



Excerpt AGI Employee Handbook: AGI Code of Conduct

4. EMPLOYEE CODE OF CONDUCT

AGI is committed to high ethical standards. AGI leads by example and drives an ethical business culture in the industry. Our core values and code of conduct provide consistent guidelines for how to work with clients, each other, our communities, and our business partners.

We expect our employees to adhere to the same ethical principles. Our reputation is tantamount to our success, and our success is largely determined by our treatment of our employees, suppliers, and stakeholders.

AGI requires that employees comply with all applicable laws, rules, regulations, and standards within the geographies in which they operate.

GIFTS, GRATUITIES, BUSINESS EXPENSES, AND OFFERS OF EMPLOYMENT

AGI has established a reputation as a company with the highest standards of integrity and honesty. To maintain this reputation, AGI discourages any practice that may reflect unfavorably upon itself or its staff. As such, employees are prohibited from:

- 1) Offering gifts or gratuities of any kind to any individual or organization with whom AGI does business or is likely to do business;
- 2) Accepting gifts of any kind from any patron, tenant, concessionaire, vendor, supplier, or from anyone else with whom AGI does business or is likely to do business, or accepting payment in any form for any services rendered to anyone with whom AGI does business or is likely to do business;
- 3) Accepting cash discounts on merchandise or services obtained in any way connected with his/her or a co-worker's employment with AGI (except for discounts granted to employee organizations, other formal groups, or to "AGI Employees" as a generic classification).
- 4) Accepting any favors or any kind, including entertainment, meals, transportation, etc. either free or at reduced rates from any patron, tenant, concessionaire, vendor, or anyone else with whom AGI does business or is likely to do business;

5) Accepting payment or reimbursement for, or permitting payment to be made on their behalf, of any expenses that would constitute business expenses, whether or not reimbursable by AGI, that are incurred by such employee, including entertainment, meals, transportation, etc. from any patron, tenant, concessionaire, vendor, or anyone else with whom AGI does business or is likely to do business; and

6) Soliciting, demanding, accepting, or agreeing to accept from any patron, tenant, concessionaire, vendor, or anyone else with whom AGI does business or is likely to do business, an offer of employment, for the employee or for a member of the employee's immediate family, which offer of employment is related in any way to the performance of the public duties and responsibilities of the employee on behalf of AGI. This prohibition does not preclude consideration of the experience and expertise of an employee by a prospective employer.

EXPECTATIONS OF EMPLOYEES

Bribery and Corruption

Employees shall refrain from bribery or corrupt behavior. Employees shall not offer, promise, or accept any monetary or other advantage for the purpose of receiving a business benefit.

Environmental Management

AGI recognizes the importance of environmental preservation and encourages employees to engage in environmentally sound practices.

Freedom of Association and Non-Retaliation

Employees shall, in accordance with local legislation, have the right to associate and join trade unions. Employees' representatives shall not be discriminated against and shall not be subject to retaliation.

Freely Chosen Employment

Employees are employed of their own free will. No employee shall be forced to work beyond maximum hours, subject to threat, human trafficking, servitude, or involuntary prison labor.

Health and Safety

Employees shall be entitled to a safe, hygienic working environment that minimizes health and safety hazards.

Non-Discrimination

Employees shall not discriminate against any vendor, supplier, customer or co-worker on the basis of gender, religion, race, or any other protected category.

Working Hours

Employees shall uphold fair working conditions, and to the extent an employee is employed or engaged in any supervisory capacity, shall ensure that employees they supervise are paid in compliance with local legal requirements, at a minimum at the local industry rate or minimum wage stipulated by the country legislation, whichever is higher. Additionally, employees employed in any supervisory capacity shall ensure that the maximum working hours comply with national laws.

Respectful and Professional Conduct

Employees are expected to be respectful and professional to coworkers, customers, business partners, competitors and anyone else in contact with the Company. Employees are to act professionally and courteously in dealings with coworkers, customers, business partners, competitors and anyone else in contact with the Company. Rudeness or unprofessional behavior toward a coworker, customer, business partner, competitor or anyone else in contact with the Company is in violation of this policy. Insubordinate conduct will not be tolerated.

Threatening, intimidating, coercing or assaulting conduct toward fellow employees, customers, business partners, competitors, or visitors is strictly prohibited.

Employees are not permitted to disparage AGI's products or services. Employees are expected to cooperate with each other, management/supervisors, customers, and business partners in the performance of their work.

Employees who fail to maintain proper standards of conduct toward their work, their co-workers or the Company's customers, or who violate any of the Company's policies, are subject to appropriate disciplinary action, up to and including suspension without pay and termination of employment.

All instances of misconduct should be referred to the local or corporate Human Resources Department immediately.

5. ANTI-CORRUPTION POLICY

Introduction

Combating Corruption: AGI and its existing and future subsidiaries, (collectively, the "Company") operates in a wide range of legal and business environments, certain of which could pose challenges to our ability to conduct our business operations with integrity. As a company, we strive to conduct ourselves according to the highest standards of ethical conduct. Throughout its operations, the Company seeks to avoid even the appearance of impropriety in the actions of its managers, officers, employees, representatives and agents.

Rationale for Policy and Broad Interpretation: This Anti-Corruption Policy ("Policy") reiterates the Company's commitment to integrity, and sets forth the specific requirements and prohibitions applicable to our operations under various anti-corruption laws, including, but not limited to, the US Foreign Corrupt Practices Act of 1977 ("FCPA").

This Policy contains information intended to reduce the risk of corruption and bribery from occurring in the Company's activities. The Company strictly prohibits all forms of corruption and bribery and will take all necessary steps to ensure that corruption and bribery do not occur in its business activities.

