

**SUNGARD DATA SYSTEMS INC.  
GLOBAL BUSINESS CONDUCT AND COMPLIANCE  
PROGRAM FOR THE UNITED KINGDOM**

**TO ASK QUESTIONS AND REPORT POSSIBLE VIOLATIONS:**

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 General Counsel, 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. You are invited to contact SunGard's Chief Compliance Officer 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. The Chief Compliance Officer may be reached directly by calling +484.582.5576 or by e-mail at [johanna.rogers@sungard.com](mailto:johanna.rogers@sungard.com).
3. You may 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).
4. You may call SunGard's Hot Line toll-free at 1-800-381-8372 from anywhere in the world (you may remain anonymous when calling this line). Dial the AT&T USADirect Access Number + [800](tel:800) + 381-8372. Find your AT&T Access Number at <http://www.usa.att.com/traveler/index.jsp>

## Honesty–Integrity–Professional Excellence

### GLOBAL BUSINESS CONDUCT AND COMPLIANCE PROGRAM FOR THE UNITED KINGDOM

(This document is posted at [www.inside.sungard.com](http://www.inside.sungard.com))

**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.**

---

#### TABLE OF CONTENTS

<b>Introduction</b> .....	<b>5</b>
<b>General Principles</b> .....	<b>5</b>
CONSEQUENCES OF VIOLATING THE COMPLIANCE PROGRAM .....	5
GIVING NOTICE OF VIOLATIONS .....	6
PROMISE OF NO RETALIATION .....	7
OPEN DOOR.....	7
EMPLOYEE RESPONSIBILITY .....	7
ETHICAL BUSINESS CONDUCT.....	7
GLOBAL OPERATIONS .....	8
COMPANY RELATIONSHIPS .....	8
<b>Conflict of Interest</b> .....	<b>9</b>
EXAMPLES OF CONFLICTS OF INTEREST .....	10
NOTIFYING THE COMPANY OF CONFLICTS.....	12
REVIEW AND RESOLUTION OF CONFLICTS.....	12
DISQUALIFICATION AND WITHDRAWAL FROM CONFLICT .....	12
<b>Entertainment, Gifts and Gratuities</b> .....	<b>12</b>
OFFERING TO OTHERS.....	13
ACCEPTING FROM OTHERS .....	13
COMMON SENSE GUIDELINES .....	13
PUBLIC OFFICIALS AND GOVERNMENT EMPLOYEES .....	14
<b>Doing Business with Government Entities</b> .....	<b>14</b>
<b>Regulated Entities</b> .....	<b>15</b>
<b>Accurate Public Disclosures, Books and Records</b> .....	<b>15</b>

PROTECTING THE QUALITY AND INTEGRITY OF COMPANY RECORDS .....	15
EXAMPLES OF VIOLATIONS .....	16
SPECIALIZED ROLE OF FINANCIAL PROFESSIONALS .....	16
LEADERSHIP ACCOUNTABILITY AND FINANCIAL INTEGRITY .....	17
<b>Records Retention .....</b>	<b>17</b>
<b>Acquiring Competitive Information .....</b>	<b>17</b>
<b>Company Information.....</b>	<b>18</b>
CONFIDENTIAL AND PROPRIETARY INFORMATION.....	18
EXAMPLES OF CONFIDENTIAL AND PROPRIETARY INFORMATION.....	18
OWNERSHIP OF COMPANY INFORMATION .....	19
CONDITIONS FOR DISCLOSURE OF COMPANY-OWNED INFORMATION .....	19
<b>Company Property and Services.....</b>	<b>19</b>
<b>Company Internet, Network and E-mail.....</b>	<b>20</b>
PROPER USE OF INTERNET, NETWORK AND E-MAIL.....	20
PIRACY, SPAMMING AND OTHER MISUSE .....	21
REFERENCES AND LINKS TO SUNGARD.....	21
MONITORING COMPANY IT RESOURCES INCLUDING E-MAIL .....	21
A SPECIAL NOTE ON THE USE AND RETENTION OF E-MAIL .....	21
<b>Limited Personal Use .....</b>	<b>22</b>
<b>Licensed Software.....</b>	<b>23</b>
<b>Insider Trading.....</b>	<b>24</b>
PROHIBITION ON INSIDER TRADING .....	24
<b>Antitrust and Competition Laws .....</b>	<b>25</b>
AGREEMENTS WITH COMPETITORS .....	25
AGREEMENTS BETWEEN BUYERS AND SELLERS.....	26
OTHER RESTRICTIONS AND ARRANGEMENTS .....	26
ACQUISITION OF COMPETITORS.....	26
<b>Legal Matters and Investigations.....</b>	<b>29</b>
SPECIALIZED ROLE OF LEGAL PROFESSIONALS .....	29
LEGAL REPRESENTATION AND ASSISTANCE WITH LEGAL MATTERS.....	29
RELATIONSHIP WITH OUTSIDE COUNSEL.....	29
LEGAL ACTIONS.....	29
LEGAL COUNSEL FOR SUNGARD EMPLOYEES .....	30
GOVERNMENT INSPECTIONS AND INVESTIGATIONS .....	30
PRESERVING COMPANY DOCUMENTS AND RECORDS .....	31
<b>Illegal Payments.....</b>	<b>31</b>
BRIBERY RED FLAGS.....	32
RETAINING THIRD-PARTIES OUTSIDE THE UNITED STATES .....	33
<b>Export and Trade Regulations .....</b>	<b>33</b>

COMPLIANCE WITH TRADE REGULATIONS .....	33
UNITED STATES EXPORT REGULATIONS .....	33
UNITED STATES BOYCOTTS AND TRADE EMBARGOES .....	34
PROHIBITED PARTICIPATION IN BOYCOTTS AND EMBARGOES .....	34
<b>Political Activity</b> .....	35
<b>Privacy</b> .....	35
EMPLOYEE INFORMATION .....	36
CUSTOMER INFORMTION .....	36
<b>Equal Employment Opportunity</b> .....	37
<b>Discrimination</b> .....	37
REPORTING DISCRIMINATORY CONDUCT .....	38
<b>Sexual and Other Harassment</b> .....	38
HARASSMENT PROHIBITED .....	38
SEXUAL HARASSMENT DEFINED.....	39
OTHER HARASSMENT DEFINED.....	39
CONSENSUAL RELATIONSHIPS.....	40
REPORTING HARASSMENT .....	40
INVESTIGATION OF HARASSMENT CLAIMS .....	40
<b>A Safe and Healthy Workplace</b> .....	40
<b>Illegal Substances and Alcohol</b> .....	41
<b>Immigration</b> .....	41
Appendices	
<b>APPENDIX A</b> , ANNUAL CERTIFICATION FORM...	43
<b>APPENDIX B</b> , COMPLIANCE PROGRAM IMPLEMENTATION .....	44
<b>APPENDIX C</b> , SUNGARD COMMITMENT TO PRIVACY .....	47
<b>APPENDIX D</b> , GENERAL DEFINITIONS.....	52

## **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. This Compliance Program is Company Policy. 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 C 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 stockholders and ourselves by adhering to the highest standards of ethical behavior and by maintaining an environment that is fair, open and honest.

