

Table of Contents

1. Introduction	2
2. Compliance with Laws	2
3. Confidential Information	2
4. Conflict of Interest	4
5. Employee Appearance	5
6. Employee Communication	6
7. Employment References	6
8. Employee Conduct	7
9. Guidelines for Appropriate Conduct	7
10. Employee/Customer Relations	8
11. Insider Trading	9
12. Internet Access Policy	10
13. No Expectation of Privacy Policy	11
14. Legally Sensitive Issues	11
15. Media Relations	12
16. Outside Employment/Activity	12
17. Protection and Use of Syntel's Assets	12
18. Solicitation	13
19. Bribery	13
20. Smoking & consumption of Tobacco products	13
21. Drinking and Substance Abuse	13
22. Distracted Driving	13

1. Introduction

Our purpose and values define our approach to the way we work in Syntel. Our values govern our performance and serves as a foundation while achieving Syntel's goals. To reinforce our behavior, we have formulated this Code of Conduct & Ethics which serves as principal guide while delivering in the most professional and ethical way.

We expect temporary and contract staff, consultants and agents and any other third party who works for Syntel to act in accordance with this Policy. This policy can be found in our Internal Portal (Syntelligence) and you have a duty to comply with it.

2. Compliance with Laws

It is Syntel's policy to comply with all applicable legal requirements, especially applicable laws and regulations. Any employee whose work is affected by laws and regulations should acquire sufficient understanding of them in order to recognize risk areas and to know when management or Legal Department advice is needed. An employee dealing with any potentially sensitive legal issue, such as discussions with or about competitors, sensitive business strategies or recruiting or terminating employees in certain situations should ensure confidentiality of such issues and contact the Legal Department immediately.

Syntel is in a "high technology" industry. As a result, Syntel technology in the form of software, software data, hardware and all technical data relating to the design, production and use of such software or products and is subject to U.S. and foreign export control laws and regulations (especially applicable for onsite project work). This means that when Syntel software data and technical data are exported, Syntel must, if required, obtain an export authorization from the U.S. or appropriate foreign government. While most employees are not likely to be involved in the direct export of Syntel software, products or data, they should be aware of how export law affects the company. Export laws apply to all international transactions, including intra-company, with suppliers, other software and equipment manufacturers and affiliate/group companies - any relationship where Syntel will be involved in exporting commodities, technical data, software, technical assistance and similar support. It is against the law and Syntel policy to facilitate the unauthorized export of Syntel technology. If employees have questions on export related issues, they should talk with his /her respective project manager or Syntel's TSG dept. or its General Counsel/his designate.

3. Confidential Information

Information that is not available to the public, whether it concerns Syntel or its customers or any third parties with whom Syntel has a confidentiality agreement, should be considered confidential information. Information which is circulated internally (to Syntel employees) should not be considered available to the public unless also contained in a published Syntel news release. Employees should not comment on speculation or other information which may be published by the media (print, radio, TV, Internet, etc.) concerning Syntel and/or its customers. Employees must be conscious of the need to protect the sensitive, proprietary and confidential information entrusted to them in connection with their jobs, including software, the business, financial, development, and marketing plans associated with Syntel, senior management changes and the confidential data of Syntel's customers and employees. Keep in mind that harmful disclosure may start with the smallest leak of information. Fragments of information disclosed by one employee may be pieced together with fragments from other sources to form a fairly complete picture.

The unintentional disclosure of confidential information can be just as harmful as intentional disclosure. To avoid unintentional disclosure, do not discard documents containing confidential information without shredding them first, lock files containing confidential information and never discuss confidential information that has not been made public by Syntel with any unauthorized person. An employee should not discuss confidential information with authorized Syntel employees if in the presence of others, employees or third parties, who are not authorized. This also applies to discussions with family members or with friends, who might innocently or inadvertently pass the information on to someone else.

Confidential information may not be disclosed except as authorized by Syntel. Employee disclosure of confidential information may harm Syntel's customer relationships and is grounds for disciplinary action, up to and including termination of employment.

If someone outside Syntel asks questions about the company, its employees or its business activities, including who our customers are or what new contracts have been signed or are in the pipeline, either directly or through another person, employees should not attempt to answer them unless they are certain they are authorized to do so. If not authorized to answer, employees should take the inquirer's name, number and business affiliation, refer them to the appropriate source within Syntel and provide the information to the appropriate source.

