Privacy Policy

1.0 Company Intentions and Management Responsibilities

Intentions And Objectives—In the course of its business, it is necessary for Impact to record, store, process, transmit, and otherwise handle private information about individuals. Impact takes these activities seriously and provides fair, secure, and fully-legal systems for the appropriate handling of this private information. All such activities at Impact are intended to be consistent with both generally accepted privacy ethics and standard business practices.

Management Responsibilities—Management must take reasonable efforts to ensure that all private information maintained by Impact is accurate, timely, relevant, and complete. Management also must make reasonable efforts to ensure that all private information is used only as intended, and that precautions preventing misuse are both effective and appropriate. Management is responsible for establishing appropriate controls to ensure that private information is disclosed only to those who have a legitimate business need for such access. Management must establish and maintain sufficient controls to ensure that all Impact information is free from a significant risk of undetected alteration.

2.0 Disclosure of Private Information

Revealing Information about Policies and Procedures—As a general rule, information security policies and procedures should be revealed only to Impact workers and selected outsiders, such as auditors, who have a legitimate business need for this information. A notable exception involves the policies that deal with private information about individuals. All involved individuals have a right to receive an officially-approved statement of Impact policies and procedures regarding the handling of information about them. In addition, Impact must disclose the existence of systems containing private information and the ways that this information is used. With the exception of criminal and policy-violation investigations, there must be no system of personnel records within Impact whose very existence is kept secret from the people described therein.

Handling Private Information Requests—All requests for private information coming from a person or organization outside Impact must be forwarded to Impact's Chief Administrative Officer, who will be responsible for deciding whether requests will be granted.

3.0 Appropriate Handling of Private Information

Collect Only Necessary Information—In general, Impact may collect, process, store, transmit, and disseminate only that private information that is necessary for the proper functioning of its business. For example, Impact management must not collect information about worker activities during non-work hours unless these activities are highly likely to influence the involved worker's performance, or unless they could adversely affect the reputation of Impact.

Destruction of Private Information—When private information is no longer needed, it must be destroyed by shredding, or by other destruction methods approved by the Information Security Team. Destruction of private information resident on computer disks and other magnetic media must be accomplished with an overwriting process. A simple erase process is not sufficient. To assure the proper destruction of private or confidential information, disposal of computers with embedded hard disk drives or other data storage systems must proceed according to procedures outlined in Impact's Data Retention and Destruction Procedure.

Removal of Private Information—Private or confidential information must not be removed from Impact offices. Permission to take such information offsite may be granted by a departmental manager provided the involved worker has completed the information security segment of telecommuter training, and passed the associated test. Signed third-party non-disclosure agreements may additionally be required when private information is removed from Impact offices. Private information must not be moved to another country unless the permission of the manager of the Information Security department is obtained.

Preventing Inadvertent Disclosure on Screens—The display screens for all personal computers, workstations, and dumb terminals used to process sensitive or valuable data, including private information, must be positioned such that they cannot be readily viewed through a window, by persons walking by a hallway, or by persons waiting in reception and related areas.

Preventing Inadvertent Disclosure by Hardcopy—Whenever a worker is handling private information, if a person who is not authorized to view that information enters the immediate area, steps to conceal the information must promptly be taken. If

the information is in physical form, the information can be covered with other material. If the information is displayed on a computer screen, the worker can minimize the application displaying the information, invoke a screen saver, or log off.

4.0 Private Information on Computer and Communication Systems

Expectation of Privacy—All messages sent over Impact internal computer and communications systems are the property of Impact. Management reserves the right to examine all information transmitted through these systems. Examination of such information may take place without prior warning to the parties sending or receiving such information. Because the Impact computer and communications systems must be used for business purposes only, workers must have no expectation of privacy associated with the information they store in or send through these systems.

Examination of Stored Information—At any time and without prior notice, Impact management reserves the right to examine archived electronic mail, private file directories, hard disk drive files, and other information stored on Impact information systems. Such examinations are typically performed to assure compliance with internal policies, support the performance of internal investigations, and assist with the management of Impact information systems.

Manager Involvement in Monitoring—Whenever a worker's computer or communications user ID is monitored for investigative or disciplinary purposes, the involved worker's manager must be informed of this activity promptly. All worker monitoring must itself be logged for subsequent management review and possible use in disciplinary or legal actions.

Department Manager Activity Review—Impact routinely logs web sites visited, files downloaded, and related information exchanges over the Internet. Impact records the numbers dialed for telephone calls placed by each worker. Department managers may receive reports detailing the usage of these and other internal information systems, and are responsible for determining that such usage is both reasonable and business-related.

Changing Information Resident on Systems—Management reserves the right to delete, summarize, or edit any information posted to Impact computers or communication systems. These facilities are privately-owned business systems, and not public forums, and as such do not provide free-speech guarantees.

Routine Usage of Backup Systems—All files and messages stored on Impact systems are routinely copied to tape, disk, and other storage media. This means that information stored on Impact information systems, even if a worker has specifically deleted it, is often recoverable and may be examined at a later date by system administrators and others designated by management.

Remote Computer Monitoring—Impact routinely scans the personal computers connected to its networks. These scans ensure that remote computers are operating only with approved and licensed software, are free from viruses and worms, and have been used only for approved business purposes.

Encryption of Electronic Mail—Workers must consider electronic mail to be the computerized equivalent of a postcard. Unless material sent by electronic mail is encrypted, workers must refrain from sending credit card numbers, passwords, research and development information, medical histories, computer programming source code, and other private or confidential information through electronic mail.

Links between Separate Types of Private Data—Without advance consent from the manager of the Information Security department, Impact information systems must not be configured to support new links between private information and other types of information related to the same individual.