## **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 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.

It is your responsibility to read this document and to clarify any questions you have by contacting either Human Resources or the Chief Compliance Officer. If you fail to adhere to this Compliance Program, you are acting outside the scope of the authority given to you by the Company. It is important that you understand this Compliance Program and your obligations. By following the guidance in this Program, you will be in compliance with the laws referred to in this document.

### ***Consequences of Violating the Compliance Program***

If you fail to follow the policy stated in this Compliance Program, your actions may result in very serious consequences for both you and the Company. Employees violating the Compliance Program may be subject to disciplinary actions. In some cases, this may include immediate dismissal and possible legal action against the individuals involved. Disciplinary actions will follow the existing disciplinary procedures. The Company also may have an obligation to report the matter to appropriate law enforcement or regulatory authorities when the conduct that violates the Compliance Program also is a violation of a law, rule or regulation.

## ***Giving Notice of Violations***

Each Employee is asked to alert the Company to any situation in which the Compliance Program is being violated or is about to be violated. You are strongly encouraged also to notify SunGard of any situation where you feel 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. You may report your concerns if the activity in question has not yet occurred, but is being planned or considered. Furthermore, you are strongly encouraged 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. If you have a reasonable belief you are encouraged to make your concerns known in a reasonable manner. 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:

- In most cases you should discuss your concerns with your Supervisor. Discussions with Supervisors resolve or clarify most issues. . If you are uncomfortable talking with your Supervisor, you are invited to contact any leader in your company's management chain.
- However, if for any reason you are uncomfortable talking with your Supervisor or other leaders in your company's management chain, you are invited to contact Human Resources or any Company official including the Chief Compliance Officer, the General Counsel, the Director of Human Resources or the Chief Financial Officer. You may contact any corporate officer by name or title by calling Company headquarters in Wayne, Pennsylvania at +484.582.2000.
- You are invited to call the Chief Compliance Officer directly at +484.582.5576. You may send an e-mail directly to the Chief Compliance Officer at [johanna.rogers@sungard.com](mailto:johanna.rogers@sungard.com) or [compliance@sungard.com](mailto:compliance@sungard.com).
- You may 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).
- You may call SunGard's Hot Line toll-free at 1-800-381-8372 from anywhere in the world (you may remain anonymous when calling this line). Outside the U.S., dial the AT&T USADirect Access Number + [800](tel:800) + 381-8372. Find your AT&T Access Number at <http://www.usa.att.com/traveler/index.jsp>

If your concern involves accounting or auditing principles or practices, internal accounting controls, 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.

In many sections of this Compliance Program you are invited and encouraged to ask questions, report your concerns or notify the Company. You may follow the reporting guidance here unless specific procedures are set out in the particular section.

All reports and investigations will be handled in a manner consistent with privacy principles. To the extent that a report can remain confidential and still be effectively investigated, the report will be held in confidence. 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 respond to the allegation and explain the circumstances.

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 certainly will be taken into account in determining how to deal with a self-reporting Employee. You are encouraged to use the Compliance Line to seek guidance as to self-reporting a violation.

### ***Promise of No 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. Any suggestion to the contrary is itself a violation. As a serious violation of this Compliance Program, any retaliation or threat of retaliation 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. However, an Employee who participates in a violation, avoids following Company procedure without reasonable excuse or knowingly submits a false or malicious report may be disciplined for that conduct

### ***The Open Door***

Remember, you are strongly encouraged to ask questions about the Company's business practices, and to seek guidance when you are uncertain of the right course of action to follow. All Supervisors and other Company officials are required to maintain an "open door" policy with respect to your questions including questions concerning 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.

### ***Employee Responsibilities***

In addition to understanding the Compliance Program, each Employee is responsible for understanding other 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. You are responsible for being well informed and up-to-date on your legal and ethical responsibilities.

### ***Ethical Business Conduct***

Ethical business conduct means more than complying with the law. It means honesty and integrity in every aspect of the Company's activities even when there is no particular legal or regulatory obligation. Every Employee should be guided by the following general principles:

- SunGard asks its Employees to exemplify, honesty, integrity, and professional excellence. Never accept or tolerate fraud or deception of any kind.

- Apply our standards of honesty, integrity and professional excellence 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. A fundamental tenet of this Policy is openness and transparency.
- Every transaction we engage in must be correctly recorded in the Company's books and records. Never do anything to jeopardize the accuracy and completeness of this information. Take care that you never provide false or incomplete information to a Company Supervisor or Corporate Official. Our information becomes part of the Company's books, records, documents, financial statements and public reports. The Company should have no fear of inspection.
- Accept responsibility for your actions. Learn what you need to know to make informed decisions. Never set aside your good judgment.
- Always use the authority given to you by the Company in the best interest of the Company.

The Company cannot hope to write a policy or provide ethical guidance for every situation you will encounter in your job. Ultimately, we must rely on our own sense of fair play, good judgment and honesty. However, you always have resources to help you in tough situations. You are always invited to talk with your Supervisors, Human Resources or any other Company officials including the Chief Compliance Officer, the General Counsel, and the Chief Financial Officer.

SunGard Employees are unique for their dedication to honesty, integrity and professional excellence. These are traits that define SunGard Employees.

### ***Global Operations***

As a global company, SunGard is committed to complying with the laws of the countries in which it operates or does business. These laws usually differ from country to country, and sometimes are inconsistent or may seem inconsistent. Employees involved in the Company's operations should be aware of their legal responsibilities in the countries in which they conduct business. Consult your local SunGard counsel for advice.

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. Where there appears to be a conflict between the laws of the United States and the local law, you should seek advice from the SunGard General Counsel's office which can be reached at +484.582.2000.

### ***Company 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.

- **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.

- **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.
- **With Investors:** Our investors have entrusted us with their invested dollars. Our responsibility to them is to do our very best to keep their 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.
- **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 natural resources

### **CONFLICT 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. It is the Employee's obligation to make the conflict known. 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 report the conflicts and to eliminate them or handle them properly. When a conflict of interest does occur, the Employee whose objectivity is or appears to be affected, should abstain from acting on behalf of the Company in connection with the situation and report the conflict as directed in this Policy.

### *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 seek guidance concerning 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 of interest. This list is not exclusive.