Inquiries by industry analysts and investors should be referred to the Chief Financial Officer (or his designate) as soon as possible. All recruiting firms requests for information on former employees should be referred to the Global Head - Human Resources (or his designate) without discussion. If an employee receives a request from an attorney, investigator, or any law enforcement officer for information on or to conduct an interview concerning Syntel's business, the request should be referred to the General Counsel or the Global Head -Human Resources (or their designates). Similarly, unless authorized to talk to the media, or to anyone else writing about or otherwise covering Syntel or the industry, an employee should direct the person to the **Head – Marketing/Chief Marketing officer**. If an employee does not know the functional area to which the questioner should be referred, questions should be directed to his/her respective manager or to the HR department.

Besides their obligation not to disclose any of Syntel's confidential information to anyone outside the company, employees may not use such information for personal matters. These obligations apply whether or not the employee developed the information.

Syntel's computer software, documentation and related materials including patent, trademark, etc. are protected by intellectual property rights including copyright as well as being preserved as trade secrets in the company. In some instances Syntel has access to copyrighted or copyrightable materials owned by others. Whether owned by Syntel or by third parties, all employees should be aware that no third party may be permitted to make copies without authority in advance from Syntel's management. Data privacy rules as applicable shall be strictly adhered to.

Never accept confidential information regarding competitors unless from an authorized source by that competitor. If employees inadvertently receive such information, they should immediately inform the General Counsel. Never contact a former Syntel employee in an effort to obtain unauthorized confidential information.

Notwithstanding the above, in the course of employment with Syntel, employees may become aware of information about Syntel or other companies, such as customers, suppliers or competitors that has not been made public. Employees may not use such nonpublic or "inside" information about Syntel or another company for an employee's financial benefit. Syntel shall not tolerate the improper use of inside information. Here are some examples of how to avoid the improper use of inside information:

- If employees know that Syntel is about to announce a new service or make a purchasing decision that could affect the price of the stock of a competitor or supplier, they should not buy or sell the securities of that company until after the information becomes public
- Similarly, if employees have material nonpublic information about Syntel or know that Syntel is about to make an announcement that could affect the price of its own securities, they should not buy or sell Syntel securities until after the announcement
- Employees should not buy or sell the stock of a customer or supplier based on any inside information employees have about that company
- Employees should not disclose inside information to Syntel employees who do not have a business need to know, or to anyone outside of Syntel
- Employees should not evade these guidelines by acting through anyone else. Until the information is officially disclosed to the public and the public has had an opportunity to absorb it (this usually takes about two trading days after official disclosure through a press release or otherwise), employees must refrain from the purchase or sale of securities of the corporation to which the information relates

Employees should immediately report any incident associated with any of these prohibited activities to Syntel's General Counsel or the Global Head - Human Resources. Any employee to report such behavior will remain confidential and may not be retaliated against.

See also: Insider Trading

4. Conflict of Interest

All employees must conduct themselves with the highest standards of integrity, honesty and fairness to avoid any conflict between their personal interests and the interests of Syntel. A conflict of interest exists whenever an employee's interest in a competitor, customer or supplier is to the extent or nature that it affects, or appears to affect, the employee's responsibilities to Syntel. An obvious example is an employee authorizing purchases from a customer/supplier in which he or she has an actual or prospective ownership, financial or other significant interest. Thus, the employee's responsibility to Syntel and his or her personal desire to benefit from such a transaction are incompatible. In this regard, all employees should avoid even the appearance of impropriety. While it is not possible to list all situations constituting unacceptable conflicts, some typical situations are described below.

No employee may accept employment with or become directly or indirectly involved as an independent contractor, consultant or otherwise with any Syntel competitor. No employee may accept employment with or become directly or indirectly involved as an independent contractor, consultant or otherwise with any Syntel customer or supplier without the prior written approval of the employee's manager and the

Global Head- Human Resources. No employee may accept a position with any other company if the time demand of the position will impair the employee's ability to fulfill obligations to Syntel.

No employee may accept a position as a director of a Syntel competitor. No employee may accept a position as a director of any Syntel customer or supplier, or a company which enhances the marketability of or otherwise supports a competitor's products or services, without the prior written approval of Global Head - Human Resources. Syntel employees may not receive separate compensation for service on the Board of Directors of a Syntel group company if the service is at Syntel's request or in connection with a Syntel investment in or relationship with that company.

