ELECTRONIC & EXTERNAL COMMUNICATIONS

1.0 Purpose

This policy provides guidelines regarding the use of electronic communication and data storage devices by employees and is intended to apply to communications between employees, and between employees and third parties, by means of verbal communication, telephones, fax machines, computers, computer networks, the Internet, and similar existing or future means of communicating, and to the data transmitted and/or stored using such devices.

2.0 Background

Technological advances are rapidly making new means of communicating available to the Company and its employees. Traditional forms of communicating, including paper correspondence and verbal discussions by telephone, have been supplemented by methods which can enhance communications by moving and recording larger volumes of information more efficiently than traditional means. As business communications and record storage become more technology dependent, there is a need to adopt Company-wide guidelines in order to ensure that the Company's professional standards are maintained by all of its employees.

3.0 Professional Conduct

The Company's image and work environment depend greatly upon how its communications and records are perceived by its employees, customers, prospective customers and suppliers. The Company's electronic communications are expected to adhere to the same standards as all other business activities and must always adhere to Company policies governing the conduct of its business. Employees are directed to Procedures GP-C-01 (Conduct of Business), GP-C-04 (Equal Employment Opportunity), GP-C-05 (Harassment) and the GP Internet Posting/Social Media Guidelines for more specific guidance. In addition, as the Company's clients increasingly entrust the Company with sensitive information in both tangible and intangible (e.g., electronic) form, the Company's employees must demonstrate vigilance in protecting the Company's and its clients' sensitive information. Employees are directed to Procedures GP-ITS-01 (Information Classification) and GP-ITS-02 (Information Handling), for specific guidance.

4.0 Procedures In A Crisis Communications Event

It is the company's policy to manage its relations with the media in an open and pragmatic way. In a time of crisis employees may receive communications from many parties trying to obtain privileged information. The company will be responsive to the legitimate interests

of the media and relevant partners. It will also be proactive in disseminating information about the company, its policies and products when it is judged to be in the best interests of the business by corporate, functional or local management.

During a period of perceived crisis or following an emergency event involving GP Strategies and its clients, employees must avoid external verbal or written contact with third parties about events that emerge affecting our clients or are taking place within our Company. Third parties include the media and interacting on any other social medium. If an employee receives a request for information, prior approval must be obtained from the supervisor and the Corporate Marketing and Communications department before responding. The employee is responsible to notify their supervisor of the request. Emergency information for public consumption will be released at a corporate level or by a designated onsite manager. Matters likely to be important to GP Strategies and likely to come to public notice at a time of crisis, include:

- Introduction, withdrawal, acquisition or sale of products or the acquisition or sale of businesses;
- Major personnel changes, operating procedures, organization, products or policy involving or affecting GP Strategies;
- Public statements, publications or coverage relating to government actions or investigations affecting GP Strategies;
- Litigation issues; and
- Emergency incidents involving our employees and/or those incidents involving GP Strategies interactions with clients and local communities.

5.0 Business Purpose for Electronic Communication

The software, equipment and outside services utilized by the Company and its employees in the course of their employment are intended solely to advance the business interests of the Company. Personal use by Company employees is generally not compatible with advancing the Company's interests and may lead to disciplinary action, up to and including termination of employment. Electronic communication media made available to employees by the Company may not be used for advocating political, religious or other personal opinions or causes that have not been approved in advance by the President. In addition, electronic communication media may not be used by an employee for personal gain or recreation. All such media utilized by the Company are intended for use as business tools only.

Furthermore, employees should not seek access to sensitive information relating to the Company, its employees or its clients that is not necessary for them to perform their assigned duties. Employees who violate this Policy will be subject to disciplinary action, up to and including suspension or termination of employment.

6.0 Monitoring

The Company reserves the right to (i) determine which employees will have access to electronic communications media or data, (ii) place such restrictions or limits on the use of such media or data as the Company shall deem to be necessary or appropriate in its discretion, (iii) monitor for noncompliance with or circumvention of those restrictions or limits, (iv) refuse or deny access to or use of electronic media, (v) monitor usage of electronic media by employees, including all communications by way of such media, (vi) monitor computers for compliance with current software licensing contracts and laws, and (vii) take such disciplinary action, up to and including suspension or termination of employment, as the Company deems to be appropriate in response to instances of unauthorized access, disclosure, use, misuse, recklessness or other use of electronic media or data by employees which violates Company Policies or Procedures, or which the Company determines in its discretion to not be in the best interests of the Company. Employees desiring privacy for personal communications should not utilize Company communications media for such purpose.

7.0 Protection of Intellectual Property

Technology affords tremendous opportunities for rapidly transmitting, receiving and storing information. Employees must at all times protect against unauthorized transmission or disclosure of the Company's and its clients' intellectual property and confidential information (including but not limited to copyrighted materials, employee personal information, financial data, trends and projections, and other data which could adversely affect the Company's competitive position and business prospects). Employees must also guard against receiving or using unauthorized or defective intellectual property received from outside the Company, including unauthorized copies of copyrighted software and software containing "viruses." It is illegal to copy copyrighted software without permission of the copyright owner, and the Company prohibits the use of unlicensed, "pirated", personal or otherwise unauthorized software on Company computers. Any questions regarding the legitimacy of software found on a Company computer should be addressed to the Vice President of Corporate IT. The Company will acquire sufficient authorized copies of software needed to conduct its business. Employees who violate this policy will be subject to disciplinary action, up to and including suspension or termination of employment.