While the concept of prohibiting corruption and bribery is simple, a better understanding of the applicable laws, including the FCPA, is essential as they can directly affect business interactions between the Company and third parties, including governments and government-owned or government-controlled entities. Under the FCPA, for example, it is illegal for U.S. persons, including U.S. companies or any companies traded on U.S. exchanges, and their subsidiaries, directors, managers, officers, employees, representatives and agents, to bribe non-U.S. government officials. Violations of the FCPA also can result in violations of other U.S. laws, including anti-money laundering, mail and wire fraud and conspiracy laws. The penalties for violating the FCPA are severe. In addition to being subject to the Company's disciplinary policies (including termination), individuals who violate the FCPA also may be subject to imprisonment and fines.

Aside from the FCPA, the Company also may be subject to other U.S. and non-U.S. anti-corruption laws, in addition to the local laws of the countries in which the Company conducts business. While this Policy generally sets forth the expectations and requirements for compliance with those laws, it is not intended to cover the specific provisions of every applicable law or be an exhaustive list of prohibited activities and practices. It is designed to assist parties in "doing the right thing." Parties should construe this Policy broadly and give effect to both the letter and the spirit of the Policy. This Policy should not prevent Company Personnel from conducting legitimate business with private parties or any government or government official, as long as they comply with the Company's policies and procedures and all applicable laws and regulations.

Applicability: This Policy is applicable to all of the Company's operations worldwide. This Policy applies to (i) all of the Company's managers, officers and employees and (ii) the Company's agents, consultants, joint venture partners and any other third-party representatives that have conducted business with, or on behalf of, the Company (collectively, "**Personnel**").

Prohibited Payments

Company Personnel are prohibited from directly or indirectly making, promising, authorizing or offering anything of value to any government official on behalf of the Company to secure an improper advantage, obtain or retain business, or direct business to any other person or entity. This prohibition includes payments to third-parties where Company Personnel knows, or has reason to know, that the third-party will use any part of the payment for bribes.

a) **Cash and Non-Cash Payments: "Anything of Value":** Prohibited payments may arise in a variety of settings and include a broad range of payments beyond the obvious cash bribe or kickback. For example, the FCPA prohibits giving "anything of value" for an improper purpose. This term is extremely broad and can include:

- (i) Gifts;
- (ii) Travel, meals, lodging, entertainment, or gift cards;

- (iii) Loans or non-arm's length transactions;
- (iv) Charitable or political donations; and
- (v) Business, employment, or investment opportunities.

b) **Government Official:** This term should be interpreted broadly to mean any official or employee of a government or public organization (including departments or agencies thereof), or a person acting in an official governmental capacity as well as employees of state-run or state-owned entities such as public utilities or schools, and shall specifically include under the FCPA:

- (i) Officers or employees of a non-U.S. government or any department, agency or instrumentality thereof;
- (ii) Officers or employees of a company or business owned in whole or in part by a non-U.S. government ("state owned or controlled enterprises");
- (iii) Officers or employees of a public international organization (such as the United Nations, World Bank or the European Union);
- (iv) Non-U.S. political parties or officials thereof;
- (v) Candidates for non-U.S. political office; and
- (vi) Anyone acting on behalf of any of the above.

On occasion, a government official may attempt to solicit or extort improper payments or anything of value from Company Personnel. Anyone so solicited must inform the government official that the Company does not engage in such conduct and immediately report the incident to AGI's Chief Operating Officer.

c) **Commercial Parties:** Bribery involving commercial (e.g., non-governmental) parties also is prohibited under this Policy. To this end, Company Personnel shall not offer, promise, authorize the payment of, or pay or provide anything of value to any person, employee, agent, or representative of another company to induce or reward the improper performance of any function or any business-related activity. Company Personnel shall not request, agree to receive, or accept anything of value from any person employee, agent, or representative of another company or entity as an inducement or reward for the improper performance of any function or business-related activity.

Permitted Payments

While it is important to remember that this Policy generally prohibits the payment, or provision of anything of value, to others if the purpose is to induce or reward the improper performance of any function or any business-related activity, the anti-corruption laws do permit, in certain very limited and unique situations, the making of what would otherwise be considered impermissible payments. For example, under the FCPA, there are three categories of these types of permitted payments:

d) **Facilitating Payments:** The FCPA includes a very limited and technical exception for nominal payments made to low-level government officials to ensure or speed the proper performance of a government official's routine, non-discretionary duties or actions, such as: (i) clearing customs, (ii) processing governmental papers such as visas, permits, or licenses, (iii) providing police protection, and (iv) providing mail, telephone, or utility services. Notwithstanding this statutory exception, it is the Company's policy that all such payments are

strictly prohibited except in very limited circumstances (e.g., imminent threats to health or safety). If you have a question about whether a certain payment represents a facilitation payment, encounter a demand for a facilitation payment, or you suspect one has been made, please contact the AGI Chief Operating Officer immediately.

e) Promotional Hospitality and Marketing Expenses or Pursuant to a Contract: The Company may be permitted to pay for the reasonable cost of a non-U.S. government official's meals, lodging or travel if, and only if, the expenses are bona fide, reasonable, and directly related to the promotion, demonstration or explanation of Company products or services, or the execution of a contract with a non-U.S. government or agency. Again, any question as to whether a payment might fall within this category should be presented to the AGI Chief Operating Officer for approval.

f) Promotional Gifts: Promotional gifts of nominal value may be given to a non-US government official as a courtesy in recognition of services rendered or to promote goodwill. Personnel should seek prior approval of any such gift from the AGI Chief Operating Officer, and all such gifts must be nominal in value and should generally bear the trademark of the Company or one of its products.