Syntel employees may not own a financial interest in, lend substantial sums to or borrow substantial funds from any Syntel customer, supplier or competitor that might cause divided loyalty or even the appearance of divided loyalty. Whether there is a financial conflict of interest depends upon many factors, including: (a) the employee's ability to influence Syntel decisions that might affect personal financial interest, (b) the size of the investment in relation to the employee's income, investments and financial needs, and (c) the nature and extent of the competition or the relationship between Syntel and the other business.

Unless otherwise permitted by Syntel, no employee may: (a) sell his or her own services or products, or those of another person or firm, if Syntel offers similar services or products, or (b) engage in activities which enhance the marketability of or otherwise support a competitor's products or services. No employee may conduct Syntel business with a member of his or her family, or with an individual or a business organization with which the employee or the employee's family has an association or with any other business entity, without first obtaining written approval from his or her manager and the Global Head - Human Resources.

A Syntel employee may not personally take advantage of a business opportunity rightfully belonging to Syntel or derive personal profit, gain or advantage (other than compensation from Syntel) as a result of any transaction undertaken on behalf of Syntel. Employees should neither purchase nor seek to purchase any corporate asset not offered publicly for purchase, either directly or indirectly through family or other affiliations. If employees and their families choose to purchase Syntel stock, it should be undertaken as a long-term investment. Speculative trading in Syntel's stock is discouraged.

Each employee must promptly disclose in writing actual or potential conflicts of interest to the employee's manager. The manager will review the matter and communicate Syntel's position in writing. The manager should seek the advice of the Global Head - Human Resources and/or the Chief Administrative Officer/General Counsel. Approval will not be given unless the relationship will neither interfere with the employee's duties nor damage Syntel or its reputation. The manager's response will indicate either (a) that Syntel has no present objection to the relationship, but the decision is subject to future review, or (b) the steps to be taken to resolve the conflict to Syntel's satisfaction.

5. Employee Appearance

In general, Syntel asks all employees to maintain a neat and professional appearance. Please remember that each of us represents Syntel to our customers. Employees of Syntel located at client sites must be in compliance with client site dress codes. Further, all Syntel employees going to a client location should adhere to the dress code adopted by the client for that location. Similarly, clients visiting such Syntel facilities should be notified of our dress code prior to their visit.

Business casual attire means that employees of Syntel may wear appropriate business casual attire while at work at any Syntel facility adopting this dress code. Appropriate business casual attire for men includes shirts with collars, Polo neck T-shirts, sweaters (not sweatshirts), and slacks (not sweatpants, or shorts). Appropriate business casual attire for women includes dresses, skirts, slacks (not sweatpants, or shorts), casual shirt, collared t-shirt, tops, tunics blouses with collars, and sweaters (not sweatshirts). Appropriate business casual attire does not include tennis shoes, sandals, cut-offs, torn or ripped items, or items with inappropriate writing, pictures, or logos.

Even with a business casual attire dress code, employees are expected to dress appropriately for situations which call for more formal business attire. For example, Syntel managers and supervisors meeting with clients who maintain a more formal dress code (e.g., suit and tie), should adhere to that dress code for the meeting, whether the meeting is at a Syntel location or at a client location. For visitors to Syntel, you may choose to advise our guests that we have adopted a business casual dress code at our offices.

Business casual attire is a privilege, not a right. Please remember (and remind your co-workers) to abide by the policy so that we can continue to have a business professional attire.

Remember: no sweatpants, no sweatshirts, no inappropriate writings, pictures, or logos.

If you question whether something is appropriate, err on the side of business professional attire.

The dress code policy guidelines cannot cover all contingencies, so we expect employees to demonstrate certain amount of wisdom while selecting the suitable attire for professional environment.

6. Employee Communication

To keep you informed, Syntel communicates information about new account wins, corporate events, and personnel moves. We do this to keep everyone apprised of Syntel's progress and exciting events shaping our future.

In order to maintain some control over this news, Syntel is asking each employee to treat all internal communication as CONFIDENTIAL. With all of the Internet chat rooms, electronic mail, and instant news vehicles, rumors and information can make its way to the public very quickly. These "news leaks" not only damage our credibility but can harm our relationships with customers who prefer for our agreements to remain anonymous.

If employees are identified to be communicating internal news to outside audiences, disciplinary action may be taken up to and including termination.