- **Gratuities and Entertainment.** Accepting and giving extravagant gifts or hosting events is a situation ripe for the appearance of a conflict of interest. Be alert to the appearance you create. How would this look if the gift or event were reported on local news? Avoid giving or receiving gifts that are not in the customary expense range. . (See ENTERTAINMENT, GIFTS AND GRATUITIES for more information.)
- **Improper Payments.** Doing favors and giving money or its equivalent to someone in order to gain or retain business is illegal in virtually every country. Never offer to provide money or a lavish gift to a customer's representative or to someone who works for a prospective customer. (See ENTERTAINMENT, GIFTS AND GRATUITIES AND ILLEGAL PAYMENTS for more information.) Remember, Employees may not use outside persons or entities in connection with the Company's business for the purpose of avoiding this Policy.
- **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 where the interest has not been disclosed to the Employee's Supervisor **and** the Chief Compliance Officer.
  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 by acquiring property or leases in which the Company may be interested.
  6. 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.
- **Conflicts of Duty.** The Company requests that Management Employees 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 notifying your Supervisor. Non-Supervisory Employees are asked to carefully consider 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. This provision applies only to outside employment with business enterprises and not to associations with charitable, religious, civic, educational purposes or other non-profit organizations.
  - **Loans.** 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.
  - **Family and Close 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, it is advisable to disclose any family or close personal relationship among Employees or with customers or suppliers. This does not include every work-related friendship, but would include 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. Here is a list of examples, but there may be other situations that also give rise to an actual or apparent conflict of interest.
    1. An Employee who is related to or in a personal relationship with an applicant for a position at SunGard should disclose the relationship and avoid influencing the hiring decision.
    2. An Employee who has direct supervision of or responsibility for the performance evaluations, business approvals, pay, or benefits of a close relative or other person with whom you have a close personal relationship. Individuals in a family or personal relationship working in the same operating company may be required to take steps so that neither party supervises the other or otherwise has any ability to affect the work assignments, compensation, business approvals, performance review or promotion of the other

**Romantic or Sexual Relationships.** Other members of the work group often reasonably perceive a conflict of interest regardless of facts and assume one party or the other is receiving special benefits when colleagues are romantically involved. In order to protect our Employees from the effects of perceived and actual conflicts of interest and from unwelcome sexual advances and to protect the

Company's interests, it is recommended that parties in a romantic or sexual relationship notify the Company of the situation. Where one of the parties is a Supervisor, the Company has a direct business need to know about the relationship and reporting is strongly encouraged. (See SEXUAL AND OTHER DISCRIMINATORY HARRASSMENT.)

### ***Notifying the Company of Conflicts***

Whenever you become aware of an apparent or actual conflict of interest, whether it involves you or someone else, it can be helpful to all parties involved if you report the situation. Supervisors must notify the Chief Compliance Officer in addition to their management chain.

A SunGard Corporate Director who becomes aware of a conflict of interest should report the matter to the Chair of the Audit Committee, SunGard's Chief Compliance Officer, General Counsel or Chief Financial Officer, in addition to any other reporting deemed appropriate under the circumstances.

### ***Review and Resolution of Conflicts***

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 Company's Compliance Program Committee.

### ***Disqualification and Withdrawal from Conflict***

It is SunGard policy that Employees and Directors in an apparent or actual conflict of interest are disqualified from taking part in or influencing through decision, approval or otherwise, the resolution of an apparent or actual conflict of interest situation involving the financial or other personal interests of that Director or Employee, any member of his or her immediate family, or any company or firm with which that Employee or any member of his or her immediate family is associated. An Employee acting as a director of a non-United States subsidiary may take part in a corporate action involving an apparent or actual conflict of interest of that Employee provided he or she complies with the provisions of the subsidiary's constitutional documents and local law.

## **ENTERTAINMENT, GIFTS AND GRATUITIES**

This section applies to gifts and gratuities offered or received in between SunGard Employees and others in connection with the Company's business. (See ILLEGAL PAYMENTS)

### ***Offering to Others***

The use of Company funds for any unlawful or improper purpose is strictly prohibited. Bribes, kickbacks or other unlawful payments are strictly prohibited. No Employee should ever use a gift or an offer of a gift to obtain or retain business. Favors are considered payments under this policy. Donations to a non-profit institution or to an educational entity must be made publicly and in accordance with the institution or entity's written policies permitting such gifts. Donations must be approved by the President of the applicable SunGard Company and properly recorded in the Company's books and records.

The Company markets its products on the basis of price, quality and service. The Company will not use inappropriate gifts, 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.

Employees may not use outside persons or entities in connection with the Company's business for the purpose of circumventing this Policy. If you receive a request for an improper payment, you should inform your Supervisor or the Chief Compliance Officer immediately.

Gifts of cash or the equivalent of cash are strictly prohibited.

### ***Accepting from Others***

Generally, Employees should not accept 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 accept routine promotional items of nominal value; for example, pens, paperweights, and tee shirts. Employees may never accept cash or the equivalent of cash, no matter the amount.

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, invitations to sporting or cultural events are common business practices and may be accepted provided the expense associated with the event is nominal. Extravagant trips such as to a World Cup or Super Bowl are not appropriate.

Employees who are offered an inappropriate favor, gratuity or payment, should notify the Company immediately. Supervisors should notify their management chain and the Chief Compliance Officer.

### ***Common Sense Guidelines***

The following guidelines 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.
- Never ask for a gift for yourself or for anyone else.
- Never give a gift to an employee of a government customer.
- Business gifts, if appropriate, should be modest in value.
- 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. The term "entertainment" describes events such as meals and charitable or sporting events, including 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.

If you receive a gift that you believe is inappropriate and you cannot politely return it, take other steps to diffuse the problem such as redirecting the gift to a charity or sharing the gift within your office. Be tactful, but let the sender know that future gifts are not appropriate.

### ***Public Officials and Government Employees***

Most countries including the United States make it illegal to give anything of value to a public official or government employee in return for that person's influence, actions or testimony. It is typically illegal to do anything that will benefit a public official or government employee directly or indirectly, if such action results in, or is a reward for, that person's influence, actions or testimony. Violations can result in severe fines and imprisonment. A "**public official**" includes a person who has been nominated for a position as a public official, even if the person does not yet occupy that position.

As a consequence of this ban, SunGard prohibits gift giving or the offer of a gift or a favor to any public official or government employee unless the government employer has public written policies permitting such gifts. Even where such government policies exist, this SunGard Policy limits permissible gifts to those of nominal value. SunGard coffee and tea mugs are examples of gifts of nominal value.

In any event, no Employee may make a gift—including a meal or entertainment—to a public official or employee without express prior permission from a member of the Legal Department. In the United States, Employees may provide public officials with meals and refreshments that are reasonable and directly related to business discussions such as a modest lunch provided during contract negotiations.

The rules of government agencies with which SunGard does business may be more restrictive than the Policy stated here. Local country laws may also further restrict gift giving to public officials and government employees. Be sure you know the rules and regulations that apply to your government agency customer or prospect. If you have doubts you can contact you local SunGard Legal Department counsel or the Chief Compliance Officer for advice concerning gifts, meals or entertainment offer to public officials or government employees.

## **DOING BUSINESS WITH GOVERNMENT ENTITIES**

There are special rules that apply to doing business with a government entity including the United States government. Unless your SunGard Company regularly does business with government customers, consult with the Legal Department or local SunGard counsel concerning proper bidding 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.

## **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 National Association of Securities Dealers, the New York Stock Exchange and the U.K. Financial Services Authority. As a result, these subsidiaries are subject to subject matter specific 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 the Regulated Entity’s compliance policies as well as this Compliance Program. To the extent that the Regulated Entity’s compliance policies are more restrictive, address different business activity or are inconsistent or broader than this Compliance Program, Employees of the firm should adhere to the policies of the regulated entity.