Political and Charitable Contributions

Contributions on behalf of the Company to candidates for political office are prohibited unless the AGI Chief Operating Officer pre-approves them in writing. Personnel are entitled to their own political views and activities, but they may not use Company resources to promote those views or associate their personal views with those of the Company.

As part of its corporate citizenship activities the Company may support local charities or provide sponsorship. Appropriate due diligence must be conducted on any proposed recipient charity, and charitable contributions or sponsorships must be pre-approved in writing by the AGI Chief Operating Officer.

Record Keeping

It is the Company's policy to implement and maintain internal accounting controls based upon sound accounting principles. All accounting entries in the Company's books and records must be timely and accurately recorded and include reasonable detail to fairly reflect its transactions. These accounting entries and the supporting documentation must be periodically reviewed to identify and correct discrepancies, errors, and omissions. With regard to compliance with anti-corruption laws in particular:

g) Authorization for Transactions: All transactions involving the provision of anything of value to any government official must occur only with appropriate Company authorization.

h) Recording Transactions: All transactions involving the provision of anything of value to a government official must be timely and accurately recorded in the Company's books.

i) **Tracking Transactions:** All transactions involving the provision of anything of value to a government official must be tracked in a separate log or record, with supporting documentation identifying:

- (i) The names and positions of the Personnel requesting and authorizing the transaction.
- (ii) The name and position of the government official involved in the transaction.
- (iii) A description, including the value, of the payment or provision of anything of value, and where applicable, a description of the Company's products or services being promoted or the relevant contractual provision if the payment was made pursuant to a contract.

Other Financial Policies (Money Laundering, Tax Evasion, Exchange Controls)

As part of, and in addition to, the record keeping requirements referred to above, the Company is committed to: (i) conducting its business transactions in an open and transparent manner; (ii) maintaining financial books, records and accounts that accurately, fairly and reasonably reflect such transactions; and (iii) complying with all applicable laws, rules and regulations, including those governing money laundering, tax evasion and exchange controls. Therefore, all Personnel must maintain financial and other records which accurately reflect Company transactions and transactions with others on the Company's behalf. Suspicious transactions without prior approval are prohibited, including any transactions that might appear to involve money laundering, tax evasion or exchange control violations.

Money laundering is a generic term used to describe the process of hiding the criminal origins of money or money's worth (*i.e.*, the proceeds of crime) within legitimate business activities and transactions. Tax evasion is the process of improperly concealing taxable funds from taxing authorities such as the Internal Revenue Service for the purpose of avoiding taxes. Exchange controls are laws governing how foreign or domestic currency can be exchanged in a particular jurisdiction. Company Personnel are routinely trained to comply with procedures outlined by the Bank Secrecy Act (BSA) and the reporting of instances of suspicious activity as mandated by the Financial Crimes Enforcement Network (Fin CEN). The following transactions may give rise to suspicions regarding money laundering, tax evasion or exchange control violations:

- (i) Transactions involving unknown parties or conducted through unknown or unnecessary intermediaries;
- (ii) Transactions involving abnormal, unexplained or unnecessary transactions or settlement methods;
- (iii) Transactions using shell companies and/or companies in tax havens or jurisdictions known for money laundering activities;
- (iv) Cash transactions or transactions using bank drafts, money orders or cashier's checks;
- (v) Transactions involving payments sent to a country other than the country where the transaction is taking place or the services are being performed; and

- (vi) Transactions involving payments to persons or companies who are not directly related to the transaction or the services performed.

Personnel are prohibited from engaging in transactions on the Company's behalf of the type listed above without prior written approval from the AGI Chief Operating Officer, and only in very limited cases where there is an identifiable legitimate business need for the transaction.

Cooperation with Auditors, Investigators and Law Enforcement

The Company may at times undertake a more detailed review of certain transactions. To ensure that the Company can properly monitor compliance with this Policy, all Personnel must be honest, accurate and transparent when responding to requests for information from the Company's internal and external auditors regarding relevant transactions and from the Company's personnel and advisors investigating allegations of potential misconduct. Potential violations of this Policy may also be investigated by law enforcement or other regulatory authorities. Any oral or written requests for information from any law enforcement body or any other regulatory authority should be referred immediately to the AGI Chief Operating Officer. The Company will cooperate fully with all law enforcement and regulatory authorities having legitimate grounds to request information. Any failure by Personnel to cooperate in an internal or external review will be viewed by the Company as a breach of your obligations to the Company, and will be dealt with in accordance with Company policy and any local laws or regulations.

Compliance; Reporting; Questions

Company Personnel must be familiar with and perform their duties according to the requirements set out in this Policy. Company Personnel who violate this Policy are subject to disciplinary action, up to and including termination of employment. Third-party representatives who violate this Policy may be subject to termination of all commercial relationships with the Company.

Any Personnel who suspect that this Policy may have been violated immediately must notify the AGI Chief Operating Officer. Anyone who, in good faith, reports suspected legal, ethical or Policy violations will not suffer any adverse consequence for doing so. When in doubt about the appropriateness of any conduct, the Company requires that Personnel seek additional guidance before taking any action that may subject the Company to potential liability.

Personnel with any questions relating to this Policy, its interpretation or its application, should contact AGI's Chief Operating Officer.

6. ANTI-NEPOTISM POLICY

Members of an employee's immediate family will be considered for employment with the Company on the basis of their qualifications. Except for employees already employed by the Company, immediate family may not be hired if employment would:

- (i) Create a supervisor/subordinate relationship with a family member;
- (ii) Have the potential for creating an adverse impact on work performance; or

- (iii) Create either an actual conflict of interest or the appearance of a conflict of interest.

This policy must also be considered when assigning, transferring, or promoting an employee. For the purpose of this policy, immediate family includes: spouse, parent, child, sibling, in-law, aunt, uncle, niece, grandparent, grandchild, and members of household. This policy also applies to persons involved in romantic relationships.

