the expense.
- Submitting a false timecard or time report.
- Retaining e-mail, letters, and other information beyond the retention period prescribed in the Records Retention Policy except when normal deletion is suspended for legal matters.

Protecting the quality and integrity of Company records means Employees should:

- Spend Company funds only for legitimate and necessary business purposes.
- Keep accurate expense records and submit timely expense reports.
- Know the limits of your authority to obligate the Company and never act outside your delegated authority.
- Protect access to Company and customer computer and communication systems.
- Prepare and sign only accurate and necessary Company records.
- Retain and destroy documents in accordance with the Records Retention Policy.

Specialized Role of Financial Professionals

SunGard's financial and accounting professionals have an important role in ensuring that reports and documents submitted to the United States Securities and Exchange Commission are full, fair, accurate, timely and understandable. Our financial and accounting professionals must understand and adhere to the rules for financial reporting and accounting. Financial and accounting professionals are required to act independently and exercise their professional judgment even if their opinion is in conflict with the desires or instructions of others in the Company. Financial and accounting professionals are required to report any event, act or attempted action that could result in a breach of the strict financial reporting and recording standards demanded by SunGard.

Accountability and Financial Integrity

Quarterly, the senior financial officer and senior operating officer of each business unit, group and division (and appropriate corporate officers) are required to provide certifications of financial and operational matters within their areas of responsibility needed in connection with the Company's preparation and filing of reports and documents submitted to the United States Securities and Exchange Commission, including the annual report on Form 10-K, the annual report to investors, the annual proxy statement and the quarterly reports on Form 10-Q.

Each Employee participating in the preparation of such certifications has a duty to carefully compile, analyze and report all relevant information under his or her control necessary to make a timely, accurate and complete statement of the Company's financial and operating condition. Failing to properly disclose relevant information or otherwise jeopardizing the quality and sufficiency of the Company's financial reporting is a violation of Company policy and may subject the individual and the Company to civil and/or criminal liability.

RECORDS RETENTION

The Company has adopted a Records Retention Policy that governs the retention and destruction of all Company documents, communications, correspondence, e-mail and other records. The Records Retention Policy is in effect and should be consulted before any documents are destroyed. The Records Retention Policy may be modified when needed to comply with appropriate laws and regulations.

Special rules governing the Regulated Entities lengthen the amount of time certain types of records such as e-mail must be retained. Employees of Regulated Entities should consult with their compliance officers concerning the relevant requirements.

The Records Retention Policy will be suspended as necessary for legal matters. Therefore, if you become aware of any lawsuit, threat of legal action, government investigation or criminal action, you must immediately suspend destruction of certain documents and contact the Legal Department or the Chief Compliance Officer. Please see the section on LEGAL MATTERS AND INVESTIGATIONS for further instruction.

It is a crime to destroy or alter any record or document with the intent to obstruct any government investigation or legal proceeding. The Records Retention Policy is available internally on KnowHow under Resources, Policies and Guidelines, or on your SunGard business division intranet.

CONFIDENTIAL AND PROPRIETARY INFORMATION

Confidential information is information that the Company considers private and which is not common knowledge among other persons or organizations. Proprietary and trade secret information is information that the Company owns, develops, pays to develop, possesses or to which it has an exclusive right.

During the course of your employment and in performance of your job duties, confidential or proprietary information or Company trade secrets may become available to you. You must safeguard such information. You also must safeguard all confidential information of our customers that they provide to us for purposes of processing data or otherwise conducting business. Access to customer-provided information is on a business "need-to-know" basis.

You must follow confidentiality restrictions from previous employers. You may not use or share at the Company any confidential information or trade secrets obtained from previous employers.

Confidential information, proprietary information and trade secrets include, but are not limited to, the following:

- Information that the Company is required by law, agreement, regulation or policy to maintain as confidential (including customer information or information concerning government examinations or audits).

- The Company's medical, personnel and payroll records of its employees.

- Information that could help others commit fraud, misuse the Company's products and services, or damage the Company's business or the business of our customers.

- The identity of customers and prospects, their specific requirements, and the names, addresses and telephone numbers of individual contacts, prices, renewal dates and other detailed terms of customer and supplier contracts and proposals.

- Information not generally known to the public upon which the goodwill, welfare and competitive ability of the Company depends, including information regarding product plans and designs, marketing and sales plans and strategies, pricing policies, information about costs, profits and sales, methods of delivering software and services, and software and service development strategies, source code, object code, specifications, user manuals, technical manuals and other documentation for software products, screen designs, report designs and other designs, concepts and visual expressions for software products, information, ideas or data developed or obtained by the Company, such as marketing and sales information, marketplace assessments, data on customers or prospects, and other confidential information relating to the business of the Company.

Information about the Company's business plans, including forecasts, budgets, acquisition models and other non-public financial information, expansion plans, business or development plans, management policies, information about possible or pending acquisitions or divestitures, potential new products, markets or market extensions, and other business and acquisition strategies and policies.It is a violation of this Policy for an Employee to disclose, use, release, or discuss any confidential, proprietary or trade secret information belonging to SunGard or to SunGard's customers to or with unauthorized persons both during and after the Employee's association with SunGard. Employees may use, disclose or discuss confidential, proprietary or trade secret information belonging to SunGard or to SunGard's customers information as required by their job responsibilities, as permitted by this Policy, or as required by appropriate court order following prior notice to the Company.

This Policy applies to Employee conduct toward other companies, as well as to Employee activities within the Company. While you should always obtain as much information as possible about the marketplace, you may do so only in accordance with applicable laws and with this Policy. The Economic Espionage Act makes it a crime to take, use or disclose without authorization the trade secrets of another person or organization (including competitors of the Company). SunGard Employees will not obtain proprietary or confidential information improperly from another company. If an Employee is approached with an offer of confidential information, the Employee must immediately discuss this matter with his or her immediate Supervisor, the Chief Compliance Officer or the Legal Department. The Company opposes the unlawful use of our competitors' trade secrets. For more information, see SunGard's *Guidelines for Competitive Intelligence Gathering* available internally on the Compliance and Business Ethics site on KnowHow or on your SunGard business division intranet.

The files, manuals, reports, notes, lists and other records or data of the Company, in any form, are the exclusive property of the Company and must be returned at the end of employment with the Company.

Also, all correspondence files, business card files, customer and prospect lists, price lists, software, manuals, technical data, forecasts, budgets, customer materials, notes and other materials that contain any confidential or proprietary information must be returned; and the departing Employee must not retain any copies, excerpts or summaries of those materials. Further, confidential, proprietary or trade secret information remains confidential after an Employee's employment with the Company and may not be disclosed or used for any purpose after the Employee's employment with the Company ends. The Economic Espionage Act also makes it a crime to use the Company's trade secrets for the benefit of another person or organization.

INTERNET, NETWORK AND COMMUNICATION RESOURCES

Use of the Internet through the SunGard Network is provided for business purposes. This access represents the use of Company resources for telecommunications, networking, software and storage.

Except as stated in USE OF COMPANY PROPERTY AND SERVICES below, the SunGard Network (including the intranet) and Internet are to be used for business-related purposes only. Employees are required to act honestly and appropriately, respecting the copyrights, software licensing rules, property rights, and privacy of others. When using the Internet, Employees should remember that they are entering a global community and that all information is public. Any actions taken by an Employee will be a reflection upon SunGard, and such actions must be both ethical and legal. All existing Company policies including property protection, privacy, misuse of Company resources, sexual harassment, harassment, information and data security and confidentiality apply to Employee conduct on the Internet, subject to and consistent with local law requirements.

The Internet may not be used in any way that may be illegal, excessive, disruptive, offensive to others, or considered harmful to the Company. The display or transmission of sexually explicit images, messages, jokes or cartoons is prohibited. No transmission or use of e-mail may contain racial or sexual slurs or anything that may be construed as harassment or disparagement of others based on their race, creed, pregnancy, ancestry, religion, color, national origin, citizenship status, genetic information, political status, age, marital status, sex, sexual orientation or preference, veteran or disabled veteran status, or the presence of a disability or any other protected characteristic.

Employees may not download or distribute illegally obtained software, distribute any virus, attempt to disable a system or network or attempt to defeat network security. Company communication equipment and Company Internet access will not be used for "spamming," mass mailings, cold-call telemarketing, unsolicited fax broadcast marketing, chain letters, file sharing, outside business ventures, unauthorized distribution of confidential information, or political or religious purposes.

Except where sponsored by SunGard Marketing, Employees are prohibited from creating links between any external web site and a web presence created by or for the Company or any of its businesses or affiliates. Employees may not use SunGard trademarks or any language that implies SunGard endorsement on non-SunGard web sites. Employees may participate in social media, so long as they comply with the *SunGard Social Media Guidelines*.

The Company reserves the right to monitor and inspect network or Internet usage and e-mail. Subject to local law requirements, Supervisors may review Internet activity, network use and e-mails to confirm compliance with this Policy and that the highest standards are maintained when Company resources are used.

Should the Company's resources be used to violate laws and regulations, the Company will report the illegal activity to the appropriate law enforcement agency and this activity will be grounds for immediate termination.

For more information on technical systems and resources, refer to SunGard's Acceptable Use of Technology Policy, the Global Information Security Handbook and the *Social Media Guidelines* which are available internally on KnowHow under Resources, Policies and Guidelines, or on your SunGard business division intranet.