The Supervisors over each Regulated Entity are responsible for setting rules and policies 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 PUBLIC 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. Not only is keeping accurate records required by law, it is good business practice.

### ***Protecting the Quality and Integrity of Company Records***

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. Entities located outside the United States may be also required to maintain books and records in accordance with local rules and regulations. Books and records include invoices, timecards, expense reports, internal or external memoranda, correspondence or other communications, including telephone, e-mail or telegram.

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.

In part, as Employees we can protect the quality and integrity of Company books and records by following these simple rules.

- 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.
- Prepare and sign only accurate and necessary Company records.
- Retain and destroy documents in accordance with the Records Retention Policy.
- Protect financial systems from unauthorized access.

### ***Examples of Violations***

Examples of violations of this Policy include but are not limited to the following:

- Recording a payment as though it was made to one person, when it was actually made to another.
- Submitting expense reports or invoices 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.

### ***Specialized Role of Financial Professionals***

SunGard's financial and accounting professionals have an important role in ensuring that the Company's public financial disclosures, including reports and documents submitted to the United States Securities and Exchange Commission, when applicable, 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. Non-routine matters should be immediately reported up the Financial Management leadership chain.

## ***Leadership 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. These certifications are used in connection with the Company's preparation and filing of disclosures, reports and documents that are submitted to our investors, lenders, the United States Securities and Exchange Commission when applicable, including the annual report on Form 10-K, quarterly reports on Form 10-Q, and the public including information provided to the press and to financial analysts.

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 to disciplinary action and 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. Subject to local law requirements, the Records Retention Policy is in effect and should be consulted before any documents are destroyed. The Records Retention Policy should be modified at the local level to include specific company records not covered in the Records Retention Policy. In addition, the Records Retention Policy must be modified to comply with appropriate local country laws and regulations. Where the local country law retention and the United States law retention periods are different, the longer of the retention periods should be adopted.

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 certain legal proceedings.

The Records Retention Policy is available on-line at [www.inside.sungard.com](http://www.inside.sungard.com) and from the Legal Department.

### **ACQUIRING COMPETITIVE INFORMATION**

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. SunGard adopts the standards set out in the United States Economic Espionage Act of 1996, which makes it a crime to take, use or disclose without authorization the trade secrets of another person or

organization (including competitors of the Company). [The Economic Espionage Act also makes it a crime to use the Company's trade secrets for the benefit of another person or organization.] The Company's policy is that employees should not take, use or disclose without authorization, the trade secrets and confidential information of another person or organization (including competitors of the Company). A trade secret is a piece of highly confidential information which if disclosed would cause real or significant harm to the Company. SunGard Employees should 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.

## **COMPANY INFORMATION**

### ***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 employment, confidential or proprietary information or Company trade secrets may become available to Employees. 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.

Employees also 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.

### ***Examples of Confidential and Proprietary Information***

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).
- Employee medical, personnel and payroll records.
- Information that could help others to 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. Examples of this type of information includes 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.

### ***Ownership of Company Information***

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 Company property and continues to be confidential and may not be disclosed or used for any purpose after the Employee's employment with the Company ends.

### ***Conditions for Disclosure of Company-Owned Information***

All disclosures of material information, other than those contained in normal product announcements and similar marketing materials about SunGard, will be made by corporate press release under the direction of the Company's General Counsel and Chief Financial Officer. It is a violation of this Policy for an Employee to discuss, disclose, use, or release any confidential, proprietary or trade secret information belonging to SunGard or to SunGard's customers both during and after the Employee's association with the Company. Information posted on blogs, in chat rooms, on public message boards or on personal web sites or the equivalent is subject to this restriction. Any Employee releasing confidential or proprietary information about SunGard or a SunGard Customer through other than authorized Company Officers will be considered in violation of this policy and considered for disciplinary action up to and including dismissal.

Employees may use, disclose, or discuss Company owned information only if required by their job responsibilities, as permitted by this Policy, or as required by appropriate court order following prior notice to the Company. It is also a violation of this Policy for an Employee to use any confidential or proprietary information for the Employee's own use or to use such information in any way inconsistent with the Company's interests.

## **COMPANY PROPERTY AND SERVICES**

All Company property is for the Company's benefit. Except as permitted in this section, no Employee may use Company property or services (including Company-owned software) for personal benefit or for the personal benefit 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.

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

Employees should not expect that any business related items created with, stored on, or stored within Company property will remain private. This includes computer files and business e-mail, even if protected with a password.

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.

### **COMPANY INTERNET, NETWORK AND E-MAIL**

Use of the Internet, network and e-mail through the SunGard Network is provided for business purposes. This access represents the use of Company resources for communications, networking, software and storage. In connection with the use of these Company resources, Supervisors and Employees are equally responsible for maintaining workplace dignity and assuring compliance with any global or local regulatory or legal requirements.

#### ***Proper Use of Internet, Network and E-mail***

No Company system including the Internet, e-mail or other communication systems may be used in any way that may be illegal, excessive, disruptive, offensive to others, or considered harmful to the Company. Employees are not allowed to use the Company's Internet, network, e-mail and communication resources to display store or transmit sexually explicit material including images, messages, jokes or cartoons. The prohibition includes transmissions or use of e-mail that 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, 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.

All existing Company Policies including property protection, privacy, misuse of Company resources, information and data security and confidentiality apply to the use of these Company-owned resources, subject to and consistent with local law requirements. Employees are required to act honestly and appropriately, respecting the copyrights, software licensing rules, property rights, and privacy of others.

Except as stated in LIMITED PERSONAL USE, the SunGard network (including the intranet), Internet, e-mail and other communication resources including PDAs, are exclusively for business-related purposes only.

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.

### ***Piracy, Spamming and Other Misuse***

Employees may not download or distribute illegally obtained music, movies, or software. Distributing any virus, attempting to disable a system or network or attempting to defeat network security is strictly prohibited. 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.

### ***References and Links to SunGard***

Except where sponsored by SunGard Global Marketing, Employees are prohibited from creating hot links or other linkage between any web site, including a personal web site, blog or similar online presence, with which the Employee may be affiliated, and a home page created by or for the Company or any of its businesses or affiliates. Employees may not include any mention of the Company, its businesses or affiliates on any commercial web site, including a personal web site or similar online presence, with which the Employee may be affiliated. Where a reference to SunGard, such as in an Employee’s e-mail address, work address, or work telephone number, appears in connection with the Employee’s participation in a charitable or community event, the reference to SunGard must reflect well on the Company, be in good taste and be in compliance with all Company Policies.

### ***Monitoring Company IT Resources Including E-mail***

SunGard recognizes that Employees have a general right to privacy in the workplace, which includes a right to privacy in their personal mail and personal e-mail that is clearly marked “private”. The Company will not inspect personal e-mails marked as private sent or received by employees. However, subject to local law requirements, the Company reserves the right to monitor and inspect network or Internet usage and business e-mail. Subject to local law requirements, Supervisors may review Internet activity, network use and business e-mails to confirm compliance with this Policy.