Employees who become immediate family members or establish a romantic relationship may continue employment as long as it does not involve any of the above. If one of the conditions outlined should occur, attempts will be made to find a suitable position within the Company to which one of the employees will transfer. If employees become immediate family members or establish a romantic relationship, the Company will make reasonable efforts to assign job duties so as to minimize problems of supervision, safety, security or morale. If accommodations of this nature are not feasible, the employees will be permitted to determine which of them will resign. If the employees cannot make a decision, the Company will decide in its sole discretion who will remain employed.

7. ROMANTIC OR SEXUAL RELATIONSHIPS

Consenting “romantic” or sexual relationships between a supervisor/manager and an employee may at some point lead to unhappy complications and significant difficulties for all concerned — the employee, the supervisor/manager and the Company. Any such relationship may, therefore, be contrary to the best interests of the Company.

Accordingly, the Company strongly discourages such relationships and any conduct (such as dating between a supervisor/manager and an employee) that is designed or may reasonably be expected to lead to the formation of a “romantic” or sexual relationship.

By its discouragement of romantic and sexual relationships, the Company does not intend to inhibit the social interaction (such as lunches or dinners or attendance at entertainment events) that are or should be an important part or extension of the working environment; and the policy articulated above is not to be relied upon as justification or excuse for a supervisor’s/manager’s refusal to engage in such social interaction with employees.

If a romantic or sexual relationship between a supervisor/manager and an employee should develop, it shall be the responsibility and mandatory obligation of the supervisor/manager to promptly disclose the existence of the relationship to the employee’s department head. The employee may make the disclosure as well, but the burden of doing so shall be on the supervisor/manager. Failure to disclose the existence of the relationship, in accordance with this policy, may lead to discipline up to and including termination of employment.

The Company recognizes the ambiguity of, and the variety of meanings that can be given to the term “romantic.” It is assumed, or at least hoped, however, that either or both of the parties to such a relationship will appreciate the meaning of the term as it applies to either or both of them and will act in a manner consistent with this policy.

The department head shall inform the Company's corporate Human Resources Department and others with a need-to-know, of the existence of the relationship, including in all cases the person responsible for the employee's work assignments.

Upon being informed or learning of the existence of such a relationship, the Company's corporate Human Resources Department may take all steps that it, in its discretion, deems appropriate. At a minimum, the employee and supervisor/manager will not thereafter be permitted to work together on the same matters (including matters pending at the time disclosure of the relationship is made), and the supervisor/manager must withdraw from participation in activities or decisions (including, but not limited to, hiring, evaluations, promotions, compensation, work assignments and discipline) that may reward or disadvantage any employee with whom the supervisor/manager has or has had such a relationship. If in a direct or indirect reporting relationship, the team member will need to be re-assigned.

In addition, and for the Company to deal effectively with any potentially adverse consequences such a relationship may have for the working environment, employees who believes they have been adversely affected by such a relationship, notwithstanding its disclosure, should make their views about the matter known to the COO or the Director of Human Resources.

This policy shall apply without regard to gender and without regard to the sexual orientation of the participants in a relationship of the kind described.

8. VIOLENCE IN THE WORKPLACE

The Company strongly believes that all employees should be treated with dignity and respect. Acts of violence will not be tolerated. Any instances of violence must be reported to the employee's supervisor and/or the local or corporate Human Resources Department. All complaints will be fully investigated.

The Company will promptly respond to any incident or suggestion of violence. Violation of this policy will result in disciplinary action, up to and including suspension without pay and/or immediate termination of employment.

Contraband

To maintain the safety and security of its employees and guests, the Company prohibits the possession of weapons in its buildings; in Company vehicles; or while conducting Company business, including on customer or airport property/premises. Under no circumstances shall any firearms be brandished or carried by employees on their person on Company, customer, or airport property, unless otherwise permissible in accordance with applicable state law.

Examples of banned weapons include but are not limited to handguns, stun guns, knives, mace, pellet guns, rifles, batons, and blackjacks.

9. WORKPLACE SAFETY

It is the responsibility of each employee to conduct all tasks in a safe and efficient manner complying with all local, state, and federal safety and health regulations and program standards, and with any special safety concerns for use in a particular area or with a customer.

Although most safety regulations are consistent throughout each department and program, all employees are responsible for identifying and familiarizing themselves with the emergency plan for their work area. Each facility shall have an emergency plan detailing procedures in handling emergencies such as fire, weather-related events, and medical crises.

It is the employee's responsibility to complete an Accident and Incident Report for each safety and health infraction that occurs by or that the employee witnesses. Failure to report such an infraction may result in employee disciplinary action, including termination of employment.

Furthermore, the Company requires that employee assumes the responsibility of individual and organizational safety. Failure to follow Company safety and health guidelines or engaging in conduct that places employees, customers or Company property at risk can lead to disciplinary action, up to and including termination of employment.

The Safety Committee shall have the responsibility to develop and the authority to implement the safety and health program in the interest of a safer work environment.

10. WORKPLACE INJURIES

Maintaining a safe work environment requires the continuous cooperation of all employees. The Company strongly encourages employees to communicate with their coworkers and their supervisors regarding safety issues.

Employees who sustain a work-related injury must immediately notify their department supervisor and the local or corporate Human Resources Department, no later than the end of the employee's work shift.

All employees will be provided care, first-aid and emergency service, as required, for injuries or illnesses while on the Company premises. Employees should contact their supervisors, the nearest supervisor, and/or 911 in the event of an accident or emergency. Emergency services will be contacted, when appropriate.