See also: Confidential Information

7. Employment References

It is Syntel's policy to provide employment verification letters to its employees or former employees upon request. All requests should be directed to the Human Resources Department. Employment verification letters will confirm the dates during which an employee worked at Syntel and job title. However, Syntel will not provide reference or experience letters that indicate a current or former employee learned, used or possessed specific skills while employed by Syntel. Syntel employees may not provide any reference or experience letters in their capacity as employees of Syntel. If Syntel employees provide references in their

individual capacity, they must not use Syntel letterhead or sign the letter as a Syntel employee. In addition, letters provided in an employee's individual capacity must include the following statement:

"The opinions expressed in this letter are those of the undersigned and are not authorized by and do not necessarily reflect the opinions of Syntel, Inc. (or its subsidiaries/group companies) or any of its officers, employees or agents."

8. Employee Conduct

Syntel strives to provide all employees with a healthy, safe and productive work environment that is free from discrimination and harassment based on race, color, religion, sex, sexual orientation, age, national origin, disability or veteran status. The use of racial, religious or other slurs or any other remarks, jokes or conduct that creates an offensive work environment will not be tolerated. Syntel expects employees to be polite, professional and courteous to fellow employees as well as to customers and to refrain from swearing, rowdiness or any other inappropriate behavior. Each of us has the responsibility to do our utmost to make all of our customers feel that the treatment they receive is friendly, courteous and a natural part of our commitment to providing quality service. Fighting, abusive or threatening language or behavior and the possession of weapons of any type will not be tolerated. Any conduct by an employee that violates this standard of employee conduct shall be subject to disciplinary action up to and including termination.

Syntel shall not tolerate discrimination, sexual harassment, physical or verbal threats or any other form of harassment or abuse, all of which deny employees the opportunity to contribute to the best of their abilities and deprives the company of their full talents. Integrating the unique abilities and talents of a diverse work force allows for greater flexibility and creativity in the workplace and in the community. Preventing harassment, discrimination and threats is a matter of respecting each other's rights and dignity, which is a basic value at Syntel. Syntel employees and business associates are entitled to conduct their business in a work environment free of these distractions. To help ensure such an environment, all employees must take any discrimination, harassment or threat seriously and promptly advise appropriate management.

Whether you are on or off duty, your conduct reflects on Syntel. You are constantly encouraged to observe the highest standards of professionalism at all times.

9. Guidelines for Appropriate Conduct

As an integral member of the Syntel team, you are expected to accept certain responsibilities, adhere to acceptable business principles in matters of personal conduct, and exhibit a high degree of personal integrity at all times. This not only involves sincere respect for the rights and feelings of others but also demands that both in your business and in your personal life you refrain from any behavior that might be harmful to you, your co-workers, and/or Syntel, or that might be viewed unfavorably by current or potential clients or by the public at large. Whether you are on or off duty, or working in a Syntel or client facility, your conduct reflects on Syntel. You are, consequently, encouraged to observe the highest standards of professionalism at all times.

Listed below are some of the rules and regulations of Syntel. This list should not be viewed as being all-inclusive. Types of behavior and conduct that Syntel considers inappropriate and which could lead to disciplinary action up to and including termination of employment without prior warning, at the sole discretion of the company, include, but are not limited to, the following:

- Falsifying employment or other Syntel records
- Violating Syntel's nondiscrimination and/or sexual harassment policy
- Soliciting or accepting gratuities from customers or clients
- Establishing a pattern of excessive absenteeism or tardiness
- Engaging in excessive, unnecessary, or unauthorized use of Syntel's or its client's supplies, particularly for personal purposes
- Reporting to work intoxicated or under the influence of non-prescribed drugs
- Illegally manufacturing, possessing, using, selling, distributing, or transporting drugs
- Bringing or using alcoholic beverages on Syntel property or using alcoholic beverages while engaged in Syntel business while off Syntel's premises, except where authorized
- Fighting or using obscene, abusive, or threatening language or gestures
- Stealing property or assets from coworkers, clients or Syntel
- Having unauthorized firearms on Syntel premises or while on Syntel business
- Disregarding safety or security regulations of Syntel or its clients
- Engaging in insubordination
- Failing to maintain the confidentiality of Syntel or client information
- Using the computer to do anything that is of an unethical, immoral or illegal nature
- Having an intimate or dating relationship between any Syntel manager and a direct report of that manager without the prior written approval of the CEO and Head of HR.
- Having an intimate or dating relationship between any Syntel employee of B7 category and above and any other Syntel employee without the prior written approval of the CEO and Head of HR.