E-MAIL

Like Internet and network usage, use of e-mail through the Company is a privilege intended for business purposes, not a right. Any e-mail sent by an Employee will be a reflection on SunGard and, therefore, must conform to the Company's ethics and principles. E-mail has the same legal import as other written communications such as letters and memoranda and is not to be used for non-business purposes (except see USE OF COMPANY PROPERTY AND SERVICES below). All e-mail on SunGard computers or drafted by SunGard Employees as part of their employment is the property of SunGard and may create binding contracts, actionable expectations and other legal consequences. E-mail is fully discoverable in litigation and other proceedings to the same extent as other written communications. Therefore, any e-mail may be subject to monitoring, search or interception at any time, with or without notice to the sender or recipient, in compliance with applicable laws.

Accordingly, when preparing e-mail, you should use the same careful deliberation as when preparing a letter or memorandum. You should never say something in an e-mail that you would not say in a letter. Likewise, imprecise or unprofessional communications are not any more appropriate in e-mails than they would be in letters or memoranda. When evaluating what information to put in e-mail, you should consider who the recipients are, the level of confidentiality necessary, and the possible repercussions if confidentiality is not maintained.

All existing Company Policies including property protection, privacy, misuse of Company resources, sexual harassment, harassment and discrimination, information and data security and confidentiality apply to Employee e-mails, subject to and consistent with all applicable laws and regulations. E-mails may not be used in any way that may be illegal, excessive, disruptive, offensive to others, or considered harmful to the Company. The display or transmission of sexually explicit material including images, messages, jokes or cartoons is strictly prohibited. No transmission or use of e-mail may contain racial or sexual slurs or anything that may be construed as harassment or disparagement of others based on their race, creed, pregnancy, ancestry, religion, color, national origin, citizenship status, genetic information, political status, age, marital status, sex, sexual orientation or preference, veteran status, disabled veteran, the presence of a disability, or any other characteristic protected by law.

In the same way that a written letter or report is subject to the Records Retention Policy, an e-mail once sent or received is also subject to the Records Retention Policy (available internally on KnowHow under Resources, Policies and Guidelines, or on your SunGard business division intranet). In determining how long to retain e-mail, you must evaluate the content of the message. E-mail retention is determined by its content, not its format.

INTELLECTUAL PROPERTY

Intellectual property is a valuable asset. Intellectual property includes patents, trade secrets, trademarks, copyrights including moral rights, and proprietary information. SunGard will protect, maintain and defend its rights in all commercially significant intellectual property and it is every employee's obligation to safeguard SunGard's intellectual property.

In addition to protecting SunGard's intellectual property, SunGard respects the intellectual property rights of others. Unauthorized use of the intellectual property of others may expose SunGard to legal action and potentially to damages. In many countries, theft and misappropriation of intellectual property or proprietary information may result in significant fines and even criminal penalties for SunGard and the individuals involved. Before using intellectual property of others, you must ensure that you have a license to do so and that your proposed use is consistent with the terms of the license. You should consult with a SunGard attorney before soliciting, accepting or using proprietary information from anyone outside of SunGard.

A Special Word about Software

Most computer software is protected by copyright laws including moral rights laws, and contractual restrictions that safeguard the software manufacturer's investment in creating the software. As a software manufacturer, the Company has a special appreciation for the importance of respecting other manufacturers' investments in their products.

When the Company or an Employee licenses a copy of a software product, the third-party licensor or copyright owner, and not the licensee of the software, retains the right to control the number of copies made of the software. The licensee's rights to use the software are set out in a license agreement that comes with the software.

The precise terms of software licenses vary among software vendors and products, but certain key restrictions are common to most licenses. The Company intends to honor all third-party software copyrights and license agreements.

Most software licenses prohibit the sharing of licensed software packages, other than with the networking application for which they were purchased. Only SunGard licensed software and materials may be placed on the Company's technology. If you feel that SunGard should purchase licensing rights to particular software, please discuss this matter with your manager and, if approved, Information Technology Office. To promote compliance with third-party software license agreements (e.g., word processing software), the following procedures will be followed by all Employees:

- All third-party software must be properly licensed. Employees should use third-party software only in the manner specified in the supplier's manual and license agreement. Copies of software may not be made without appropriate licenses being obtained. Pirating software has legal ramifications for users as well as for SunGard and is strictly prohibited.

- If you feel that SunGard should purchase licensing rights to particular software, please discuss this matter with your manager and, if approved, an authorized representative from your Segment's Information Technology Office. Employees may not make any copies of software manuals. Requests

for additional software manuals should be made to the Employee's Supervisor or Information Technology Office.

- No trademark or copyright notices on any third-party software should be changed or deleted.

- Do not share software, or download software from the Internet without authorization from your Segment's Information Technology Office.

It is extremely important for all Employees to follow these procedures. Improper copying or use of computer software can subject the Employee and the Company to civil and criminal penalties, and may cause substantial disruption and embarrassment to our Company. Unauthorized software use can also expose computer hardware and software to harmful computer viruses. For additional information on this topic see the Acceptable Use of Technology Policy.

USE OF COMPANY PROPERTY AND SERVICES

All Company property is for the Company's benefit. No Employee may use Company property or services (including Company-owned software) for personal profit or for the personal profit of anyone else. Theft and misuse of Company property and services are prohibited. Any Employee having knowledge of a theft or misuse of Company property and services should report the matter to his or her immediate Supervisor. The term **"Company property"** includes every physical item and electronic system in the workplace, including information stored on computers, e-mail, voicemail, interoffice mail, photocopiers, fax machines, vehicles, tools, equipment, office supplies and office furniture. The term "**Company services"** means services rendered by Company Employees or representatives in the regular course of business, including, but not limited to, secretarial and administrative services.

Limited Personal Use

The Company realizes that sometimes the occasional and limited personal use of Company Property may benefit both the individual and the Company, for example, participating in continuing education programs or writing technical articles. Because it may be difficult to judge when Company business becomes personal use, except as permitted below and the in Acceptable Use of Technology Policy, you should speak to your Supervisor before using Company property or services for matters outside of your job responsibilities.

Company Internet connection, e-mail, telephones and copy and fax equipment are intended for use in conducting SunGard's business and these assets must always be used with the best interests of SunGard in mind. The Company recognizes that the occasional personal use of these assets will accommodate legitimate personal needs such as checking the weather on the Internet for travel destinations, quick correspondence through e-mail with family members and friends, checking flight arrival/departure times for personal travel, making doctor appointments, and arranging childcare, to name a few. It is essential that the use is not excessive and does not interfere with business-related responsibilities or the responsibilities of others. Therefore, the Company's Internet connection, e-mail, telephones and copy and fax equipment may be used for occasional and limited personal use by SunGard Employees under the following conditions:

- All personal use must comply with applicable law and with Company's policies.

- Personal use must be occasional and not interfere with your own or anyone else's work responsibilities or with service to our customers.

- Personal use must not interfere with the conduct of our business.

- Company assets must not be used to support or conduct a business or commercial enterprise other than SunGard's business.

- Personal use must never reflect unfavorably on SunGard, its reputation, its credibility or its customers or Employees.

- When you visit a web site for personal reasons, you are expected to use professional judgment and adhere to the guidance provided in this Compliance Program and the Acceptable Use of Technology Policy.

The Company has the right to access and inspect all electronic systems and physical property belonging to it. Employees should not expect that any items created with, stored on, or stored within Company property will remain private. This includes desk drawers, even if protected with a lock, and computer files and electronic mail, even if protected with a password. Personal use of Company electronic systems and other Company assets will result in SunGard's access to the content of personal e-mail, personal telephone conversations, and personal files.

If an Employee leaves SunGard, all Company property must be returned on or before the departing Employee's last day of work.

For more details on the Company's policy relating to Company property including e-mail, see the sections on INTERNET, NETWORK AND COMMUNICATIONS RESOURCES, E-MAIL, and INTELLECTUAL PROPERTY.

ILLEGAL INSIDER TRADING AND DISCLOSURE

"Insider trading" is a term that most Employees have heard. It is usually associated with illegal conduct. But the term actually includes both legal and illegal conduct. The legal version is when corporate insiders—officers, directors and employees of a company—buy and sell stock or other registered securities in their own companies. Insiders are permitted to trade in their company's securities provided they comply with the strict requirements of United States securities laws.

Illegal insider trading refers generally to buying or selling a security, in breach of a fiduciary duty or other relationship of trust and confidence, while in possession of material, nonpublic information about the security. Insider trading violations may also include "tipping" such information, securities trading by the person "tipped," and securities trading by those who misappropriate such information.

Under the securities laws of most countries including the law of the United States, people who engage in illegal insider trading are subject to civil and criminal penalties. For that reason, SunGard makes this policy applicable to every Employee regardless of location.

The general rule against illegal insider trading can be stated as follows: It is a violation of securities laws for any person to buy or sell securities if he or she is in possession of material inside information. The

information is ***material*** if it could affect an investor's decision to buy, sell or hold a security. It is ***inside information*** if it has not been publicly disclosed. These scenarios are examples of illegal insider trading:

- Corporate officers, directors, and employees who trade the corporation's registered bonds after learning of important and confidential corporate developments.

- Friends, business associates, family members and other "tippees" of such officers, directors, and employees, who traded the bonds after receiving the information.

- Employees of law, banking, brokerage and printing firms or other suppliers who are given the information to provide services to the corporation whose securities they traded.

- Other persons who misappropriated, and took advantage of, confidential information from their employers or who received the information from an employee of a customer, supplier or competitor.