For any non-critical injury, employees will be required to complete the following injury process:

- The employee and the witness will be asked to complete a statement providing details on how the injury occurred.
- The employee may be asked to submit to a post-injury drug/alcohol test if there is a reasonable possibility that drugs or alcohol may have been a contributing factor in the injury.
- The employee and their supervisor will seek assistance from a triage service to determine whether immediate medical care is recommended or whether self-care is sufficient.

If you are referred to a clinic or doctor, you will be provided with paperwork that outlines AGI's modified duty/return to work program. You are expected to provide this paperwork to the clinic/doctor.

You are required to provide your local manager with any and all documents from your medical visit within 48 hours. You are expected to make all follow-up medical appointments and keep AGI updated on your progress. Make every attempt to schedule appointments on your scheduled time off from work. AGI will provide modified duty assignments to you as part of your return-to-work program, if necessary. These duties may be at times other than your normal shift times, and may include duties that are different from those you typically perform. You are expected to work within the limitations of those modified duties.

Failure to report accidents is a serious matter as it may preclude an employee's coverage under Workers' Compensation Insurance.

11. WORKPLACE SECURITY

The warehouses are "bonded" or secured for the protection of customs-controlled merchandise. Our employees must pass rigid Airport, TSA, and US Customs certification tests and screening to be allowed to conduct business within the warehouse.

It is every employee's responsibility to question anyone of unknown status within the warehouse. The warehouses are full of valuable and desirable merchandise and the temptation to steal is strong and constant. Anyone who steals will be terminated from employment and prosecuted. NO EXCEPTIONS!

Personal bags, including but not limited to briefcases, handbags, purses, lunch bags and lunch boxes, are not permitted in work areas, unless an employee's supervisor provides prior authorization.

12. SOLICITATIONS, DISTRIBUTIONS, AND USE OF BULLETIN BOARDS

Employees may not solicit any other employee during working time, nor may employees distribute literature in work areas at any time. Under no circumstances may an employee disturb the work of others to solicit or distribute literature to them during their working time.

Persons not employed by AGI may not solicit AGI employees for any purposes on Company premises.

Bulletin Boards

Bulletin boards maintained by AGI are to be used only for posting or distributing material of the following nature:

- notices containing matters directly concerning Company business; or
- announcements of a business nature which are equally applicable and of interest to employees.

All posted material must have authorization from the local Human Resources Department. All employees are expected to check these bulletin boards periodically for new and/or updated information and to follow the rules set forth in all posted notices. Employees are not to remove material from the bulletin boards.

13. COMPUTER SYSTEMS POLICY

The computer hardware, software, electronic mail, voice mail and other computer or electronic communication or data storage systems ("Computer Systems") are the property of AGI. Every AGI employee is responsible for using the Computer Systems properly and in accordance with this policy. Any questions about this policy should be addressed to the local or corporate Human Resources Department.

Generally, the Computer Systems are to be used for Company business purposes only, and use of the Computer Systems for personal purposes is prohibited.

All communications and information transmitted by, received from, or stored in the Computer Systems are Company records and property of AGI.

No Expectation of Privacy

Employees have no right of personal privacy in any matter stored in, created, received, or sent over the Computer Systems. The Company has the right, but not the duty, to monitor any and all of the aspects of its Computer Systems, including, without limitation, reviewing documents created and stored on its Computer Systems, deleting any matter stored in its Computer Systems in violation of policy (including, without limitation, its e-mail, texts, database and word processing systems), monitoring sites visited by employees on the Internet, monitoring chat and news groups, reviewing material downloaded or uploaded by users to the Internet, and reviewing e-mail sent and received by users. Further, the Company may exercise its right to monitor its Computer Systems for management reasons to ensure compliance with policy and without the permission of any employee. Employee use of the Company's Computer Systems constitutes consent to all the terms and conditions of this policy.

Even if employees use a password to access any of the Company's Computer Systems, the confidentiality of any message stored in, created, received, or sent from the Computer Systems still cannot be assured. Use of passwords or other security measures does not in any way diminish AGI's rights to access materials on its systems or create any privacy rights of employees in the messages and files on the systems. Any password used by employees must be revealed to AGI as files may need to be accessed by the Company in an employee's absence for business or management reasons.

Employees should be aware that deletion of any electronic messages or files will not truly eliminate the messages from the system. Electronic messages and files are stored on a central back-up system in the normal course of data management.

Professional Use of Computer Systems Required

AGI's policies against discrimination and harassment, sexual or otherwise, apply fully to its Computer Systems, and any violation of those policies is grounds for discipline up to and including termination of employment. Therefore, no e-mail messages should be created, sent, or received if they contain intimidating, hostile, or offensive material concerning race, creed, color, gender/sex, pregnancy, religion, national origin, citizenship status, ancestry, ethnicity, age, marital status, disability, sexual orientation, gender identity, transgender status, genetic information, military service or any other classification protected by law. Similarly, material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory or otherwise unlawful, inappropriate, offensive (including offensive material concerning race, creed, color, gender/sex, pregnancy, religion, national origin, citizenship status, ancestry, ethnicity, age, marital status, disability, sexual orientation, gender identity, transgender status, genetic information, military service or other characteristic protected by law) may not be downloaded from the Internet or displayed or stored in the Company's Computer Systems. Employees encountering or receiving this kind of material should immediately report the incident to the Director of Information Technology.

The Company may (but is not required) to use software to identify inappropriate or sexually explicit Internet sites. Such sites may be blocked from access by Company networks. Notwithstanding the foregoing, the Company is not responsible for material viewed or downloaded by users from the Internet. The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. In addition, having an e-mail address on the Internet may lead to receipt of unsolicited e-mail containing offensive content. Users accessing the Internet do so at their own risk. Employees who encounter inappropriate or sexually explicit material while browsing on the Internet should immediately disconnect from the site, regardless of whether the site was subject to Company blocking software.