Perhaps the best guideline of all is to use good judgment. It would be virtually impossible to cite examples of every type of activity that might give rise to a question of unethical or inappropriate conduct. Therefore, it is important that each of us rely on our own good judgment in the performance of our duties and responsibilities. When those situations occur where the proper course of action is unclear, request advice and counsel from your department head. The reputation and good name of Syntel depends entirely upon the honesty and integrity of each one of us.

10. Employee/Customer Relations

Syntel employees are key contributors to the delivery of quality service to our customers. Syntel recognizes the importance of its employees and works hard to provide strong support in order to focus on customer satisfaction rather than internal issues. In spite of our best efforts, problems may occasionally arise. When this happens, you should immediately contact your Syntel manager, not the customer.

We all have an individual responsibility not to burden our customers with internal Syntel matters, whether personal or business related. Involving customers in our problems is an imposition on their time, may complicate and delay resolving the matter and is damaging to the professional image of the employee and Syntel. Syntel is committed to treating its employees fairly and if you feel your immediate Syntel manager is not responsive to your issue or concern, notify his or her Syntel manager or superior and finally, Global Head - Human Resources but never the Syntel client/customer or Syntel vendor.

Your adherence to this policy will help Syntel to grow by continuing to provide quality service and maintaining and improving healthy working relationships with our customers.

11. Insider Trading

This policy applies to all officers, directors, employees and agents of Syntel.

- I. It is the policy of Syntel to comply, and that its officers, directors, employees and agents comply, with all applicable securities laws and regulations.
- II. No person covered by this Policy shall purchase or sell any security issued by Syntel while such person is in possession of material information about Syntel that has not been disclosed to the public. Nor shall any such person provide such information to any other person, whether employed by Syntel or not, except persons with a need to know such information in order to perform their duties for Syntel. No person covered by this policy may use any material information relating to Syntel that has not been disclosed to the public as the basis for purchasing or selling any security issued by any other entity.
- III. All external Board of Directors members and the following employees of Syntel: the Chairman, President & CEO, Vice-Presidents, , Senior Directors, Executive Officers and other persons designated by the President & CEO or a person designated by the President & CEO for this purpose the Compliance Officer may not purchase or sell any security issued by Syntel unless the transaction (1) occurs during a Window Period (as defined below) or (2) has received the prior approval of the Board of Directors or the Compliance Officer (in the case of a proposed trade by the Compliance Officer, with the prior approval of the President & CEO and in the case of a proposed trade by the Chairman or President/CEO, with the prior approval of the Board of Directors). Daniel M. Moore shall be the initial Compliance Officer until his resignation or removal from that position by the President/CEO.
- IV. No executive officer or director of Syntel shall sell any equity security of Syntel if such person either (1) does not own the security sold or (2) does not deliver the security against such sale within twenty days thereafter or does not within five days after such sale deposit the security in the mails or other usual channels of transportation.
- V. Each executive officer and director of Syntel shall comply with the filing requirements of Section 16(a) of the Securities Exchange Act of 1934 or such other statutory rules, as applicable. The Compliance Officer, in conjunction with Syntel counsel, shall implement a system to assist executive officers and directors in the timely filing of all required reports under the foregoing provisions.
- VI. Each executive officer and director making sales in the open market shall make such sales in compliance with Rule 144 under the Securities Act of 1933 or such other statutory rules, as applicable.
- VII. The Compliance Officer may adopt such reasonable procedures as he or she shall deem necessary or desirable in order to implement this policy statement. Each person covered by this policy statement may be required to execute and deliver a statement to Syntel, certifying that such person has complied with this policy statement at all times from the date hereof (or such lesser time as such person has been covered hereby)

- VIII. All officers, directors, employees and agents of Syntel are encouraged to consult with the Compliance Officer if they have questions about the applicability of this policy to them or their activities.

See also: Confidential Information.

12. Internet Access Policy

Syntel's Internet connection is a corporate resource, and during business hours should be used only for Syntel's business purposes. Whenever an employee is using Syntel's Internet connection, she/he should use good judgment and adherence to the policies below. Employees working at customer sites are required to adhere to the customers' policies on Internet use.