We are often in a position to learn information from our customers or suppliers and even from our competitors. If you are offered material non-public information or you become aware of material non-public information, you are prohibited under this Policy from buying, selling or otherwise trading, applying for or procuring another person to apply for, buy or sell, or tipping anyone concerning any public company securities. Actions that violate this policy may also violate the securities law. The prohibition applies for a period of one full business day after any such material information becomes publicly available. The one-day restriction allows a reasonable period for the market to react to announced information.

Restrictions on Disclosure

Insiders are prohibited from discussing non-public material information with any person outside of the Company or otherwise disclosing non-public material information outside of the Company, unless and only to the extent required in the normal performance of assigned responsibilities.

Special care must be taken to observe this disclosure restriction when responding to inquiries from the media, such as representatives of trade publications. If an Employee receives an inquiry from an actual or potential investor, a financial reporter, an investment analyst, or another member of the financial community, he or she should decline to comment on behalf of SunGard or in a way that could be construed as being on behalf of SunGard, and instead should refer the inquiry to SunGard's Chief Compliance Officer, Corporate Secretary, Chief Legal Officer or Chief Financial Officer.

Even within the Company, disclosure of and access to non-public material information must be strictly limited to those authorized to receive it.

This restriction also applies to disclosure of information via the Internet, including, but not limited to, participation in "chat rooms," "message boards" or similar Internet venues.

The above disclosure restrictions apply whether or not the disclosure would be intended to influence trading in any SunGard registered securities.

All disclosures of material information, other than those contained in normal product announcements and similar marketing materials, will be made by corporate press release under the direction of the Company's Chief Legal Officer and Chief Financial Officer.

ANTITRUST AND COMPETITION LAWS

The Company's policy is to comply fully with both the letter and spirit of the United States and all non-United States local antitrust and competition laws. These laws seek to preserve a free competitive economy, which is essential to the interests of the public, the business community and the Company itself. Violations of the antitrust and local competition laws can result in individual and corporate criminal liability and prosecution. Substantial civil fines and injunctions can also result.

Antitrust and competition laws are extremely complex and the Company must have specialized legal advice to analyze potential issues in this area. The purpose of antitrust and competition laws is to benefit consumers by keeping prices low and the quality of services high. This Policy statement is intended only to highlight some areas that may involve antitrust and competition law issues so that Employees recognize problems and seek guidance before problems arise. You should contact the Company's Legal Department whenever you have any antitrust or competition law questions.

Agreements with Competitors

Competitors should not agree together on the prices they will charge for their products or services or on other price-related matters. This is the clearest of all antitrust rules, and a violation of this rule likely will be prosecuted. Care also should be taken during trade association meetings to avoid pricing discussions. Given the serious nature of this type of violation, no Employee should ever discuss or reach an agreement with a competitor (or supplier) on Company prices or the competitor's prices, pricing policies such as discounts and profit margins, or practices, fees, or terms or conditions of sales.

It also may be illegal for Company representatives to allocate markets between competitors, to agree with competitors on the territories in which each company will sell its products, or the customers to which each company will offer its products, or the types of products or the amount of any product each company will produce or offer for sale in the marketplace.

In addition, you should not have discussions with competitors in relation to limiting production, whether or not to deal with any other business, or share any competitive information concerning the Company's or a competitor's business. Do not have discussions with competitors about any of the subjects listed in this section unless you have first consulted with the Legal Department.

A violation of these guidelines is almost always illegal. Any contact with a competitor can inadvertently create the appearance of an antitrust or competition law violation. Employees should avoid any conduct that could be interpreted as an illegal agreement with competitors (or suppliers). These restrictions also apply in the context of an acquisition.

Agreements between Buyers and Sellers

- **Tying Arrangements.** An unlawful tying arrangement exists when one company conditions the sale of a product on the purchase of some other unrelated product. For example, in the software industry, "tying" may occur when a company conditions a contract for one software system on the purchase of

a contract for another, unrelated system. "Tie-in sales" arrangements are generally illegal. You should never attempt to force or mislead customers into purchasing software or services. Any questions about tying arrangements should be referred to the Legal Department.

- **Resale Price Maintenance.** Company Employees should not enter into agreements to fix the price or the minimum price that a purchaser will resell Company products. However, it is not illegal to have "suggested" retail prices.

Other Restrictions and Arrangements

- **Selection of Customers and Vendors.** SunGard is generally free to select its own customers and vendors. This right, however, must be exercised by the Company alone and not jointly with other companies. Agreements between two (2) or more companies not to do business with a third company can be a violation of antitrust and competition laws.

- **Restrictions on Dealing with a Competitor.** SunGard will not make the sale of products and services to any customer contingent upon the customer's refusal to do business with competitors. By requesting such a contingency, you could create antitrust and competition law issues. This could also be an unfair method of competition. You cannot condition the sale of Company products on a customer's refusal to deal with competitors.

- **Reciprocal Dealing Arrangements.** The Company will sell products and services on the basis of their value to our customers, not by using our purchasing power as a real or implied threat. SunGard will not require our suppliers to buy from the Company. SunGard also will not agree to purchase goods or services from our customers under any circumstances that amount to or suggest reciprocal dealing.

Special Concerns Applicable to the Acquisition of Competitors

In the context of antitrust and competition law the term "competitor" is a specially defined term that has a specific legal definition. Not all acquisitions of other companies involve the acquisition of a "competitor" as that term is applied in antitrust and competition laws. However, when the parties to an acquisition are "competitors" according to the legal definition, antitrust laws continue to apply to their interactions before closing, no matter how sure you are that the deal will close. Therefore, the need to exchange information for valuation and planning purposes must be tempered by the obligation to comply with antitrust laws. To do this, you must avoid exchanging certain types of sensitive competitive information, and you must not engage in certain types of anti-competitive activities. In addition, with all acquisitions, our Policies require that you limit access to information to only those people within SunGard who need to be involved in order to evaluate and negotiate the transaction or to plan post-closing operations. When acquiring a competitor, this becomes even more important. To the fullest extent possible, you should exclude from the need-to-know group all sales, marketing, operations and other personnel who are directly involved in our business units that compete with the target.

The need-to-know concept applies not only to information and documents received in due diligence, but also to all internally produced documents and communications (including e-mail) about any aspect of the transaction.

- **Due Diligence.** You must limit the exchange of information to only what is required to evaluate and negotiate the transaction and to plan post-closing operations. The first list below provides examples of types of information that generally may be exchanged. The second list provides examples of sensitive, competitive information that generally may not be exchanged.

  Examples of information that generally **may** be exchanged:

  - All public information.
  - Historical financial information presented at an aggregate level, including financial statements such as income statements, balance sheets and profit and loss statements.
  - Historical production information, including production costs, capacity, and utilization rates (if applicable).
  - Historical percentage of revenue derived from key customers.
  - Contracts of top customers.
  - Historical systems and IT information.
  - Possible efficiencies that can be achieved from the merger.
  - Historical aggregate cost and price information (avoid "micro" information about cost or prices to specific customers).
  - Tax, environmental, health and safety data.
  - Aggregate historical labor costs and employee information including non-price terms of labor agreements, such as termination provisions. Wage information cannot be exchanged unless that information is public.

  Examples of information that generally **may not** be exchanged:

  - Current or prospective pricing of the Company's products.
  - Bids, fee schedules and pricing policies.
  - Current or future costs (other than as indicated above).
  - Names of prospective customers or vendors (i.e., targets).
  - Long and short-term marketing and strategic plans, including future distribution and circulation plans.
  - Plans to expand or reduce output.

- Trade secrets and other proprietary technology and data.

- Current and future wages and wage scales for employees.

- Status of negotiations with existing and potential customers.

To the extent that a limited exchange of sensitive competitive information is necessary to evaluate the transaction, it must be handled carefully and should be coordinated by counsel. For example, before delivery of documents to you, the target's counsel should redact customer names and pricing information from copies of proposals and pending customer contracts. Also, review of sensitive competitive information should be handled by legal or financial personnel rather than business personnel; and you should consider using outside firms to do the detailed reviews, providing to you only the necessary summaries of the information.

- **Planning Post-Closing Operations.** In planning post-closing operations of the target (or the combined business), you must avoid any attempt to influence or control pre-closing operations of the target. You may form transition teams to plan the post-closing integration of information systems, staffing requirements, administrative functions and the like. You may not, however, do any of the following before closing:

  - Reach any agreement on bids, prices, fee schedules, pricing policies or marketing plans that may affect either party's activities before closing.

  - Jointly approach existing or potential customers, unless a customer requests a joint meeting in writing and you first consult with counsel.

  - Allocate customers, prospects or territories in planning post-closing operations.

  - Delay or refrain from soliciting new customers that you would have pursued in the absence of the transaction. You must continue to compete as if the transaction were not to close.

  - Exchange the names or identities of any potential customers or the details of proposals made to potential customers.

  - Reach any agreement or otherwise influence or control the timing of customer contract signings.

  - Base individual business decisions on any confidential information received from the other party.

- **Appropriate Contract Terms.** It is generally appropriate for SunGard, when agreeing to acquire a company, to:

  - Require that the to-be-acquired company during the pre-consummation period will continue to operate in the ordinary course of business consistent with past practices.

  - Condition the transaction on a requirement that the to-be-acquired company during the pre-consummation period not engage in conduct that would cause a material adverse change in the business.

- Require that the to-be-acquired company during the pre-consummation period will not offer or enter into any contract that grants any person enhanced rights or refunds upon the change of control of the to-be-acquired person.

- Provide that either party may conduct reasonable and customary due diligence prior to closing the transaction (subject to the restrictions on information exchange discussed above).