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 may be grounds for immediate termination.

For more information on technical systems and resources Employees can refer to SunGard’s IS Security Policy and the IT Policy which are available at [www.inside.sungard.com](http://www.inside.sungard.com).

### ***A Special Note on the Use and Retention of E-mail***

Any business 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. All business 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. Business e-mail is fully discoverable in litigation and other proceedings to the same extent as other written business related communications. Therefore, any business e-mail may be subject to monitoring, search or interception at any time, with or without notice to the sender or recipient, subject to compliance with applicable laws.

Accordingly, when preparing business 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.

In the same way that a written letter or report is subject to the Records Retention Policy, a business e-mail once sent or received is also subject to the Records Retention Policy (available to Employees at [www.inside.SunGard.com](http://www.inside.SunGard.com)). In the United States, e-mail is managed by its content, not its format. In some countries outside the United States e-mail is managed by its format regardless of its content. In the United States and where permitted by law, the corporate standard for retention of business-related e-mail is six months after the date it is sent or received (except Regulated Entities which must keep e-mails for longer periods). If you have a business reason to keep the e-mail communication longer than six months, you must take steps to retain it in accordance with the Records Retention Policy and in a manner best suited for its retrieval. As an example, if you need to retain an e-mail relating to an on-going contract, you may keep the e-mail in a specially-designated folder, directory or e-mail file. In jurisdictions outside the United States, you must preserve e-mails for the proscribed period under local record retention standards. Like other forms of records, and regardless of retention requirements, e-mail pertaining to pending audits or judicial or public disclosure proceedings must not be destroyed until the issue is resolved. (See RECORDS RETENTION)

### **LIMITED PERSONAL USE**

Certain activities 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 business, you should speak to your Supervisor before using Company property or services for matters outside of your job responsibilities.

The Company realizes that sometimes there is little separation between personal time and Company time. Even though Company Internet connection, e-mail, telephones and copy and fax equipment are intended for business purposes, the Company recognizes that the occasional personal use of these assets will accommodate legitimate personal needs. Therefore, SunGard permits the occasional and limited use of these specific company assets by SunGard Employees under the following conditions:

- To permit the necessary monitoring of Company systems, Employees who wish to take advantage of this offer will be required to give individual written consent to the Company's monitoring.
- All personal use must comply with applicable law and with Company policies.
- Personal use must 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 other than SunGard's business interests.

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

When Employees are permitted personal use of Company systems such as e-mail, there is the potential for unintended intrusion into personal information. Personal items should be clearly marked as personal.

Subject to local law requirements the Company has an obligation to access and inspect all electronic systems and physical property belonging to it to ensure compliance with the Company's policies, in order to maintain workplace dignity, and to ensure compliance with global or local regulatory or legal requirements.

For more details on the Company's policy relating to company property including e-mail, see the sections on USE OF COMPANY INTERNET, NETWORK AND E-MAIL and LICENSED SOFTWARE.

### **LICENSED SOFTWARE**

Most computer software is protected by copyright laws and contractual restrictions that safeguard the software manufacturer's investment in creating the software. As a software manufacturer itself, 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.

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. Copies of software may not be made without appropriate licenses being obtained.
- Subject to local laws, employees may make and maintain one copy of any third party software program strictly if it is necessary for backup purposes. The backup copy should be stored on alternate media and kept separate from the computer itself.
- Employees may not make any copies of software manuals. Requests for additional software manuals should be made to the Employee's Supervisor or office manager.
- Employees should use third party software only in the manner specified in the supplier's manual and license agreement. No trademark or copyright notices on any third party software should be changed or deleted.
- Employees should be particularly careful in sharing software, downloading software from the Internet, and opening e-mails due to technical concerns such as computer viruses.

It is extremely important for all Employees to follow these procedures. Improper copying or use of computer software can result in disciplinary action against the Employee and 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.

## **INSIDER TRADING**

Under the securities laws of most countries including the law of the United States, corporate Insiders cannot trade in their company's stock on the basis of non-public material information, nor can they "tip" material information to others who use it to trade in the public company securities. These laws are designed to ensure that all investors are on an equal footing and are relying upon the same information in making their investment decisions. Under certain circumstances, anyone who has knowledge of non-public material information may be considered an Insider even if they are not an employee by the issuer of the security.

SunGard Employees must comply with insider trading law in any jurisdiction applicable to the purchase or sale of securities and with this Policy. The purpose of this section is to assist Employees in fully complying with applicable securities laws and with this Policy.

### ***Definitions***

- **"Insider"** means all directors, executive officers, other employees, and all other persons who have knowledge of or access to non-public material information regarding a public company, and their immediate family who share the same household.
- **"Material Information"** means any information that might influence a reasonable investor's decision to buy, sell, and exercise or hold any public company securities, or that might otherwise affect the price of any public company securities. Examples of material information include monthly and quarterly revenues and earnings, the gain or loss of an important customer, the completion or discontinuance of an important product, a significant competitive development, a possible or pending acquisition, or an important change in management.
- **"Securities"** means any publicly-traded stock, bonds or other securities, and any options to purchase any publicly-traded stock, bonds or other securities. With respect to SunGard, this includes its publicly traded debt instruments (will we have such?).

### ***Prohibition on Insider Trading***

SunGard employees are not permitted to trade on inside information. We are often in a position to learn information from our customers and suppliers. If you become an Insider, or receive a tip from an Insider, it is Company policy that you are prohibited from buying, selling or otherwise trading, or applying for or procuring another person to apply for, buy or sell, in any public company securities, at any time while you have knowledge of non-public material information and for a period of one full business day after any material information becomes publicly available. The one-day restriction allows a reasonable period for the market to react to announced information.

Furthermore, whenever you have knowledge of non-public material information concerning a public company, you are prohibited from tipping that information to family members, friends or anyone else who might use the information to trade in any securities of the public company.

These restrictions apply whether or not the disclosure would be intended to influence trading in any public company securities.

In order to avoid the appearance of impropriety and the risk of subsequent challenge, all of the above trading restrictions apply even if the proposed trade would, in fact, be based upon matters independent of the non-public material information known to the person involved. However, in certain cases the above restrictions may be lifted in instances where **full prior disclosure of the trade** is given and it is clear that no unlawful act has taken place.

## **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 is likely to be prosecuted. Care also should be taken during trade association meetings to avoid pricing discussions. Given the very 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 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 the Company's Legal Department.

A violation of these guidelines is almost always illegal. In the UK, a violation is committed only if an individual acts dishonestly. However, 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 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.

### ***Acquisition of Competitors***

When the parties to an acquisition are competitors, 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 & 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 very 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 and its Employees have the right to be represented by legal counsel at all times when questioned by government/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 although the Company cannot guarantee that this will be granted by the investigating entity.

You should not engage in discussions or proceedings with internal auditors, private investigators or lawyers representing the commercial interests of private parties or other entities without Company counsel present or involved.

### ***Legal Counsel for SunGard Employees***

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.