The Computer Systems may not be used to solicit for religious causes, commercial enterprises, or other non-job related solicitations that do not concern terms and conditions of employment.

The Computer Systems shall not be used to send (upload) or receive (download), trade secrets, non-public proprietary financial and other Company information, or similar confidential business information of AGI or AGI's customers without prior authorization from AGI management. Employees, if uncertain about whether certain information is a trade secret, proprietary, or otherwise inappropriate for transfer, should resolve all doubts in favor of not transferring the information and consult the Director of Information Technology.

When using the Computer Systems, employees must respect all copyright and other intellectual property laws. For AGI's protection as well as the employee's protection, it is critical that employees show proper respect for the laws governing copyright, fair use of copyrighted material owned by others, trademarks and other intellectual property, including the Company's own copyrights, trademarks and brands.

Even though AGI has the right to retrieve and read any e-mail and text messages, those messages should still be treated as confidential by other employees and accessed only by the sender and intended recipient(s). Employees are not authorized to retrieve or read any e-mail messages that

are not sent by, or sent or otherwise provided to, them. Any exception to this policy must receive the prior approval of AGI management.

Employees are reminded to be courteous to other users of the Computer Systems and always to conduct themselves in a professional manner. E-mails and texts, in particular, are sometimes misdirected or forwarded and may be viewed by persons other than the intended recipient.

Limitations on Internet Use

Although AGI recognizes that the Internet may have useful applications to AGI's business, employees may not engage in Internet use (including but not limited to accessing social media sites) without prior written approval from the Director of Information Technology, and unless a specific business purpose requires such use. Absent such approval, employees may not access the Internet using AGI's computer systems, at any time or for any reason. Even when Internet access is approved, "Surfing the Net," playing games, or downloading entertainment software, including wallpaper and screen savers, are not legitimate business activities.

Management approval is required before anyone can post any information on commercial on-line systems or the Internet using the Company's Computer Systems. Any approved material that is posted should contain all proper copyright and trademark notices. Absent prior approval from AGI to act as an official representative of AGI, employees posting information must include a disclaimer in that information stating, "Views expressed by the author do not necessarily represent those of AGI." Without the express permission of their supervisors, employees may not send unsolicited e-mail to persons with whom they do not have a prior relationship.

Maintaining and Securing the Systems

Users should routinely delete outdated or otherwise unnecessary e-mails, voice mails and computer files. These deletions will help keep the Computer Systems running smoothly and effectively, as well as minimize maintenance costs.

To ensure security and to avoid the spread of viruses, employees accessing the Internet through a computer attached to the Company's network must do so through an approved Internet firewall. Accessing the Internet directly by modem is strictly prohibited unless the computer being used is not connected to the Company's network.

In addition, files obtained from sources outside the Company, including disks brought from home; files downloaded from the Internet, news groups, bulletin boards, or other online services; files attached to e-mail; and files provided by customers or vendors may contain dangerous computer viruses that may damage the Computer Systems. Employees should never download files from the Internet, accept e-mail attachments from outsiders, or use disks from non-Company sources without first scanning the material with Company-approved virus checking software. If an employee suspects that a virus has been introduced into the Company's Computer Systems, the employee must notify the IT Department immediately.

Violations of Policy

Any employee who discovers misuse of any of the Computer Systems in violation of this policy should immediately contact the Director of Information Technology.

Violations of this policy may result in disciplinary action up to and including suspension without pay and termination of employment.

AGI reserves the right to modify this policy at any time, with or without notice.

Employees are required to sign a Computer Systems Policy Acknowledgment Form as a condition of employment. The form is to be signed on acceptance of an employment offer by AGI.

14. PERSONAL EMAIL AND CELL PHONE USE FOR COMPANY NOTIFICATIONS

The Company uses Workday to communicate with employees. Workday can be accessed through an application on a smart phone or through a web browser. Employees who have not been assigned a Company email address may use their personal e-mail address to create an account with Workday. Once an account is created, the Company strongly encourages employees to download the Workday application to their Company provided and/or personal cell phones and sign up to receive Workday notifications via text message and/or email so that employees can be kept apprised of any job-related updates without having to log in to Workday. Employees, of course, have the option to opt out of receiving text messages or e-mail alerts to their personal cell phones or e-mail accounts. The Company will reimburse employees for personal use of their cell phones when required by applicable state law.

15. SOCIAL MEDIA POLICY

At AGI, we understand that social media can be a fun and rewarding way to share your life and opinions with family, friends and co-workers around the world. However, use of social media also presents certain risks and carries with it certain responsibilities. To assist you in making responsible decisions about your use of social media, we have established these guidelines for appropriate use of social media. This policy applies to all employees of AGI.

Guidelines

In the rapidly expanding world of electronic communication, social media can mean many things. Social media includes all means of communicating or posting information or content of any sort on the Internet, including to one's own or someone else's web log or blog, journal or diary, personal website, social networking or affinity website, web bulletin board or a chat room, whether or not associated or affiliated with AGI, as well as any other form of electronic communication.

The same principles and guidelines found in AGI's policies apply to employee activities online. Ultimately, each employee is solely responsible for what the employee posts online. Before creating online content, employees should consider the risks and rewards that are involved. Employees should keep in mind that any conduct that adversely affects job performance, the

performance of fellow employees or otherwise adversely affects customers, suppliers, people who work on behalf of AGI or AGI's legitimate business interests may result in disciplinary action, up to and including termination of employment.