LEGAL MATTERS AND INVESTIGATIONS

Specialized Role of Legal Professionals

Attorneys and other legal professionals employed by SunGard are required to act independently and to exercise their professional judgment in all matters even when their opinion is in conflict with the desires or instructions of others in the Company. Under this Policy and the SunGard Policy for Attorneys Reporting Legal Violations Including Reporting Under SEC Rule 205, which is distributed to all legal professionals employed by SunGard, legal professionals have a duty to report known or suspected violations of this Policy, local law or other applicable law or regulation arising out of the conduct of Company business.

Legal Representation and Assistance with Legal Matters

The Legal Department will provide SunGard business units assistance not only with litigation, dispute resolution, statutory and regulatory compliance, contract drafting and negotiation and similar legal matters, but also with structuring and negotiating business transactions. Once a need for legal services has crystallized, a request for legal assistance should be made as early as possible and should be accompanied by sufficient information to facilitate efficient handling of the request.

Relationship with Outside Counsel

The Legal Department is responsible for managing the Company's overall relationships with outside counsel including fee arrangements. To avoid conflicts of interest and to minimize overall legal expenditures, all referrals to outside counsel must be made in accordance with procedures established by the Legal Department or otherwise with the consent and participation of the Legal Department. A list of all expenses incurred for outside counsel should be sent to the Legal Department on a quarterly basis.

Legal Actions

It is the Company's policy to participate fully and appropriately in all legal actions arising out of the conduct of the Company's business. The Legal Department must be kept advised, on a current basis, of all legal matters involving the Company. You must notify the Legal Department immediately whenever (1) any complaint, subpoena, summons or other legal papers are received, (2) any lawsuit or other legal action is started or threatened in writing by any company, individual or other entity, or (3) any contractual dispute or other circumstances arise that have a realistic possibility of leading to litigation or other legal proceedings.

The Company has the right to be represented in legal actions and Employee interviews by its own legal counsel. You should not engage in discussions or proceedings with auditors, private investigators or

lawyers representing the commercial interests of third parties or other entities without Company counsel present or involved.

Government Investigations

It is the Company's policy to cooperate fully with governmental investigations. In this section, "government" means any department or agency of the government including the United States government and any governmental regulatory agency or body acting within the scope of its authority. The Legal Department also should be contacted immediately—before any action is taken or promised—if you receive or have knowledge of a work-related subpoena, a civil or criminal action, or a written government request for information such as a Civil Investigative Demand (called a CID) or a first-day request received before a data processing (EDP) audit. If a government investigator or government attorney asks you personally for information about SunGard, the Company would prefer to be notified before the interview and to be present at the interview.

During the course of an investigation, government investigators may contact Employees at home or at their office and request an interview. Remember that the investigator has the right to request to speak to you and you have the right either to speak to the investigator or to decline to speak. If you decide to submit to the interview, you have the right to submit only on the condition that you have legal counsel present. If you are subpoenaed or otherwise legally compelled to provide testimony, you must comply.

Sometimes it is difficult to tell when a routine government audit or inspection graduates into a governmental investigation. You should consult with the Legal Department or the Chief Compliance Officer to better understand the nature and implications of any government activities.

Preserving Company Documents and Records

Virtually all of the laws regulating the conduct of the Company's business contain criminal and civil penalties. For example, it is a crime to destroy or alter any record or document with the intent to obstruct any government investigation or legal proceedings. If an Employee violates the law or causes the Company to violate the law, then both that Employee individually and the Company may be subject to criminal penalties. SunGard's Record Retention Policy will be suspended for documents and records related to matters that are the subject of a government investigation or request for information and for any civil legal action or subpoena. (See RECORDS RETENTION in this Policy.)

No Employee should ever, under any circumstances:

- Destroy Company documents in anticipation of a request for those documents from a government agency or court.
- Alter a Company document or record after it has been adopted.
- Lie or make misleading statements to governmental investigators during any investigation. It is illegal to make false statements to governmental investigators under any circumstances.
- Encourage or pressure anyone to hide information or to provide false or misleading information.

- Fail to cooperate in any manner with any internal investigation. Employees should be forthcoming with information that pertains to the matter under investigation.

- Retaliate in any manner against any Employee for cooperating in an investigation or court action.

In some government investigations or legal actions, the Company's lawyers can protect the interests of both the Company and its Employees. In some cases, however, there may be a potential conflict of interest between the Company and individual Employees, and individual Employees may need their own legal counsel. Employees should consult with the Company's Legal Department for guidance in these cases.

The Company and its Employees have the right to be represented by legal counsel at all times when questioned by federal or state investigators or by opposing counsel in litigation, whether or not questions are asked during business hours, and whether or not questions are asked at Company premises or off-site (including at an Employee's home) about anything concerning Company business. An Employee should ask for time to consult with an attorney before answering questions about anything concerning Company business.

CHARITABLE DONATIONS

Any proposed donation must be consistent with SunGard's values and business objectives and be approved by the applicable senior finance executive and division president. Only legally recognized charities are eligible recipients. Donations must be made publicly and in accord with the recipient's written policies. Donations must be made by company draft or electronic funds transfer from SunGard to the recipient. No donation may be reimbursed via expense reimbursement request. The donation must be properly recorded in the Company's books and records.

ENTERTAINMENT, GIFTS AND GRATUITIES

For additional restrictions and information on offering gifts or gratuities to government officials, see CONTRACTING WITH GOVERNMENT ENTITIES AND OFFICIALS AND PROHIBITED PAYMENTS below.

Offering Entertainment, Gifts or Gratuities to Others

The Company markets its products on the basis of price, quality and service. The Company will not use inappropriate gifts, donations, excessive entertainment, or any improper means to influence customers or potential customers. All entertainment, gifts and gratuities must be recorded on the Company's financial records.

SunGard policy prohibits all forms of bribery regardless of the situation or the recipient. The use of Company funds for bribes, kickbacks or for any other unlawful or improper purpose is strictly prohibited. No Employee or anyone acting on behalf of the Company or providing services for or on behalf of the Company may offer, give or promise anything of value to any person for the purpose of, or as a reward for, improperly obtaining business, retaining business or for the purpose of, or reward for, improperly securing a financial or other advantage. No Employee**,** or anyone acting on behalf of the Company or providing services for or on behalf of the Company, may offer or give anything of value to any person, knowing that all or part of the payment will be directly or indirectly offered, given or promised to

someone for a corrupt purpose. Employees may not use outside persons or entities in connection with the Company's business for the purpose of circumventing this Policy. There is no exception for bribes of minimal value and even offering or promising a bribe violates SunGard policy. Personal favors and gifts are considered the same as payments under this Policy.

If you receive a request for an improper payment, you should inform your Supervisor **and** the Chief Compliance Officer immediately.

Accepting Entertainment, Gifts or Gratuities from Others

Never ask for a personal benefit from people doing business or seeking to do business with SunGard. In this context, a personal benefit includes, but is not limited to, a payment, gift, favor or travel. When offered, Employees may accept routine promotional items of nominal value, for example, pens, paperweights and tee shirts. Entertainment, including meals, is considered a "gift" and may be accepted only when it has nominal value and is reasonable and customary within ethical business practices. For example, hosted invitations to local regular season sports events or local cultural events are common business practices and may be accepted.

Generally, Employees should not accept other gifts, entertainment or other favors from any outside person or entity that does business with, seeks to do business with, or competes with the Company. Employees may never accept cash or the equivalent of cash, no matter the amount.

Before accepting invitations, travel, gifts or other gratuities, even if the thing offered complies with this policy, seek approval from your supervisor in advance.

Anything promised, offered or given that is intended to improperly influence your business judgment is inappropriate. If you receive a gift that you believe is inappropriate and you cannot return it, take other steps to diffuse the potential appearance of impropriety, such as redirecting the gift to a charity or sharing the gift within your office. Let the sender know that future gifts are not appropriate. If you are offered a favor, gratuity, or payment, that you believe was offered to improperly influence your business judgment inform your Supervisor **or** the Chief Compliance Officer immediately.

Common Sense Standards

The following illustrate the Company's policy concerning the proper approach to giving and receiving gifts and other business courtesies:

- Never give or accept, either directly or indirectly, cash gifts or cash equivalents such as gift cards or pre-paid debit cards.
- Never ask for a gift for yourself or for anyone else.
- Business gifts should be modest in value, which means unmistakably inexpensive.
- Consumer electronics like computers and tablets are not inexpensive and are not appropriate gifts.
- Gifts should have a clear business nexus such as SunGard branded items, business books, or desk items.

- Gifts should be exchanged publicly or in such a way that an independent person would perceive the exchange as appropriate.

- Most companies have policies that govern their employees' ability to give and receive gifts. To avoid placing a client in an awkward or compromising position, you should become familiar with each client's gift and entertainment practice before offering gifts or entertainment of any type.

- Any entertainment given or received should be moderate and in good taste and otherwise comply with this policy. The term "entertainment" describes events such as meals and charitable or sporting events, such as golf, parties, plays and concerts. Use good judgment when choosing to give or accept entertainment. The type of entertainment offered or received is a reflection on our integrity as a company, and inappropriate entertainment should never be provided or accepted.

For more information see the *Guide to Combating Bribery and Corruption* available internally on the Compliance and Business Ethics site on KnowHow or on your SunGard business division intranet.

CONTRACTING WITH GOVERNMENT ENTITIES AND OFFICIALS

There are often special rules and accounting standards that apply to doing business with a government entity (including a state-owned enterprise). Before any Employee seeks to do business with a government entity, he or she must consult with the Legal Department concerning proper bidding, accounting and performance procedures. This requirement applies when a SunGard company seeks to act as prime contractor to a government entity or as a subcontractor under a government contract.