### ***Government Inspections and Investigations***

Sometimes it is difficult to tell when a routine government audit or inspection becomes an investigation. In addition, government investigation will vary depending on the country concerned. You should consult with your local SunGard counsel, the Legal Department or the Chief Compliance Officer to better understand the nature and implications of any government activities and for advice on the best way to proceed.

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 or any document requesting or compelling work-related information.

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 although the Company cannot guarantee that this request will be granted by the investigating entity. If you are asked for information about SunGard, the Company would like to be notified before the interview and to be present at the interview. Contact your local SunGard counsel or the Corporate Legal Department at +484.582.2000 if you receive a request for information in any form.

If you are subpoenaed or otherwise legally compelled to provide testimony, you must comply.

## ***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)

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. In the United States 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.

## **ILLEGAL PAYMENTS**

Governments and multi-national organizations around the globe have enacted laws and published conventions condemning and outlawing corrupt payments (bribes) in government business. For United States companies, the United States Foreign Corrupt Practices Act ("FCPA") makes it a federal crime to offer, give or promise anything of value to a non-United States ("foreign") official, a foreign political party or party official, or a candidate for foreign political office, in any case for the purpose of obtaining business or securing any improper advantage. There is no exception for gifts of minimal value, and even offering the gift (as opposed to delivering it) may be a violation of the FCPA. (Corrupt payments to U.S. government officials are also prohibited but under a different United States law.)

The FCPA's prohibitions apply to non-United States subsidiaries of the Company. Further, non-United States nationals employed by SunGard acting outside the United States can create criminal liability for SunGard if their actions violate the FCPA.

**"Foreign officials"** under the FCPA means non-United States nationals and includes:

- Persons acting in an official capacity for a foreign government, including a foreign state agency, enterprise or organization.

- Persons acting on behalf of a public international organization such as the United Nations, World Bank or International Monetary Fund.
- Employees of businesses owned by foreign governments or agencies.
- Any candidate for foreign political office or official of a foreign political party.
- Any relatives or close family or household members of the above foreign officials.

It is the Company's policy that no Employee, agent or partner acting in connection with Company business may offer or give anything of value to a foreign official, foreign political party or party official, or candidate for foreign political office foreign official or to a third party, knowing that all or part of the gift, favor or payment will be directly or indirectly offered, given or promised for any prohibited purpose.

The term "facilitating payments" may be familiar and some people assume that facilitating payments are permissible. This assumption is almost always wrong. For a facilitating payment to be permissible under the FCPA, the payment must be lawful in the country where it is received. Virtually every country outlaws these payments and considers them bribes. If you are asked for a facilitating payment or if you consider offering a facilitating payment, you must consult with to assess the legality of the proposed payment. In the unusual situation where a payment is permitted, it is the Company president's obligation to ensure that the payment is properly recorded.

It may also be permissible under the FCPA and local law for an Employee to reimburse or cover the reasonable and bona fide travel, meal and business entertainment expenses of a foreign official related to promotion of the Company's products or services, or in connection with the execution or performance of a contract with the foreign official's government or agency. Before agreeing to pay any expenses of a foreign official, you should consult with local SunGard legal counsel, the Legal Department or the Chief Compliance Officer to determine if the payments are permissible under the FCPA and local law.

Cash payments and extravagant gifts to foreign officials or their relatives should never be made.

### ***Bribery Red Flags***

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 conditions or "red flags" exists in a Company transaction, activity or project:

- The refusal by an agent or other party to agree to abide by Company anti-bribery policies and procedures.
- The making by an agent or other party of unusual or excessive payment requests, requests for over-invoicing or unusual commissions, requests for payments in a third country, requests for payments to a third party (apparently unrelated to the transaction), or requests in cash or otherwise untraceable funds.
- A request for political or charitable contributions.
- The existence of an undisclosed government affiliation between an agent or partner and a foreign official.

- Allegations (or charges) of a violation of law against the foreign agent or partner.
- Direction by a foreign official for an agent, partner or employee to retain a particular agent or consultant for the Company.
- The ownership of a company in part or whole by the foreign official or his or her family.
- The appearance that an agent or partner is unqualified (and lacks the staff) to perform the services.
- The failure of an agent or partner to have adequate financial record keeping practices.

Violators of this Policy are subject to disciplinary action as well as criminal and civil penalties (including imprisonment) for violations of the law. The Company is also subject to criminal and civil penalties.

The FCPA also mandates that companies keep accurate books and records. For more information on this aspect of the FCPA, see **ACCURATE PUBLIC DISCLOSURES, BOOKS AND RECORDS** in this Policy.

### ***Retaining Third Parties Outside the United States***

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 with respect to business outside the United States. 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 outside the United States.

## **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.

### ***United States Export Regulations***

The United States government maintains strict controls on exports of goods and technical information from the United States, and re-exports of United States goods 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 visits to the United States by foreign nationals are 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 and their ultimate destinations. 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 has prepared a handbook for complying with export laws. The handbook, entitled United States Export Administration Regulations, is available to all employees through the Legal Department.

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 request a copy of the export handbook. You should read the handbook and be certain that you understand how the export laws apply to your work.

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.

### ***United States Boycotts and Trade Embargoes***

The United States currently maintains commercial embargoes against a number of countries. As a United States public company, SunGard complies with the applicable embargo laws. Because the listed countries and the types of restrictions change frequently, check with the Legal Department or the Chief Compliance Officer if there is any doubt or concern about doing business with a particular country through SunGard in the United States or through a non-United States SunGard subsidiary.

### ***Prohibited Participation in Boycotts and Embargoes***

Since the mid-1970s the United States has prohibited U.S. citizens, including United States corporations like SunGard, from participating in other nation's economic boycotts or embargoes. The Antiboycott laws were adopted to encourage, and in specified cases, require U.S. firms to refuse to participate in foreign boycotts that the United States does not sanction to prevent U.S. firms from being used to implement foreign policies of other nations which run counter to U.S. policy. The Arab League boycott of Israel is the principal foreign economic boycott that U.S. companies must be concerned with today. The Antiboycott laws, however, apply to all boycotts imposed by foreign 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. 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.

### **POLITICAL ACTIVITY**

National and state laws typically restrict the use of corporate assets in connection with elections. United States law prohibits certain payments and severely restricts other types of political contributions.

It is SunGard Policy to prohibit all Company contributions in connection with any election for national or local office. No Executive Officer or Employee may make a political contribution on behalf of the Company.

It is against Company policy, and also may be illegal, for any Employee 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. In general, the cost of fund-raising tickets for political functions is considered a political contribution. Therefore, including the cost of any such fund-raising dinner on an expense account, even if business is discussed, is prohibited.

Use of Employee work time in a campaign also is considered the equivalent of a contribution by the Company. Therefore, 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.

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

The political process has become highly regulated. If you have questions about proper political conduct, you should consult the Company's Legal Department before agreeing to do anything that could seem to involve the Company in political activity at the national, state or local levels.

### **PRIVACY**

Privacy law is a growing and complex area of law in the United States and around the world. In certain circumstances, an Employee's consent may be required before some types of 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.

