USE OF CLIENT INFORMATION POLICY

Summary

IAG ("the Company") upholds the highest professional standards in confidentiality and compliance when managing client and third-party information and business best practices. We also ensure that the Insurers with which we place business are compliant through every step of the policy placement and management process.

Defining Information Assets

Information assets are comprised of the information created or used to support business activities at IAG as well as the information systems with which IAG processes information. This includes:

- All the electronic and non-electronic data and communications created or used to support business activities at IAG. Examples include paper documents, electronic files, voice communication, text messages and video images; and
- Information systems are all of the applications, devices and other systems with which IAG processes information. Examples include IAG telephones, fax machines, printers, computers, networks, voicemail, e-mail, instant messaging, cellular phones and other mobile devices.

Acceptable Use of Information Assets

Our information assets are comprised of the information created or used to support business activities at IAG as well as the systems with which our Company uses to process information. Our firm must protect these assets in order to ensure that they function properly and comply with regulatory, contractual and local law requirements. This policy establishes minimum requirements for the acceptable use of our information assets.

Scope of Information Asset Use

This policy applies to all colleagues of IAG as well as third-parties retained by our Company, such as vendors, independent contractors and consultants, who collect, use, disclose, transfer, retain, process, destroy (collectively referred to as "process") or otherwise have access to our information assets. All IAG information assets are the property of IAG and must be used appropriately. Only authorized individuals can process these information assets.

COLLEAGUE RESPONSIBILITIES

Avoiding Inappropriate Disclosure of Information

Colleagues are not permitted, during or after employment with IAG, to disclose non-public or confidential information to anyone, except as necessary to perform their specific job duties or as required by law. In addition, IAG colleagues must take reasonable care to ensure that non-public or confidential information is not inadvertently disclosed to anyone who does not have a need to know such information for IAG's business purposes. Colleagues must also comply with applicable IAG document retention policies and information classification and handling standards, as well as information security and data protection policies and procedures.

Colleague Access to Information Systems

The extent of colleague access to IAG information systems is limited to the requirements of each colleague's functional role. Colleagues must not seek out, view, read or listen to any information that they are not authorized to access. If colleagues seek access to our information systems or applications beyond their extended permissions, they must obtain proper authorization from their manager. Once a colleague is no longer employed by IAG, they are not permitted to access Company resources.

After a colleague's employment has been terminated by IAG, or at the Company's request, the colleague must return any tangible information systems or devices to their IAG manager. In addition, colleagues must not retain any IAG information or software upon returning information systems to the Company.

Preventing Unauthorized Access to Information Assets

Colleagues are not permitted to share passwords. Colleagues are required to safeguard passwords and not disclose them to others without legal or otherwise compulsory purposes for doing so. Desktop computers, laptops and all portable IAG devices must be encrypted or otherwise secured. Possession and use of tools for cracking, testing or bypassing security controls are prohibited. Colleagues are not permitted to establish network connections between external third parties and IAG information systems, except when authorized by their IAG manager.

All colleagues must be logged off of their information systems at the end of each day. They must lock their unattended IAG computers or other systems electronically using a password-protected screen saver or by manually locking the system display screen. All facilities and storage locations containing Company information must have appropriate physical security controls in place to prevent unauthorized access. In addition, unattended Company portable devices must be physically secured as appropriate (such as kept in a locked drawer, locked office or safe, or locked with a steel cable lock).

Appropriate Use of Information Systems

Without an authorized and legitimate business purpose, IAG colleagues are not permitted to use IAG information systems to view, receive or store inappropriate, offensive, vulgar or illegal materials or to transmit abusive, harassing, threatening, defamatory, misleading or personal politically motivated communications.

Colleagues are not permitted to change or in any way alter the hardware or software of IAG information systems or any authorized third party-connected systems unless it is for a legitimate business purpose and authorized by an IAG manager. The installation of software on IAG information systems must be performed only by authorized IT staff, who may remove any non-standard, unlicensed or unauthorized software detected on IAG information systems.

IAG colleagues must adhere to copyrights and license agreements associated with printed or electronic materials, software or other multimedia content at all times. On IAG premises, colleagues are not permitted to use devices capable of audio or video recording, whether personal or Company-owned, to capture images, audio, video or other media.

No Use of Unapproved External Systems

IAG colleagues are not permitted to store IAG information on any computer or other type of information system that is not owned or leased by the Company. Colleagues must not connect non-company equipment (for example, computers, portable devices or removable storage) into IAG networks or other systems.

All Company-retained communications must originate only from IAG information systems. When processing IAG information or otherwise conducting Company-related business, colleagues may not use the following communications systems:

- External electronic messaging systems;
- Unapproved external electronic forums, social networking sites and/or collaboration services; or
- External networks or file sharing services.

Messages from voicemail, e-mail or other messaging systems, are permitted only with proper authorization from an IAG manager.

Personal Use of Information Systems

IAG colleagues must exercise reasonable care and good judgement in their use of IAG information systems. Occasional personal use is acceptable unless limited by local policy, but that usage should not affect the colleague's performance or productivity. Colleagues must also ensure that their use of these resources does not in any way violate IAG's corporate compliance policies. In any personal use of IAG information systems, colleagues must not misrepresent their identity or that of the Company when communicating internally or to third parties or otherwise employ that IAG endorses a colleague's personal actions or statements.

MANAGEMENT RESPONSIBILITIES

Managers are responsible for communicating, and periodically reviewing, the requirements of this policy with colleagues and third parties under their supervision. Managers are also responsible for notifying the appropriate colleagues upon a change in the employment or job status of colleagues under management to ensure that access rights to IAG information systems are updated.

Third-Party Responsibilities

When IAG retains third parties that process or have access to our information, the colleague supervising the third party is responsible for contractually ensuring that the third party:

- Is in compliance with all applicable privacy and data security regulations set for by IAG compliance policies;
- Is notified of any necessary procedures issued pursuant to this policy; and
- Is reported immediately to an IAG manager in the event of an actual or suspected breach of data security (electronic or non-electronic) involving IAG information.

Information Breach Incident Reporting

IAG colleagues are required to immediately report to an IAG manager all incidents involving actual or suspected data loss, theft, unauthorized disclosure or inappropriate use of IAG information assets. IAG's

management will investigate the implications and significance of the incident and determine the Company's obligations to the client.

Policy Training and Enforcement

Mandatory colleague training related to this policy will be required by IAG and implemented with the hire of each new colleague.

Internal auditing procedures will be enforced on an annual basis, at minimum, to monitor colleague compliance with this policy and will report findings to IAG management, directors, and clients as appropriate.

Failure for colleagues, managers, directors or third parties of IAG may result in disciplinary action in accordance with local laws and/or internal procedures, up to and including termination of employment or contract for services.

For more information about our privacy policies and procedures, please contact our Compliance Officers:

Guy Bentley, President
Telephone: (416) 363-0072
Fax: (416) 363-0060
Email: gbentley@iagi.ca

Lori Bentley, Operations Manager
Telephone: (416) 363-0075
Fax: (416) 363-0060
Email: lbentley@iagi.ca