Most countries make it illegal to give anything of value to a Government Official in return for that person's influence, action, inaction or testimony. It is also illegal to do anything that will benefit a Government Official directly or indirectly, if such action results in, or is a reward for, that person's influence, action, inaction or testimony for the improper benefit of the Company. Violations can result in severe fines and imprisonment.

See the PROHIBITED PAYMENTS section below for the definition of **"Government Official"** and SunGard's policy concerning offering of entertainment, gifts and gratuities to Government Officials. Be aware that the term Government Official is broad and includes people who are not elected or appointed public officials, such as persons acting on behalf of government-owned or controlled companies.

PROHIBITED PAYMENTS

Governments and multi-national organizations around the globe have enacted laws and published conventions condemning and outlawing corrupt payments (bribes). Most countries make it a crime to give, offer or promise anything of value to a Government Official in return for that person's influence, actions, inaction or testimony or as a reward for any such influence, action, inaction or testimony improperly exercised. In fact, doing anything that personally benefits a Government Official directly or indirectly, is illegal if such action results in, or is an improper reward for, that person's influence, action, inaction or testimony. Violations can result in severe fines and imprisonment.

In particular, the United States law known as the Foreign Corrupt Practices Act (FCPA) and the United Kingdom's law known as the UK Bribery Act 2010 (Bribery Act) apply to business inside and outside the respective countries. Both laws make bribery of government officials criminal. The Bribery Act also

criminalizes bribery in a commercial or private business context. (See the section on ENTERTAINMENT, GIFTS AND GRATUITIES.) The Bribery Act, which became effective July 2011, also makes failing to prevent bribery a criminal offense for commercial organizations. Under both laws, SunGard can be liable for the actions of its employees and the actions of those who perform services for or on its behalf, such as agents or contractors.

The Compliance Program sections on ENTERTAINMENT, GIFTS AND GRATUITIES, CONTRACTING WITH GOVERNMENT ENTITIES AND OFFICIALS, PROHIBITED PAYMENTS, and ACCURATE DISCLOSURES, BOOKS AND RECORDS and the *Guide to Combating Bribery and Corruption* adopt the standards of the FCPA and Bribery Act as the models for SunGard's policy. All SunGard subsidiaries and Employees in every country are governed by these policy standards.

SunGard policy prohibits all forms of bribery regardless of the situation or the recipient, including bribery of a Government Official. No Employee or anyone acting on behalf of the Company or providing services for or on behalf of the Company may offer, give or promise anything of value to a Government Official for the purpose of, or as a reward for, improperly obtaining business, retaining business or for the purpose of, or reward for, improperly securing a financial or other advantage. No Employee or anyone acting on behalf of the Company or providing services for or on behalf of the Company may offer or give anything of value to anyone knowing that all or part of the payment will be directly or indirectly offered, given or promised to a Government Official for a corrupt purpose. There is no exception for bribes of minimal value and even offering or promising a bribe violates SunGard policy.

Definition of Government Official

As used in SunGard's policy, the definition of Government Official includes:

- A person elected or appointed to public office or government position of any kind including legislative, administrative or judicial positions.

- A person acting in an official capacity or exercising a public function for a government, including a state administrative agency, legislature, judicial body, provincial government or municipal government.

- An employee or representative of a state-owned or state-controlled business, enterprise or organization.

- A person acting on behalf of a public international organization such as the United Nations, World Bank or International Monetary Fund.

- Any candidate for political office or official of a political party.

- Any family member, close personal friend, business partner, sexual partner or person in any other type of close personal relationship with any of the above persons.

Entertainment, Gifts, Gratuities, Travel for Government Officials

As stated above, SunGard prohibits bribes regardless of the recipient, but doing business with Government Officials must trigger special sensitivity to business hospitality, promotional activities and to the use of agents or third parties in connection with our business.

Entertainment, gifts, travel, favors and all other forms of hospitality or business courtesies can be interpreted as a form of illegal payment and must conform to strict limits when the recipient is a Government Official as defined above. Many countries prohibit Government Officials from accepting business hospitality and business courtesies, and it may be a crime to even offer such to a Government Official. Even where permitted, most government entities, including state-owned entities, have policies that limit or restrict their employees' ability to accept gifts, meals, travel and other business courtesies and hospitality. Be sure you understand the written policy applicable to the Government Official and comply with it. Even when the Government Official is permitted to accept gifts, meals, travel, etc., SunGard policy standards must be followed. SunGard Employees must follow local law and this Policy regardless of local custom.

It may be permissible under SunGard Policy for an Employee to reimburse or cover the reasonable and bona fide travel, meal and modest business entertainment expenses of a Government Official provided the expense is for the direct purpose of the legitimate promotion of the Company's products or services, or in connection with the execution or performance of a contract with the Government Official or his agency or employer.

Before agreeing to pay any travel expenses of a Government Official, you must consult with the Legal Department or Chief Compliance Officer to determine if the payments are permissible under this Policy and local law.

Any entertainment provided should be moderately priced and in good taste and otherwise comply with this policy. The term "entertainment" describes events such as meals and local golf, parties, plays and concerts. Gifts to Government Officials are not permitted unless they are strictly in accordance with the written policies of the Government Official's employer. Local custom is not a substitute for a written policy. Even where such policies permit gifts, SunGard Policy may be more limiting in what are considered permissible gifts. The most restrictive rule must be followed.

- Never give directly or indirectly cash or cash equivalents such as gift cards or pre-paid debit cards.

- Gifts for Government Officials must be unmistakably inexpensive and infrequent. A one-time gift that costs the equivalent of €20 or US $30 or less is unlikely to raise corruption concerns, but be aware that there is no safe amount.

- Food and flowers are appropriate options provided they are inexpensive and infrequent.

- Other gifts should have a clear business nexus such as SunGard branded items, business books or desk items. Regardless of the cost of the item, consumer electronics and jewelry are not appropriate gifts.

- Gifts should be exchanged publicly, such as in an office setting, or in such a way that an independent person would perceive the exchange as appropriate.

Facilitation Payments

Certain limited "facilitating payments" or "expediting fees" may be permissible, in some places, in order to secure routine governmental action to which the Company is legally entitled. For example, it may be permissible for a nominal payment to be made to secure the timely issuance of a license or expedited processing of a visa. However, the circumstances in which such a payment is legal are very limited. Therefore, before considering or making a facilitating payment, you must contact the Legal Department or the Chief Compliance Officer to determine if the proposed facilitating payment is lawful under all law that applies to the transaction, including local law. In the unlikely event that a facilitation payment is lawful, it must be properly recorded in the Company financial records as a facilitation payment.

Retaining Third Parties to Act for SunGard

Appropriate due diligence must be performed on the third party and specific contract terms must be included in the agreement in order to retain a third party to support or assist our Company. Employees must consult with the Legal Department prior to retaining or hiring any agent, distributor, independent contractor or consultant, or when entering a joint venture or partnership, alliance or other arrangement. The required due diligence and approval process is set out in the Third-Party Retention Procedures for Combating Bribery and Corruption available through the Legal Department, the Compliance Office and available internally on the Compliance and Business Ethics site on KnowHow or on your SunGard business division intranet.

Corruption Warning Signs

In addition to the circumstances described above, you should immediately contact your Supervisor, who should consult with the Legal Department or the Chief Compliance Officer, if any of the following warning signs arise in a Company transaction, activity or project:

- The refusal by any third party to agree to abide by Company anti-bribery policies and procedures.
- Unusual or excessive payment requests, requests for over-invoicing or unusual commissions, requests for payments in a third country, requests for payments to a different party (apparently unrelated to the transaction) or requests for payment in cash or otherwise untraceable funds.
- A request for political or charitable contributions in connection with a purchasing decision or contract renewal or involving a Government Official in any context.
- The discovery of a previously undisclosed affiliation between a third party engaged by the Company and a Government Official.
- Allegations (or charges) of a violation of law against the third party.
- Direction by a Government Official to retain a particular third party or consultant.
- Doing business with or recommending a company owned in part or whole by a Government Official or his or her family.

- Any indication that a third party engaged to work with SunGard is unqualified (and lacks the staff, knowledge or facilities) to perform the services.

- Any indication that a third party is not or cannot maintain adequate financial records in connection with SunGard business.

Violators of this Policy are subject to disciplinary action. Violations of this Policy may also be a violation of law resulting in criminal and civil penalties (including imprisonment) for the individuals involved.

For additional information, guidance and advice, download a copy of the *Guide to Combating Bribery and Corruption* available internally on the Compliance and Business Ethics site on KnowHow or on your SunGard business division intranet, or request a copy from the Legal Department or the Compliance Office.

EXPORT AND TRADE REGULATIONS

Compliance with Trade Regulations

It is SunGard's policy to comply with the laws applicable to the conduct of its business in every jurisdiction where it operates and, in particular, with the requirements of the laws and regulations of the United States and those of other countries regarding export, re-export and import of commodities, technology or software. It is a violation of this policy to export or import any item illegally or to conduct business with a restricted or blocked party or in violation of Untied States trade sanctions.

United States Export Regulations

The United States government maintains strict controls on exports of goods, software and technical information from the United States and re-exports of United States goods, software and information from other countries. Most of the software and technical services sold by SunGard originate in or incorporate United States origin items and are therefore subject to United States export regulations. When SunGard ships, transmits or delivers an item outside the United States, the item is an export. "Items" relevant to SunGard include software or technology, technical design plans, retail software packages, performance specifications and other technical information.