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") Member States, Asia, and

other countries 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):

### ***Employee Information***

In the course of its business operations, the Company will collect and maintain personal information about Company Employees such as information that relates to employment history, compensation, job performance, medical information and benefit information. Because the Company has operations in multiple countries, Employees acknowledge that information about Company Employees will, in accordance with the requirements of national laws, cross country borders in order to facilitate the necessary and orderly operation of business.

The Company understands the sensitive nature of personal information and commits to the following:

- Employees will be advised of the purpose for collecting personal data unless the reason for collecting the data is apparent based on the facts and circumstances. When legally required, an Employee's consent will be required before personal data is collected.
- Personal data will be used only for the purpose for which it was collected.
- Information about Company Employees will be protected from unauthorized disclosure wherever it is collected, processed or stored.
- Only Company Employees whose job responsibilities require access will be allowed access to personal information.
- Where possible sickness and injury records will be kept separately from absence and accident records, and information will only be disclosed about an identifiable employee where there is a legal obligation to disclose, or the employee has given their consent for the information to be disclosed.
- Information about employees' health will be collected and retained in accordance with local laws.
- When the data is no longer required and can legally be destroyed, the Company will destroy personal data in a responsible manner.

Personal data will not be released outside the Company except where the Company is required by government agency regulation, law, court order or decree, for the purpose of verifying employment, or with the permission of the Employee.

For a comprehensive statement of the Company's standard for protection of Employee information, see Appendix C.

### ***Customer Information***

As a global company, we must be prepared to comply with the legal and regulatory obligations applicable to the services and products we provide. Our obligation extends to compliance with

numerous laws concerning the protection of non-public personal financial information and health information, for example, the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act.

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 customer. The data we receive from our customers will be handled in accordance with our agreement with the customer and the legal requirements applicable to the scope 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.

### **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 or belief, sex, national origin, age, marital status, sexual orientation, disability, citizenship status, 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 HARASSMENT, ILLEGAL SUBSTANCES AND ALCOHOL, and IMMIGRATION below. Employees can read all of the Company's human resources policies at HR Online ([www.inside.sungard.com](http://www.inside.sungard.com)). Employees should refer to **HR Online** for further guidance.

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.

### **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 is 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 or belief, sex, national origin, age, marital status, sexual orientation, disability, citizenship status, 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, 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, Human Resources or the Chief Compliance Officer. Any Supervisor who receives a report 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 Human Resources or the Chief Compliance Officer. Any question about this Policy should also be brought to the attention of your Supervisor, Human Resources 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 as may be appropriate under 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 intent to undertake a full investigation.

Upon completion of the investigation, corrective action will be taken, if appropriate and supported by the facts. Subject to local law, corrective action may include, but is not limited to, oral or written reprimand, referral to formal counseling, disciplinary suspension or probation, or dismissal 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 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 harassment whether that harassment is because of race, color, religion or belief, sex, national origin, age, marital status, sexual orientation, disability, citizenship status, veteran status, or any other characteristic protected by law.

### ***Harassment Prohibited***

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 harassment. This Policy applies to all 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 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 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 dismissal 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 Harassment Defined***

For purposes of this Policy, “other 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 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.

### ***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 of the other party, a senior-level Employee, or 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 extremely high. The Employees involved in the consensual relationship are strongly encouraged to disclose the relationship. 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, to eliminate any existing supervisory relationship and diminish workplace contact.

### ***Reporting Harassment***

It is the Company's policy to strongly encourage and support the prompt reporting of all incidents of sexual or other harassment. If you believe that you have been subjected to sexual or other harassment, or if you have observed such conduct, SunGard strongly encourages you to promptly notify your Supervisor, Human Resources or the Chief Compliance Officer. Any Supervisor who receives a report of 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 or the Chief Compliance Officer. Any question about this Policy or potential sexual or other harassment also should be brought to the attention of your Supervisor, Human Resources or the Chief Compliance Officer.

### ***Investigation of Harassment Claims***

When a report of sexual or other harassment is received, Human Resources will promptly undertake an investigation as may be appropriate under 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 intent 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, disciplinary suspension or probation, or dismissal from SunGard.

Anyone, 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 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 harassment, or for participating in an investigation of allegations of such conduct, may expect the Company to impose the most severe disciplinary action available and consistent with the law.

## **A SAFE AND HEALTHY WORKPLACE**

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. The unauthorized possession of weapons or other dangerous devices in Company controlled or occupied premises or at any customer location is strictly prohibited. Anyone violating this Policy should expect the Company to exercise its available disciplinary options.

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.

### **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 HR Online.
- 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**

SunGard requires that Employees hired for positions are legally authorized to work in the country in which they are hired. The Company may be subject to civil or criminal penalties if an individual who is not authorized to work in the country in which they are hired is placed on the payroll for a position.

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. This should be done in advance of 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. In other countries Company Supervisors are responsible for assuring that local laws are followed. If a potential Employee does not have the correct working papers, you should consult Human Resources or the Legal Department before an offer of employment is made.

Questions on labor, employment or immigration issues in hiring should be referred to Human Resources or to the Legal Department.

Except for the promise of no retaliation, none of the benefits, policies, programs, 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 prior notice, at the sole discretion of the Board of Directors. Employees will be given prompt notice when substantive changes to the Compliance Program are approved by the Board of Directors.

## APPENDIX A

### GLOBAL BUSINESS CONDUCT AND COMPLIANCE PROGRAM

#### ANNUAL ACKNOWLEDGEMENT

I acknowledge that I have access to 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 a current version of the Compliance Program is available to me via the SunGard intranet or from Human Resources.

- I understand that I am permitted and encouraged to ask questions and to notify the Company of possible or suspected violations of the Compliance Program by contacting my Supervisor, any leader in my company's management chain, Human Resources or any other Company official including the Chief Compliance Officer, the General Counsel, the Director of Human Resources or the Chief Financial Officer. I understand that I am encouraged to contact any corporate officer by name or title by calling Company headquarters in the United States at +484.582.2000 or by e-mail.
- I understand that I can contact SunGard's Chief Compliance Officer 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 I may have. The Chief Compliance Officer may be reached directly by calling +484.582.5576 or by e-mail at [johanna.rogers@sungard.com](mailto:johanna.rogers@sungard.com).
- I understand that I may call SunGard's Hot Line toll-free at 1-800-381-8372 from anywhere in the world (I may remain anonymous when calling this line). Dial the AT&T USADirect Access Number + [800](tel:+18003818372) + 381-8372. Find your AT&T Access Number at <http://www.usa.att.com/traveler/index.jsp>.
- I understand that I may 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).

I have read the Compliance Program and fully understand that it is a Company policy and that I am expected to comply with all of its terms. I understand that failure to adhere to the Compliance Program may result in very serious consequences to me and the Company. I understand that, if I fail to follow the Compliance Program, I may be subject to appropriate disciplinary action. If my actions warrant, I may be subject to immediate dismissal and possible legal action by the Company. In any disciplinary action, the Company will have regard to its existing disciplinary procedures.