Know and Follow the Rules

Employees should carefully read these guidelines and all of the Company's employee policies to ensure postings are consistent with these policies. All of the Company's policies apply to use of social media regardless of whether the employee is engaged in social media during working time, on the Company's premises and/or through the employee's own equipment. In particular, please remember that the Company's anti-harassment and non-discrimination policies govern employee use of social media. Inappropriate postings that include discriminatory remarks, harassment, and threats of violence or similar inappropriate or unlawful conduct will not be tolerated and may subject you to disciplinary action, up to and including termination of employment.

Be Respectful

Employees should always be fair and courteous to fellow employees, customers, suppliers or people who work on behalf of the Company. Also, employees should keep in mind that work-related complaints are more likely to be resolved by speaking directly with co-workers or by utilizing our Open Door Policy than by posting complaints to a social media outlet.

Nevertheless, if employees decide to post complaints or criticism, they must avoid using statements, photographs, video or audio that reasonably could be viewed as malicious, obscene, threatening or intimidating, that disparage customers, co-employees, or suppliers, or that might constitute harassment or bullying. Examples of such conduct might include offensive posts meant to intentionally harm someone's reputation or posts that could contribute to a hostile work environment on the basis of race, sex, disability, religion or any other status protected by law or Company policy.

Be Honest and Accurate

Employees should always be honest and accurate when posting information or news. Mistakes should be corrected quickly. Employees should be open about any previous posts that have been altered. The Internet archives almost everything; therefore, even deleted postings can be searched. Employees should never post any information or rumors that are known to be maliciously false about AGI, fellow employees, suppliers, vendors, people working on behalf of AGI or competitors.

Post Only Appropriate and Respectful Content

Employees must maintain the confidentiality of the Company's business information. Employees should not disclose personal information about employees, customers, business partners or third parties that the employee creates, receives or becomes aware during employment. Employees must not disclose the Company's trade secret, confidential proprietary or privileged information or attorney-client privileged information. Trade secrets may include information regarding the

development of systems, processes, know-how and technology. Employees must not post internal reports, policies, procedures or other internal business-related confidential communications.

Employees must respect financial disclosure laws. It is illegal to communicate or give a “tip” on inside information to others so that they may buy or sell stocks or securities. In addition, employees must respect all copyright and other intellectual property laws. It is essential that employees comply with all laws governing copyright, fair use of copyrighted material, trademark and other intellectual property.

Employees may not create a link from any personal blog, website or other social networking site to the Company website without identifying themselves as employees of AGI.

Employees should only express their personal opinions. Employees may not post anything in the name of AGI or in a manner that could be attributed to the Company without prior written authorization from the Human Resources Department. Without such authorization, employees may never represent themselves to be spokespersons for AGI. If AGI is a subject of the content the employee is creating, the employee must be clear and open about the fact that the employee works for AGI and make clear that the employee’s views do not represent those of AGI, fellow employees, customers, suppliers or people working on behalf of AGI. If employees do publish a blog or post online that identifies them as employees of AGI or where the employee would be easily identifiable as working for the Company, related to the work the employee does or subjects associated with AGI, the employee must make it clear that the employee is not speaking on behalf of AGI. It is required to include a disclaimer such as “The postings on this site are my own and do not necessarily reflect the views of AGI.”

Using Social Media at Work

Employees must refrain from using social media while on working time or on equipment we provide, unless it is work-related, as specifically authorized by the employee’s supervisor. Without prior authorization, social media must be undertaken during non-working time in non-working areas and with equipment not provided by the Company. Employees may not use Company email addresses to register on social networks, blogs or other online tools utilized for personal use.

Retaliation is Prohibited

AGI prohibits taking negative action against any employee for reporting a possible deviation from this policy or for cooperating in an investigation. Any employee who retaliates against another employee for reporting a possible deviation from this policy or for cooperating in an investigation will be subject to disciplinary action, up to and including termination of employment.

Scope of this Policy

This policy does not restrict employee rights to engage in protected activity under the National Labor Relations Act or any other applicable federal, state or local law. This policy does not prohibit discussing or disclosing information regarding an employee’s own wages, terms and

conditions of employment or the wages, terms and conditions of employment of other employees. It also does not prohibit discussion about or criticism of AGI's labor and employment policies or treatment of employees. However, we suggest that employees may wish to bring any such issues to the attention of the employee's supervisor or another member of management for resolution.

16. USE OF MOBILE TELEPHONES AND RELATED DEVICES

Use of Personal Mobile Phones

Employees are prohibited from using personal mobile telephones and other wireless communication devices ("personal mobile phones") during working time. Employees may make personal calls on their personal mobile phones during their break periods while on non-working time but must keep their personal mobile phones on vibrate mode during working time.

Use of Mobile Phones While Operating a Vehicle

AGI is aware that many employees use mobile telephones and other wireless communication devices ("mobile phones") in carrying out their daily duties and responsibilities. AGI is also aware of the potential distractions that may arise when mobile phones are used by employees while operating a moving vehicle, such as a van, automobile or truck ("moving vehicle"). In keeping with its obligations under federal and state occupational health and safety laws, to maintain a safe and healthful workplace, and to minimize the safety risks for our employees, customers, passengers in moving vehicles, and the public at large, AGI has adopted the following policy with respect to the use by employees of mobile phones while operating a moving vehicle. This policy applies regardless of whether the employee is operating a company-owned vehicle, or the employee's own vehicle in the course of employment.

Definitions

For purposes of this policy, "use" of a mobile phone includes dialing, texting, e-mailing, talking or listening on a mobile phone.

"Hands-free" devices, include any attachment, add-on or addition to a mobile phone, whether or not permanently installed in the vehicle, that when used, allows the operator of the vehicle to maintain both hands (or prosthetic devices or aids in the case of a disabled person), on the applicable steering device of the vehicle (e.g., dash-mounted devices, handsets).