Export laws cover more than just physical shipments. For example, internet and intranet technology transfers, travel across country borders with software or technical specifications, and information shared during visits to the United States by foreign nationals may all involve regulated exports. In addition, some destinations and persons (individuals or groups) are subject to comprehensive export controls, including controls on widely-traded consumer products.

The severity of the rules varies greatly, depending on the nature of the exports, their destinations, the persons to whom the exports are directed and their intended use. The rules also change frequently, often depending on changes in the policies of the United States and its allies toward various countries. The sanctions for violating the export rules, even when the violation is inadvertent, can be severe. Both criminal and civil penalties apply. Because the rules are complex and change frequently, the Company makes a guide available which provides an overview for complying with United States export laws. The guide is available to all employees through the Legal Department and Compliance Office, and is also

available internally on the Compliance and Business Ethics site on KnowHow or on your SunGard business division intranet.

Employees who are likely to encounter export issues on the job should familiarize themselves with applicable export laws. If you are involved with exports, you should obtain a copy of the export guide from the Legal Department or Compliance Office, or from the Compliance and Business Ethics site on KnowHow or your SunGard business division intranet. You should read the guide and be certain that you understand how the export laws apply to your work. Consulting support is available from the Compliance Office.

Supervisors must:

- Require that appropriate licenses or other authorizations are in place for each import or export undertaken by his or her group; and

- Maintain such records of exports and imports as are appropriate under applicable legal requirements.

Boycotts and Trade Embargoes

The United States currently maintains commercial embargoes against a number of countries. As a United States company, SunGard complies with the applicable embargo laws. Other countries also maintain commercial embargoes and consequently, compliance with domestic and international trade sanctions is complex. Because the listed countries and the types of restrictions change frequently, do not conduct business with any entity or person unless you are certain that the proposed business partner is not subject to restrictions or sanctions. Check with the Legal Department or the Chief Compliance Officer if there is any doubt or concern about the legality of doing business with an entity or person or doing business in a particular country. These restrictions and obligations apply whether doing business through SunGard in the United States or through a non-United States SunGard subsidiary.

Prohibited Participation in Unsanctioned Economic Boycotts and Embargoes

The United States prohibits United States citizens, including United States corporations like SunGard, from participating in other nations' economic boycotts or embargoes. The antiboycott laws were adopted to encourage, and in specified cases, require United States firms to refuse to participate in foreign boycotts that the United States does not sanction to prevent United States firms from being used to implement foreign policies of other nations which run counter to United States policy. The Arab League boycott of Israel is the principal foreign economic boycott that United States companies must be concerned with today. The antiboycott laws, however, apply to all boycotts imposed by other countries that are unsanctioned by the United States.

As a United States corporation, SunGard must comply with the antiboycott provisions of the United States. SunGard will not:

- Refuse or agree to refuse to do business with or in Israel or with blacklisted companies.

- Discriminate or agree to discrimination against persons based on race, religion, sex, national origin or nationality.

- Furnish or agree to furnish information about business relationships with or in Israel or with blacklisted companies.

- Furnish or agree to furnish information about the race, religion, sex, or national origin of another person in support of an unsanctioned boycott or embargo.

- Honor, negotiate or implement letters of credit containing prohibited boycott provisions.

Requests to participate or support illegal boycotts may be received in the form of bid invitations, purchase orders, contracts, letters of credit, shipping documents or other forms of communication including oral requests. Receipt of such a request must be reported in a timely manner to the United States government. Report any request to participate in or support an economic boycott not sanctioned by the United States government to the Legal Department or to the Chief Compliance Officer.

For more information on these topics, refer to SunGard's Export Control and Economic Sanctions Compliance Policy which is available internally on KnowHow under Resources, Policies and Guidelines, or on your SunGard business division intranet.

POLITICAL ACTIVITY

Company employees have the right to participate individually in the political process and to make voluntary contributions of their personal resources and non-working time to support federal and state candidates and political parties of their choice. The Company encourages employee involvement in the political process but these activities must not in any way suggest the Company's support or involve the use of the Company's resources.

All Employees and others acting on the Company's behalf must comply with laws that apply to the use of Company resources for political purposes. United States Federal election law and the election law of many U.S. states generally prohibit the use of corporate resources to directly or indirectly support or oppose candidates or political committees. The Company will not make a contribution to support or oppose a political candidate or political committee. No one is permitted to make a contribution on behalf of the Company.

Employees are not allowed to include, directly or indirectly, any political contribution on the Employee's expense account, or in any other way to cause the Company to reimburse the Employee for political contributions. As an example, the cost of tickets to a fund raising event for political functions is considered a political contribution and is not a legitimate Company expense.

The Company does not allow political campaign or partisan political activities at the Company's work place or facilities, and does not permit the use of the Company's resources, including computers, telephones, copiers, email, or employee work time for political campaigning, political fundraising, or other partisan political activities. Employees cannot be paid by the Company for time spent in campaign efforts for a political candidate or party. Similarly, if an Employee runs for elective office, the time spent campaigning or performing the duties of that post must be the Employee's own time, such as after hours, weekends, unpaid leave or vacation.

The Company does not permit employees to distribute campaign literature, solicit campaign contributions, or participate in other political activities during paid working hours. Employees are

prohibited from making, copying or distributing political materials using the Company's equipment or resources, or engaging in other political activities during paid working time.

No employee may use the influence of his or her position to persuade another employee to work for candidate, political committee or other political issue or to make personal contributions to a candidate or political party. Employees will be neither favored nor penalized for their participation in, or abstention from, legal political activities.

Company employees are expected to understand and abide by this policy. If you have any questions about proper political conduct at the work place, you should contact SunGard's Chief Compliance Officer or a member of the SunGard legal department before agreeing to do anything that would involve the Company in political activity at the national, state or local levels.

EQUAL EMPLOYMENT OPPORTUNITY

All applicants and Employees are entitled to equal employment opportunities within the Company. It is the Company's policy to recruit, hire, train, compensate, terminate and otherwise treat individuals without regard to race, color, religion, sex, national origin, age, marital status, sexual orientation, disability, citizenship status, genetic information, Vietnam-era or other veteran status, or any other characteristic protected by law. The Company will make reasonable accommodations for the known physical or mental disabilities of an otherwise qualified applicant or Employee.

Certain of the Company's significant human resources policies are contained in this Compliance Program. See PRIVACY, DISCRIMINATION, SEXUAL AND OTHER DISCRIMINATORY HARASSMENT, ILLEGAL SUBSTANCES AND ALCOHOL, and IMMIGRATION AND TEMPORARY WORK ASSIGNMENTS below. The Company's human resources policies are available internally on KnowHow under Resources, Policies and Guidelines, or on your SunGard business division intranet.

All Employees are expected to act in a manner consistent with the anti-discrimination policy, anti-harassment policy and the Company's other human resources policies. All Employees are expected to refrain from expressing views not supportive of any of these Policies when acting as representatives of the Company.

PRIVACY

The Company is committed to complying with all applicable privacy laws in the conduct of its business. Privacy laws in the United States, European Union ("EU"), Asia and other locations may govern the proper processing and protection of certain personal information, the accuracy of the stated uses of the information processed by the Company and the Company's adherence to its statements about the use of the information. Employees should consult the Legal Department before transferring across national borders or to third parties the following information (particularly with respect to the EU):

- **Personally Identifiable Information or Personal Data.** Defined as data which can be related back to a specific identified individual, directly or indirectly.

- **Sensitive Data.** Generally defined as personal information having particular significance for privacy expectations (e.g., racial/ethnic origin, political activities, trade union membership, religious beliefs, health or medical data, sexual preferences or criminal activities).

Privacy law is a growing and complex area of law in the United States and around the world. In certain circumstances, an individual's consent may be required before some types of personal information may be processed, collected or transferred. Please consult with the Legal Department if you have questions about this Policy or if you require guidance regarding the processing of certain information or data.

Employee Information

In the course of its business operations, the Company will collect and maintain personal information about Company Employees and other staff as outlined in the SunGard Staff Privacy Notice.

For a comprehensive statement of the Company's standard for protection of Employee information, see the SunGard Staff Privacy Notice linked at Appendix C.

Customer Information

In the course of our business, the Company processes, stores and transfers personal data entrusted to us by our customers. The data our customers entrust to us may be personal data of individuals doing business with our customers. The data we receive from our customers will be handled in accordance with our agreement with the customer and the legal requirements applicable to SunGard in performance of our customer's agreement. It is contrary to Company policy to use the data our customer entrusts to us for any purpose other than that encompassed by the agreement or expressly permitted by law.

When a specific law or regulation governs the handling of personal data, including financial data, business leaders in the effected operating units will implement and follow procedures to conform their business operations to the applicable legal requirements.

Any Employee who is uncertain of the legality or ethics surrounding the collection, transfer, processing, disclosure or destruction of personal data pertaining to Company Employees or personal data processed for a customer should contact the Legal Department before taking action.

DISCRIMINATION

SunGard has a long-standing commitment to a work environment that respects the dignity of each individual. Inappropriate workplace behavior and unlawful discrimination or harassment are wholly inconsistent with this commitment. All Employees have the right to work in an environment free from all forms of discrimination and conduct that is harassing, coercive or disruptive, including sexual harassment. The Company prohibits any form of unlawful employee discrimination based on race, color, religion, sex, national origin, age, marital status, sexual orientation, disability, citizenship status, genetic information, Vietnam-era or other veteran status, or any other characteristic protected by law. SunGard will not tolerate improper interference with any Employee's ability to perform his or her expected job duties.