The primary purposes of Syntel's Internet connection are:

- Electronic Communications: Electronic communications systems and all messages generated on or handled by electronic communications systems, including back-up copies, are considered to be the property of Syntel Inc. (including its subsidiaries).
- World Wide Web access

Due to the potential for viruses and other security risks, employees may only download material related to Syntel's business. Additionally, downloading, including "browsing," of the following type of material is prohibited at any time:

- Any material which, when taken as a whole, appeals to the prurient interest, depicts or describes sexual conduct in a patently offensive way and lacks serious literary, artistic, political or scientific value.
- "Cracking" software, utilities, or sites intended to expose or exploit security deficiencies in Syntel's or any other information system.
- Any illegal materials or materials whose purpose is to facilitate illegal activity.
- Any software ("freeware" or "shareware") of any kind, though this material may be "browsed".

The following general activities are also prohibited:

- Use of Syntel Internet resources for non-Syntel commercial purposes; e.g., in support of a home business.
- Mass mailings of unsolicited e-mail; e.g., for advertising purposes.
- Operation of any kind of "server" software (httpd, ftpd, etc.).*
- Changing network settings (e.g., IP address, DNS information) from those set up by the IS team.
- Installation of software that constantly updates information for display or later retrieval; e.g., PointCast.
- Sending out any non-business related material when posting for public access.
- Individual passwords must never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to responsibility for actions the other party takes with the password.

- Misrepresenting, obscuring, suppressing, or replacing a user's identity on an electronic communications system is forbidden. The user name, electronic mail address, organizational affiliation, and related information included with electronic messages or postings must reflect the actual originator of the messages or postings.
- Except as otherwise specifically provided, employees may not intercept or disclose, or assist in intercepting or disclosing, electronic communications.
- Workers must not use profanity, obscenities, or derogatory remarks in electronic mail messages discussing employees, customers, competitors, or others.

Messages no longer needed for business purposes must be periodically purged by users from their personal electronic message storage areas

13. No Expectation of Privacy Policy

No employee shall have any expectation of privacy regarding any information, documents, materials, or other items (personal or work-related) kept, stored or transmitted on or through any company provided desk, file, computer, server, telephone, cellular telephone, locker, vehicle or other company property. This specifically includes any and all information and is not limited to emails, calendars, phone records, internet usage, websites visited, text messages, instant messages, etc. The company has the right to search and review at any time, without notice to the employee, any and all such information kept, stored or transmitted on or through any company provided property, subject to appropriate data privacy laws and rules, as applicable.

14. Legally Sensitive Issues

Syntel often encounters situations where there is more than one method which may be used to achieve its business goals. The alternative methods may bear different levels of legal liability risk. Officers and employees who encounter these situations should contact the appropriate person in the HR and/or Legal Department to discuss the potential legal issues and ways of minimizing legal risk before proceeding. These legally sensitive areas include such topics as:

- Soliciting competitors' employees
- Terminating employees
- Claims of harassment or discrimination
- Sensitive business strategies
- Discussing competitors with third parties
- Discussing the company's future prospects with potential investors
- Discussions with competitors
- Relations with government officials
- Exporting technology
- Immigration issues
- Any potential litigation

To the extent written communication on these topics is desirable, it should be routed to or from the Legal Department for protection, under attorney/client privilege, from discovery.

15. Media Relations

In Syntel's competitive environment, it is more important than ever to maintain consistency in company messages. Syntel's intention is to provide consistent, timely messages that reflect the company's broad strategic objectives. To help obtain that consistency, all of the company's contacts should be coordinated through the Head - Marketing. These contacts include but are not limited to news releases, requests for interviews, media events, investor relations presentations and letters to the editor, etc. that focus on Syntel or purport to represent company viewpoints.

To ensure we accomplish our objectives, no Syntel employee should comment on matters related to Syntel, or matters that relate to our business without the prior involvement of the Head - Marketing. Avoid acting as spokesperson for Syntel without first contacting Head - Marketing. If you are contacted directly by someone outside of Syntel (for example a reporter, editor, stock analyst, investment banker, etc.) you should note the caller's name, company, telephone number and topic and immediately contact the Head - Marketing. Only the Head - Marketing, Chief Operations Officer, Chief Financial Officer, Chairman or Chief Executive Officer as applicable are authorized to speak on behalf of Syntel. Ensure all media announcements and press releases are approved in advance by Head of Marketing.

16. Outside Employment/Activity

Because outside employment may affect the service employees render to Syntel and its customers, Syntel employees are permitted to accept outside employment only after prior approval of BU Head and HR Head and in accordance with the following provisions.