Testing With Sanitized Data—Unless written permission is obtained from the Director of Information Security, all software testing for systems designed to handle private data must be accomplished exclusively with production information that no longer contains specific details that might be valuable, critical, or sensitive.

5.0 Activity Monitoring

Physical Security Systems—Workers may be subject to electronic monitoring of their activities while on Impact premises. This monitoring is used to measure worker performance and to protect worker private property, worker safety, and Impact property. In areas where there is a reasonable expectation of privacy, such as bathrooms, dressing rooms, and locker rooms, no electronic monitoring will be performed.

Personal Effects and Private Communications—All personal effects brought to Impact premises are subject to search at any time without advance notice. Workers wishing to keep certain aspects of their personal life private must not bring related personal effects to Impact premises. To keep these matters private, workers must not communicate about such matters using Impact telephones, electronic mail systems, or other communications systems that may be monitored and which are intended to be used for business purposes only.

Use of Informants—From time to time, Impact uses informants who may be placed in various internal positions and who may appear to be the same as any other worker. Management has no obligation to notify workers about the presence of, or nature of the work performed by, such informants.

Pretext Requests—Impact believes that all business activities must be conducted in a forthright and honest manner. However, in certain circumstances authorized by the Director of Information Security, the organization may utilize investigators who pose as other persons in order to test customer service, test security policies, or investigate alleged wrongdoing.

6.0 Handling Personnel Information

Access to Own Personnel File—Upon written request to Human Resources, every worker must be given access to his or her own personnel file, once every six months as an active employee, and once each year after termination of employment for as long as the record(s) is maintained. Employees must be permitted to both examine and make one copy of the information appearing in their personnel file. If employees object to the accuracy, relevance, or completeness of information appearing in their personnel file, each year they may add a supplementary statement of up five pages that identifies the disputed information and explains your position, this document would then become a part of the personal record.

Disclosure to Third Parties—Disclosure of private information about Impact workers to third parties must not take place unless required by law or permitted by explicit consent of the worker. Impact must not disclose the names, titles, phone numbers, locations, or other contact particulars of its workers unless required for business purposes. Exceptions will be made when such a disclosure is required by law or when the involved persons have previously consented to the disclosure. The reason for termination of workers must not be disclosed to third parties. Two permissible exceptions are the prior approval of an Impact senior manager or if the disclosure is required by law. Every disclosure of private information to third parties must be recorded by the Human Resources department and these records must be maintained for at least five years.

Summary of Disclosures—If they request it, workers must be provided with a summary of all disclosures of their private information to third parties. In addition, workers must be given sufficient information to permit them to contact such third parties to rectify errors or supply additional explanatory information.

7.0 Private Information from Job Seekers

Gathering Unnecessary Information—Private information about a prospective employee may not be gathered unless it is both necessary to make an employment decision and also relevant to the job. This policy addresses marital status, family planning objectives, off-hours activities, political affiliations, performance on previous jobs, previous employers, credit history, education, and other personal details.

Credit and Background Checks—Whenever a credit report will be examined or a background check will be performed, prospective workers must provide a written release indicating their approval of the process. These prospective workers must be given an opportunity to withdraw their application for employment or contract work if they choose not to disclose such private information to Impact.

Permissible Tests—Candidates for a job with Impact must not be subjected to drug tests, AIDS tests, psychological tests, or other tests that may illuminate the candidates' lifestyle, political associations, or religious preferences. An exception may be made if this information is clearly needed to determine a candidate's suitability for a certain position.

8.0 Private Information about Customers

Consent For Collection Required—The collection of private information on prospects, customers, and others with whom Impact does business, is customary and expected. However, Impact workers must not collect private information from prospects or customers without having obtained their knowledge and consent.

Consent for Uses Required—Before a customer places an order or otherwise discloses private information, all Impact representatives must inform the customer about the ways that this private information will be used, and the third parties, if any, to whom the information will be disclosed.

Collection of Unnecessary Information—Impact workers or information systems must never require the provision of prospect or customer private information that is unnecessary for the provision of information, for the completion of a transaction, or for the delivery of products or services. No product or service provided by Impact may be denied to any person if they refuse to provide unnecessary private information. All disputes about necessary private information will be resolved by Impact's Chief Information Officer.

Opting Out From Unsolicited Contacts—Impact customers must be given an opportunity to inform Impact that they do not wish to be contacted through unsolicited direct mail, telemarketing, and related promotions. Impact staff must faithfully observe and act on these customer requests. Impact workers must diligently observe the unconditional right of individuals to block data about them from being included in mailing lists or calling lists, block the sale of data about them to third parties, and to have data about them erased from direct marketing lists.

Sharing of Customer Information—Impact does not disclose specific information about customer accounts, transactions, or relationships to unaffiliated third parties for their independent use, except under certain circumstances. These circumstances are limited to the disclosure of information to a reputable information reporting agency such as a credit bureau, when performing its own due diligence related to a customer's request to perform a certain action such as extend the amount of an existing line of credit, those circumstances when the customer requests the disclosure, the disclosure is required by or permitted by law, or the customer has been informed about the possibility of such a disclosure for marketing or similar purposes, and has been given an opportunity to decline.

Change of Business Structure—Should Impact go out of business, merge, be acquired, or otherwise change the legal form of its organizational structure, Impact may need to share some or all of its customer information with another entity in order to continue to provide products and services. If such a change and associated information transfer takes place, customers must be promptly notified.

Use of Outsourcing Organizations—Impact may outsource some or all of its information handling activities, and it may be necessary to transfer prospect and customer information to third parties to perform work under an outsourcing agreement. In all such cases, the third parties involved must sign a confidentiality agreement prohibiting them from further dissemination of this information and prohibiting them from using this information for unauthorized purposes.