Employees are expected to refrain from making offensive comments, jokes, innuendos or gestures that are based on race, color, religion, sex, national origin, age, marital status, sexual orientation, disability, citizenship status, genetic information, Vietnam-era or other veteran status, or any other characteristic protected by law.

Reporting Discriminatory Conduct

It is the Company's policy to strongly encourage and support the prompt reporting of all incidents of discriminatory conduct. If you believe that you have been subjected to discriminatory conduct, or if you have observed such conduct, SunGard requires you to promptly notify your Supervisor, your Human Resources representative or the Chief Compliance Officer. Any Supervisor who receives a report or otherwise becomes aware of discriminatory conduct must immediately notify Human Resources. If you are uncomfortable for any reason in bringing such a matter to the attention of your Supervisor, or are not satisfied after bringing the matter to his or her attention, you should report the matter directly to your Human Resources representative or the Chief Compliance Officer. Any question about this Policy should also be brought to the attention of your Supervisor, your Human Resources representative or the Chief Compliance Officer.

When a report of discriminatory conduct is made as specified above, the Human Resources Department will promptly undertake an investigation appropriate to the circumstances. The steps to be taken during the investigation cannot be fixed in advance, but will vary depending upon the nature of the allegations. Confidentiality will be maintained throughout the investigative process to the extent practicable and consistent with the Company's need to undertake a full investigation.

Upon completion of the investigation, corrective action will be taken, if appropriate and supported by the facts. Corrective action may include, but is not limited to, oral or written reprimand, referral to formal counseling, financial consequences such as the reduction or elimination of a bonus or the postponement of a raise, disciplinary suspension or probation, or discharge from SunGard.

An individual, who reports incidents that he or she believes in good faith to be violations of this Policy, or who is involved in the investigation of discriminatory conduct, will not be subject to reprisal or retaliation. Retaliation is a serious violation of this Policy and should be reported immediately. The report and investigation of allegations of retaliation will follow the procedures set forth in this Compliance Program. Any person found to have retaliated against an individual for reporting discriminatory conduct or for participating in an investigation of allegations of such conduct will be subject to appropriate disciplinary action.

SEXUAL AND OTHER DISCRIMINATORY HARASSMENT

SunGard Employees have the right to work in an environment that is free from sexual harassment. Sexual harassment in the workplace is unlawful. No Employee, either male or female, should be subjected to unsolicited and unwelcome sexual overtures or conduct. SunGard does not intend to regulate the personal morality of employees, but rather promote a work environment that is free from all forms of discriminatory harassment whether that harassment is because of race, color, religion, sex, national origin, age, marital status, sexual orientation, disability, citizenship status, genetic information, Vietnam-era or other veteran status, or any other characteristic protected by law.

Discriminatory Harassment Prohibited

Discriminatory harassment, including sexual harassment, is unacceptable and will not be tolerated. All Employees are expected to avoid any behavior that could be interpreted or perceived as discriminatory harassment. This Policy applies to all discriminatory harassment occurring in the work environment, whether at the Company or in other work-related settings, and applies regardless of the gender, marital

status or sexual orientation of the individuals involved. This Policy covers all Employees and applicants for employment. This Policy also covers unlawful discriminatory harassment by a non-employee (e.g., clients, family members, suppliers, volunteers, interns, independent contractors, etc.) to the extent that it affects the work environment or interferes with the performance of work. Anyone who believes that he or she has been subjected to sexual or other discriminatory harassment must report the problem using the procedures set forth in this Policy. SunGard will investigate a reported incident to the extent practicable and will take remedial action where appropriate.

Sexual Harassment Defined

For purposes of this Policy, "sexual harassment" means unwelcome sexual advances, requests for sexual favors and other verbal or physical conduct of a sexual or gender-based nature in any of the following situations:

- When submission to such conduct is either explicitly or implicitly made a term or condition of an individual's employment.

- When submission to or rejection of such conduct is used as the basis for employment decisions affecting the individual.

- When such conduct unreasonably interferes with an individual's work performance or creates an intimidating, hostile or offensive working environment.

Here are some examples of what may constitute sexual harassment: threatening or taking adverse employment action, such as discharge or demotion, if sexual favors are not granted; demanding sexual favors in exchange for favorable or preferential treatment; making unwelcome and repeated flirtations, propositions or advances; making unwelcome physical contact; whistling, leering or making improper gestures; making offensive, derogatory or degrading remarks; making unwelcome comments about appearance; telling sexual jokes or using sexually explicit or offensive language; engaging in gender or sex-based pranks; or displaying sexually suggestive objects or pictures in work areas. The above list of examples is not intended to be all inclusive.

Other Discriminatory Harassment Defined

For purposes of this Policy, "other discriminatory harassment" means verbal or physical conduct that denigrates or shows hostility or aversion toward an individual because of his or her race, color, gender, age, religion, national origin, disability, veteran status or any other characteristic protected by law, in any of the following circumstances:

- When the conduct creates an intimidating, hostile, or offensive work environment.

- When the conduct unreasonably interferes with an individual's work performance.

Here are some examples of other discriminatory harassment: using epithets or slurs; mocking, ridiculing or mimicking another's culture, accent, appearance or customs; threatening, intimidating or engaging in hostile or offensive acts based on an individual's race, color, gender, religion, national origin, disability, veteran status or any other characteristic protected by law; or displaying on walls, bulletin boards or elsewhere in the workplace, or circulating in the workplace, written or graphic material that denigrates or

shows hostility toward a person or group because of an individual's race, color, gender, age, religion, national origin, disability, veteran status or any other characteristic protected by law. The above list of examples is not intended to be all inclusive.

Reporting Discriminatory Harassment

It is the Company's policy to strongly encourage and support the prompt reporting of all incidents of sexual or other discriminatory harassment. If you believe that you have been subjected to sexual or other discriminatory harassment, or if you have observed such conduct, SunGard requires you to promptly notify your Supervisor, your Human Resources representative or the Chief Compliance Officer. Any Supervisor who receives a report or otherwise becomes aware of discriminatory harassment must immediately notify Human Resources. If you are uncomfortable for any reason in bringing such a matter to the attention of your Supervisor, or are not satisfied after bringing the matter to his or her attention, you should report the matter directly to your Human Resources representative or the Chief Compliance Officer. Any question about this Policy or potential sexual or other discriminatory harassment also should be brought to the attention of your Supervisor, your Human Resources representative or the Chief Compliance Officer.

When a report of sexual or other discriminatory harassment is received, the Human Resources Department will promptly undertake an investigation appropriate to the circumstances. The steps to be taken during the investigation cannot be fixed in advance, but will vary depending upon the nature of the allegations. Confidentiality will be maintained throughout the investigative process to the extent practicable and consistent with the Company's need to undertake a full investigation.

Upon completion of the investigation, corrective action will be taken, if appropriate and supported by the facts. Corrective action may include, but is not limited to, oral or written reprimand, referral to formal counseling, financial consequences such as the reduction or elimination of a discretionary bonus or the postponement of a raise, disciplinary suspension or probation or discharge from SunGard.

An individual who reports incidents which, in good faith, he or she believes to be violations of this Policy, or who is involved in the investigation of sexual or other discriminatory harassment, will not be subject to reprisal or retaliation. Retaliation is a serious violation of this Policy and should be reported immediately. The report and investigation of allegations of retaliation will follow the procedures set forth in this Policy. Any person found to have retaliated against an individual for reporting sexual or other discriminatory harassment or for participating in an investigation of allegations of such conduct will be subject to appropriate disciplinary action.

Reporting Consensual Relationships

Consensual romantic and/or sexual relationships between Employees may compromise the Company's ability to enforce its policy against sexual harassment or lead to other employment-based claims against the Company. When one party to such a relationship is the Supervisor or Executive Officer or an individual who can otherwise impact the other party's work assignment, compensation, performance review or promotion, the risk to SunGard's ability to enforce its policy against sexual harassment is unacceptably high. The individuals involved in such a consensual relationship must disclose the relationship to a Supervisor **and** the Chief Compliance Officer. All other individuals in consensual relationships must disclose the relationship to Human Resources. Disclosure will allow the Company and the Employees involved to take appropriate steps to protect all parties from unintended work-related

consequences. Such action may include a change in the responsibilities of the individuals involved, or transfer of location within the office, in order to eliminate any existing supervisory relationship and diminish workplace contact.

ILLEGAL SUBSTANCES AND ALCOHOL

The ability to perform one's work is compromised by the illegal use of drugs and/or alcohol. The Company's objective is to keep the workplace free from substance and alcohol abuse and its effects, and the Company will not tolerate the presence of illegal drugs and/or alcohol in the workplace. Employees are prohibited from conducting Company business while under the influence of illegal drugs and/or impaired by the use of alcohol. The Company also will not tolerate the abuse of prescribed drugs by any Employee while on Company premises, engaged in Company business or operating Company equipment. These goals are not only the Company's right, but are the Company's responsibility to its customers and Employees.

The Company will try to achieve a workplace that is entirely free of substance abuse by following the steps below:

- Counseling and assisting Employees with substance abuse problems. For more details on the Company's policy relating to drug and alcohol abuse and the assistance available to Employees, see Human Resources.

- Disciplining Employees who engage in unlawful activities involving drugs and alcohol in the workplace.

Consuming alcohol at a SunGard or customer-sponsored event during or after work hours on Company or customer premises is permitted provided the event has manager approval and proper business decorum is maintained. The safety of guests and Employees should be considered when planning the event.