- Employees may not accept supplementary employment which involves:
- Any position which would be in direct competition with Syntel.
- Use of Syntel or Syntel's customers' equipment, supplies, or facilities.
- Participating in activities while on Syntel time.
- Participating in activities which might adversely affect Syntel's or the employee's community relationship or image.

17. Protection and Use of Syntel's Assets

Syntel's assets are of great value to our competitiveness and success as a business. Syntel's assets include not only our intangible assets such as information on business strategies and clients, but also our physical assets. Protecting all of these assets is very important. Loss, theft or misuse of Syntel assets jeopardizes our future. For this reason, employees are personally responsible not only for protecting Syntel property entrusted to them, but also for helping to protect the company's assets in general. Employees should be alert to any situations or incidents that could lead to the loss, misuse or theft of Syntel property. All Syntel property is subject to search including desks and computer files. Syntel reserves the right to require disclosure of all passwords to all files and information maintained on Syntel property. Further Intellectual Property Laws protect Syntel's intangible assets – our trademarks, copyrights, patents, domain names and related intellectual property rights. Employees need to ensure protection of such intangible assets and should be alert to and report any suspected infringements promptly to Legal department. Employees should report all such situations to their manager or Syntel's General Counsel as soon as they come to their attention.

Syntel equipment, systems, facilities, laptops, corporate charge cards and supplies must be used only for conducting Syntel's business or for purposes authorized by management. For example, an increasing

number of employees own equipment that is capable of using Syntel supplies, such as diskettes. Since these supplies are readily available throughout the company, the question of making personal use of them frequently arises. The answer is clear: employees may not use Syntel supplies for personal purposes.

18. Solicitation

Soliciting by employees in any form during working time is prohibited unless approved by the employee's manager. Non-employee distribution or solicitation anywhere on company premises at any time is also prohibited.

Participating in Demonstrations: Kindly do not engage yourself or participate in any demonstration, which disrupts the normal functioning of the Company.

Canvassing of Non-Official or other Influence: Kindly do not indulge in any attempt, to bring any outside influence in respect of matters pertaining to your service in the Company.

19. Bribery

Syntel will not tolerate, under any condition, offering or receiving of bribes or any other form of improper payments. Bribery is illegal and can result in criminal penalties and jail time to those involved. You should not, directly or indirectly, give or agree to give and/or accept or agree to accept, any gifts, personal benefits or money in any manner whatsoever that are or could be construed as intending to influence the decision of customers, suppliers, government officials or political representatives. You should never do anything to induce or facilitate someone else to breach this standard and always report any violations or suspected violations to Legal and/or Admin department.

20. Smoking & consumption of Tobacco products

Syntel is committed to maintaining a smoke-free work environment, and recognizes the hazards caused by exposure to environmental tobacco smoke, as well as the life-threatening diseases linked to the use of all forms of tobacco. To further this commitment, smoking or use of any form of tobacco is not allowed in company facilities, company sponsored meetings or in company vehicles. This policy applies to all employees, vendors, guests and customers.

21. Drinking and Substance Abuse

The consumption, possession or supplying of alcoholic beverages (except at functions sponsored by or approved by Syntel) and illegal drugs are prohibited in company facilities, vehicles or on company premises. Reporting for work under the influence of alcohol or non-prescribed drugs is prohibited and will result in disciplinary action up to and including termination. If requested by client or consultants at the client site, drug testing may be required.

22. Distracted Driving

Syntel advocates safe and responsible driving habits. For purposes of this policy, "hand-held electronic devices" includes but is not limited to, wireless phones, computers, on line email, pagers, palm pilots, pda's, and any other electronic device being held in the person's hand.

In order to foster a safe driving environment and to protect the welfare not only of our employees, but other persons whose safety could be jeopardized by distracted driving, the following guidelines has been adopted

- Syntel employees are prohibited from using hand-held electronic devices in any way related to Syntel business while operating a motor vehicle. This includes, but is not limited to, going to or from any Syntel facility or Syntel related activity even if the use of the device is not related to Syntel business.
- In addition to the above, Syntel employees are encouraged to:
 - Plan ahead so that you can use the hand-held electronic device before or after [but not during] the operation of a motor vehicle.
 - Pull over and stop at a safe location if you must use a hand-held electronic device.
 - Avoid all distractions and concentrate fully on the safe operation of your motor vehicle particularly if there is adverse weather, traffic or road conditions.