I am aware that the Compliance Program is not a contract and is subject to change at any time, without prior notice, at the sole discretion of the Board of Directors.

#### **Acknowledged:**

\_\_\_\_\_

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 General Counsel 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 members: the Chief Compliance Officer, a senior legal executive designated by the General Counsel, 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 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:

- Setting and maintaining an ethical "tone at the top" of the organization.

- 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 Compliance Program

Every new Employee will be given a current copy of the Compliance Program and will be asked to acknowledge receipt and understanding of it within 30 days after hiring. Continuing Employees will be given a current copy of the Compliance Program at least annually, and will be asked to acknowledge receipt and understanding of it and adherence to it by signing the attached Certification.

#### 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, General Counsel, 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 General Counsel. 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 General Counsel 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

### SUNGARD COMMITMENT TO PRIVACY

#### TWELVE PRINCIPLES OF PRIVACY

##### PRINCIPLE 1: PURPOSE OF COLLECTION OF PERSONAL INFORMATION.

Personal information will not be collected unless:

1. The information is collected for a lawful purpose connected with a function or activity of the Company; and
2. The collection of the information is necessary for that purpose.

##### PRINCIPLE 2: Source of personal information.

When the Company collects personal information, the Company will:

1. Collect the information directly from the individual concerned, except where the information is publicly available information; or
  - a. the individual concerned authorizes collection of the information from someone else; or
  - b. non-compliance would not prejudice the interests of the individual concerned.
2. The Company will adhere to this standard unless non-compliance is necessary for;
  - a. the prevention, detection, investigation, prosecution, and punishment of offences in cooperation with law enforcement officials; or
  - b. the enforcement of a law imposing a pecuniary penalty; or
  - c. the protection of the public revenue; or
  - d. the orderly conduct of proceedings before any court or tribunal of the jurisdiction where the subject resides.
3. When the Company collects information, that the information;
  - a. will not be used in a form in which the individual concerned is identified; or
  - b. will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

**PRINCIPLE 3: Collection of information from subject.**

1. Where the Company collects personal information directly from the individual concerned, the Company will take such steps reasonable to ensure that the individual concerned is aware of the following.
  - a. The fact that the information is being collected.
  - b. The purpose for which the information is being collected.
  - c. The intended recipients of the information.
  - d. If the collection of the information is authorised or required by or under law.
  - e. The particular law by or under which the collection of the information is authorised or required.
  - f. If the supply of the information by that individual is voluntary or mandatory.
  - g. The consequences (if any) for that individual if all or any part of the requested information is not provided.
  - h. The rights of access to, and correction of, personal information as provided by these principles.
2. The commitment in paragraph 1 will be taken before the information is collected or, if that is not practicable, as soon as practicable after the information is collected, unless one of the following conditions apply.
  - a. The Company has taken those steps in relation to the collection, from that individual, of the same information or information of the same kind, on a recent previous occasion.
  - b. The information will not be used in a form in which the individual concerned is identified.
  - c. The information will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

**PRINCIPLE 4: Manner of collection of personal information.**

Personal information will not be collected by unlawful means, or by means that, in the circumstances of the case, are unfair; or intrude to an unreasonable extent upon the personal affairs of the individual concerned.

PRINCIPLE 5: Storage and security of personal information.

1. The Company will ensure that information is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss; access, use, modification or disclosure and other misuse.
2. If it is necessary to give the information to a third party in connection with the provision of a service to the Company, everything reasonably within the power of the Company is will be done to prevent unauthorised use or unauthorised disclosure of the information.

PRINCIPLE 6: Access to personal information.

Where a Company holds personal information in such a way that it can be readily be retrieved, the individual concerned will be entitled to obtain confirmation of whether or not the Company holds such personal information and to have access to that information.

PRINCIPLE 7: Correction of personal information.

1. Where the Company holds personal information, the individual concerned will be entitled to request correction of the information and the correction will be made unless for some lawful reason, Company is not willing to change the information in accordance with a request by the individual. In such case the Company, if requested by the individual concerned, will take such steps reasonable in the circumstances to attach to the information, in such a manner that it will always be read with any statement provided by that individual of the correction sought.
2. The Company will, if requested by the individual or on its own initiative, take such steps to correct that information as are reasonable to ensure that, having regard to the purposes for which the information may lawfully be used, the information is accurate, up to date, complete and not misleading.
3. Where a Company receives a request under paragraph (1) of this principle, the Company will inform the individual concerned of the action taken as a result of the request.

PRINCIPLE 8: Accuracy of personal information to be checked before use.

The Company will not use information about an individual without taking reasonable steps to verify that the information is accurate, up to date, complete, relevant, and not misleading.

PRINCIPLE 9: The Company will not keep personal information for longer than necessary.

The Company will not keep the information collected for longer than is required for the purposes for which the information may lawfully be used.

**PRINCIPLE 10: Limits on use of personal information.**

Company will not use the information for any purpose other than the purpose for which it was collected unless one of the following applies.

1. The source of the information is a publicly available.
2. The other purpose is authorised by the individual concerned.
3. The non-compliance is necessary:
  - a. to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or
  - b. for the enforcement of a law imposing a pecuniary penalty; or
  - c. for the protection of the public revenue; or
  - d. for the conduct of proceedings before any Court or Tribunal (being proceedings that have been commenced or are reasonably in contemplation).
4. The use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to:
  - a. public health or public safety; or
  - b. the life or health of the individual concerned or another individual; or
  - c. that the purpose for which the information is used is directly related to the purpose for which the information was obtained.
5. The information is used:
  - a. in a form in which the individual concerned is not identified; or
  - b. for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

**PRINCIPLE 11: Limits on disclosure of personal information.**

A Company that holds personal information will not disclose the information to a third party unless one of the following is met.

1. The disclosure is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained.
2. The source of the information is a publicly available.
3. The disclosure is to the individual concerned.
4. The disclosure is authorised by the individual concerned.

5. The disclosure is necessary: for the prevention, detection, investigation, prosecution, and punishment of offences in cooperation with law enforcement officials; or
  - a. for the enforcement of a law imposing a pecuniary penalty; or
  - b. for the protection of the public revenue; or
  - c. for the orderly conduct of proceedings before any court or tribunal of the jurisdiction where the subject resides.
6. The disclosure of the information is necessary to prevent or lessen a serious and imminent threat to public health, public safety, the life or health of the individual concerned or another individual.
7. The disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern.
8. The information is to be used in a form in which the individual concerned is not identified or is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned

**PRINCIPLE 12: Unique identifiers.**

1. The Company will not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable the Company to carry out any one or more of its functions efficiently.
2. The Company will not assign to an individual a unique identifier that, the Company's knowledge, has been assigned to that individual by another agency, unless the use of the identifier benefits the individual
3. The Company will take all reasonable steps to ensure that unique identifiers are assigned only to individuals whose identity is clearly established.

## 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. The Committee is composed of the following SunGard officers: the Chief Compliance Officer, the Chief Financial Officer, the Director of Human Resources and the General Counsel
- “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.