IMMIGRATION AND TEMPORARY WORK ASSIGNMENTS

SunGard requires that Employees hired for positions or assigned to work outside their home country for any period of time are legally authorized to work in the country in which they are hired or assigned to work. The Company may be subject to civil or criminal penalties if an individual who is not authorized to work in the country is placed on the payroll for a position, performs work or travels on business without a proper visa.

All candidates for positions must present appropriate documentation to verify that they are legally authorized to work under the applicable labor, employment and immigration laws before the Employee's first day of work. In the United States, the Company is required to have Form I-9s for each Employee and will conduct regular internal audits to verify the receipt of such information. Company Supervisors are responsible for assuring that relevant labor, employment and immigration laws are followed. If a potential Employee does not have the correct working papers, consult the Human Resources Department or the Legal Department before an offer of employment is made or the Employee travels on a business assignment. No travel arrangements should be made before appropriate documentation is obtained.

Questions on immigration issues should be referred to the Human Resources Department or to the Legal Department. Questions relating to international assignments should be referred to the International Mobility Team.

APPENDIX A

GLOBAL BUSINESS CONDUCT AND COMPLIANCE PROGRAM

ANNUAL CERTIFICATION

I certify that I have access to and can obtain a copy of SunGard's Global Business Conduct and Compliance Program (the "Compliance Program"), which provides me with clear guidelines for my conduct as a representative of the Company and incorporates a code of ethics for all employees, officers, directors and other representatives of the Company. I understand that the Compliance Program is available to me via the SunGard intranet or from my Human Resources representative.

I understand that I may report possible or suspected violations of the Compliance Program by accessing the AlertLine on-line or by telephone, leaving a voicemail for the Chief Compliance Officer, sending an e-mail to compliance@sungard.com, or using any of the other reporting methods described in the Compliance Program.

I certify that I have read the Compliance Program and fully understand my obligation to comply with all of its terms. I understand that adherence to the Compliance Program is a condition of my employment or engagement with the Company and that failure to adhere to the Compliance Program could result in very serious consequences to me and the Company. I understand that, if I violate the Compliance Program, then I will be subject to appropriate disciplinary and remedial sanctions, up to and including, immediate discharge or termination of my engagement and possible legal action by the Company.

I certify that I will fully comply with all terms of the Compliance Program, and that, as of today's date, I know of no violations of the Compliance Program or the Policies contained therein other than as reported.

I understand that, except for the promise of protection from retaliation made in the Introduction to the Compliance Program, none of the benefits, policies, programs, procedures or statements in the Compliance Program is intended to confer any rights or privileges upon me or entitle me to be or remain an Employee or other representative of the Company. I am aware that the Compliance Program is not a contract and is subject to change at any time, without notice, at the sole discretion of the Company.

Certified:

_____ _____

Date Print Name

_____

Signature

APPENDIX B

GLOBAL BUSINESS CONDUCT AND COMPLIANCE PROGRAM

COMPLIANCE PROGRAM IMPLEMENTATION

Chief Compliance Officer

The Chief Compliance Officer is responsible for implementing and maintaining the Compliance Program, subject to the direction of the Compliance Program Committee and oversight of the Audit Committee. The Chief Compliance Officer's duties include (1) implementing programs to educate and train Employees about the Compliance Program and to effectively communicate the Company's Policies to all Employees, (2) implementing procedures to achieve both effective enforcement of the Compliance Program and efficient reporting by Employees, without fear of retribution, of possible and suspected violations, (3) auditing and investigating possible and suspected violations of the Compliance Program, and (4) implementing disciplinary procedures for Employees who violate the Compliance Program or who fail to report known violations by others. The Chief Compliance Officer will consult with the Compliance Program Committee and Audit Committee as necessary to effectively deal with non-routine reports and investigations and to resolve difficult issues and concerns that arise in connection with the Compliance Program. The Chief Compliance Officer will provide periodic reports to the Audit Committee regarding compliance matters. The Chief Compliance Officer will report to the Chief Legal Officer and will have a dotted-line reporting relationship to the Chair of the Audit Committee.

Compliance Program Committee

The Compliance Program Committee is a management committee that is responsible for reviewing the Chief Compliance Officer's implementation and maintenance of the Compliance Program and interpreting and monitoring the Compliance Program, subject to the oversight of the Audit Committee. The Compliance Program Committee will review the Compliance Program periodically, but no less frequently than annually, and recommend proposed changes to the Audit Committee. The Compliance Program Committee will have at least four (4) members: the Chief Compliance Officer, a senior legal executive designated by the Chief Legal Officer, a senior financial executive designated by the Chief Financial Officer and a senior human resources executive designated by the Vice President Human Resources. A minimum of three (3) members of the Compliance Program Committee are required in order for the Committee to carry out its obligations under this Policy.

Audit Committee

The Audit Committee is the final authority for resolving all disagreements that arise in connection with the Compliance Program. The Chief Compliance Officer and the members of the Compliance Program Committee will be appointed by management, subject to review and approval by the Audit Committee.

SunGard Management

Responsibility for enforcing the Company's Compliance Program extends throughout the Company. If you are a Supervisor, then you are responsible for implementing the Compliance Program for all Employees under your direction. These responsibilities include all of the following:

- Requiring all current and new Employees to participate in ongoing education and training regarding the Compliance Program and the Company's Policies.

- Regularly stressing to all Employees the need for their commitment to the principles of the Compliance Program.

- Requiring that all business activities are conducted in accordance with the highest principles of business ethics and professional excellence.

- Leading by example and maintaining an "open door" policy to handle issues and questions regarding business ethics and legal and regulatory compliance.

- Reinforcing the lines of communication that are available to Employees to make reports and resolve concerns relating to the Compliance Program.

- Reporting matters that you uncover and issues that are reported to you as a Supervisor or Company Official.

- Coordinating and cooperating with the Chief Compliance Officer to determine that all of these responsibilities are effectively and demonstrably accomplished.

Distribution and Acknowledgement of the Compliance Program

Every new Employee will be given access to current copy of the Compliance Program and, as a condition of employment, will be asked to acknowledge receipt and understanding of it within thirty (30) days after hiring. Continuing Employees will be offered an opportunity to review a current copy of the Compliance Program at least annually, and, as a condition of continued employment, will be asked certify to their understanding of the Compliance Program and their agreement to adhere to its terms.

Handling of Reports and Investigations

The Chief Compliance Officer will review all credible, non-routine reports with the Compliance Program Committee. If a credible report involves a Director or Executive Officer of SunGard or involves an allegation of fraud, whether or not material, that involves management or other Employees who have a significant role in SunGard's internal controls, or is otherwise considered material to the Company by the Chief Compliance Officer, Chief Legal Officer, Chief Financial Officer, Vice President Human Resources or majority of the Compliance Program Committee, then the Chief Compliance Officer will promptly communicate the report to the Chair of the Audit Committee.

Any Supervisor or other Company official receiving a credible report of a violation of the Compliance Program must promptly communicate the report to the Chief Compliance Officer. If a Supervisor believes that it is necessary to review or investigate the conduct of one or more Employees, then the Supervisor must seek the advice and approval of the Chief Compliance Officer or the Chief Legal Officer. No one will undertake an internal review or investigation relating to the Compliance Program or the Company's Policies without the approval of the Chief Compliance Officer, the Chief Legal Officer or the Chair of the Audit Committee.

The members of the Compliance Program Committee are authorized on behalf of the Company to conduct internal investigations, seek legal advice and request that inside or outside counsel conduct internal investigations to assist counsel in providing legal advice to the Company. Any such investigation will be conducted on a confidential basis, and the results of any such investigation will be protected from disclosure by the attorney-client privilege as well as any other applicable privilege or protection.

Waivers and Substantive Changes

Any waiver of the provisions of this Program for an Executive Officer or Director must be made by the Board of Directors or a Board Committee. Any substantive changes to this Program will be approved by the Board of Directors. Such waivers and substantive changes will be promptly disclosed as required by law or stock exchange regulation.

APPENDIX C

GLOBAL BUSINESS CONDUCT AND COMPLIANCE PROGRAM

SUNGARD STAFF PRIVACY NOTICE

The SunGard Staff Privacy Notice provides a comprehensive statement of the Company's standard for protection of Employee information. The Staff Privacy Notice is available internally on KnowHow under Resources, Policies and Guidelines, or on your SunGard business division intranet.

APPENDIX D

GLOBAL BUSINESS CONDUCT AND COMPLIANCE PROGRAM

GENERAL DEFINITIONS

- **"Audit Committee"** means the Audit Committee of the Board of Directors of SunGard Data Systems Inc.

- **"Board of Directors"** means the Board of Directors of SunGard Data Systems Inc.

- **"Company"** or **"SunGard**" means SunGard Data Systems Inc., a Delaware corporation, and all subsidiaries and affiliated entities that are more than 50% owned or controlled, directly or indirectly, by SunGard Data Systems Inc.

- **"Compliance Program"** means this Global Business Conduct and Compliance Program, as amended from time to time by the Board of Directors.

- **"Compliance Program Committee"** means the management committee responsible for interpreting and monitoring the Compliance Program.

- **"Director"** means any member of the Board of Directors of SunGard Data Systems Inc. who is not an Employee.

- **"Employee"** means any employee, consultant, volunteer or other agent or representative of the Company including all Executive Officers and including all employees who are members of the Company's Board of Directors.

- **"Executive Officer"** means any person who is considered an executive officer of the Company for federal securities law purposes, as designated by the Board of Directors from time-to-time by resolution.

- **"Policies"** means the Company policies contained in this Compliance Program. Each section of this Compliance Program contains one or more Policies.

- **"Supervisor"** means any supervisor or manager of any Employee.

Other definitions are included in specific policies.