Policy

- Employees are required to familiarize themselves, and comply at all times, with the laws of the state/locality in which they work with respect to the use of mobile phones. For example, where a local law prohibits the use of a mobile phone by anyone operating a moving vehicle, employees are also prohibited by this policy from using a mobile phone.
- No employee is to engage in the use of a mobile phone while operating a motor vehicle while the vehicle is in motion, unless such mobile phone is equipped and used with a hands-free device. (The only exception to this policy is where a phone call is made in a bona fide

emergency, such as to call “911” or a similar emergency number (e.g., to call an ambulance, fire department, etc.)).

- Even with a hands-free device, mobile phone use should be kept to a minimum, conversations should be as brief as possible, and employees should refrain from making unnecessary calls. Where possible and, again, even with a hands-free device, mobile phone calls should be made when the vehicle an employee is operating is not in motion. Employees using mobile phones should always remember not to discuss confidential issues with others present who do not have a “need-to-know” such information, and that mobile phone “courtesy” should be practiced at all times, *i.e.*, when others are present, employees should not talk loudly or in a manner which could be offensive to others.
- Employees are prohibited from using an MP3 player or similar device requiring headphones while operating a vehicle.

The Company is also aware that many employees operate other vehicles in the course of their employment, including golf and other shuttle carts, forklift trucks, and the like. While this policy does not expressly prohibit the use of mobile phones while operating such equipment, the Company discourages such use, except where essential for the employee to perform the employee’s job duties.

Reimbursement for Company-issued mobile phone and hands-free device purchases shall be handled in accordance with the Company’s normal expense reimbursement policies. Employees should consult their supervisors or local Human Resources Department for details. Questions regarding this policy should be directed by employees to their supervisors, or local Human Resources Department.

Texting/E-mailing

Many mobile telephones are also equipped with the ability to text and e-mail. Employees are reminded that the Computer Systems Policy applies equally to the use of Company-issued mobile telephones and related devices.

17. EMPLOYER INFORMATION AND PROPERTY

The protection of AGI’s trade secrets, non-public proprietary company information or similar confidential business information of AGI or AGI’s customers, AGI’s property and all other Company assets are vital to the interests and success of AGI. No trade secrets, non-public proprietary company information or similar confidential business information of AGI or AGI’s customers or AGI’s property, including without limitation, documents, files, records, computer files, equipment, office supplies or similar materials (except in the ordinary course of performing duties on behalf of AGI) may, therefore, be removed from the Company’s premises. In addition, when an employee leaves AGI, the employee must return to the Company all AGI related information and property that the employee has in the employee’s possession, including without limitation, documents, files, records, manuals, information stored on a personal computer or on a computer disc, supplies, and equipment or office supplies. Violation of this policy is a serious

offense and will result in appropriate disciplinary action, up to and including termination of employment.

18. TELEPHONE SERVICE MONITORING PRACTICES – NOTICE TO EMPLOYEES

Except when prohibited by applicable law, telephone conversations with customers and others who call Customer Service Representatives (CSRs) on the incoming business lines may be monitored and/or recorded from time to time for CSR training, quality control, and other business purposes. This notice provides information to employees about monitoring and recording practices.

So that callers may be aware of the possibility of all monitoring and/or recording, all **monitoring** (other than by traditional, unmuffled “open mike” extensions) is preceded by a pre-recorded (or live) announcement over the phone to each caller, stating that “to assure service quality, calls are sometimes monitored and/or recorded.”

It is Company policy not to monitor or record any personal or confidential calls, except to the extent of determining the personal or confidential nature of such calls. The following practices are used to promote the privacy of all personal and confidential calls:

(1) The telephones on which CSRs receive calls on the outside line are not to be used for personal calls by CSRs or other company employees, because those phones are subject to monitoring. Other phones are available in the office to be used for any necessary personal calls.

(2) Telephones that may be monitored are customarily labeled or marked: “To assure service quality, calls are monitored.”

(3) Supervisors who conduct service monitoring should simply leave the line immediately if they monitor a call which for any reason seems to be personal or confidential in nature.

19. USE OF COMPANY EQUIPMENT AND COMPUTER SYSTEMS

The Company provides any supplies, uniforms, equipment, automobiles and materials necessary for employees to perform their jobs. These items are to be used solely for the Company’s purposes. Employees are expected to exercise care in the use of Company equipment and property and use such property only for authorized purposes. Loss, damages or theft of Company property should be reported at once. Negligence in the care and use of Company property may be considered grounds for discipline, up to and including termination of employment.

The Company’s equipment, such as telephone, postage, facsimile and copier machine, is intended to be used for business purposes. An employee may only use this equipment for non-business purposes in an emergency and only with the permission of a supervisor. Personal usage, in an emergency, of this or other equipment that results in a charge to the Company should be reported immediately to a supervisor or accounting so that reimbursement can be made.

Use of the Company Computer System

Generally, use of AGI's Computer Systems is limited to Company business purposes only, and use of Computer Systems for personal purposes is prohibited. Employees are strictly forbidden from installing software on the Company's Computer Systems. Further, this policy reaffirms that employees have no reasonable expectation of privacy with respect to any computer hardware, software, electronic mail or other computer or electronic means of communication or storage maintained by the Company, whether or not employees have private access or an entry code into the particular computer system. The Company reserves the right to monitor the use of its Computer Systems for business and management purposes to ensure compliance with policy.

(See also the Computer Systems Policy).

Use of Company Vehicles

Only employees with an unrestricted, current driver's license (and airport ID, if applicable) and who have adequate insurance coverage may operate AGI vehicles or use a vehicle to conduct AGI business. An employee operating a Company vehicle or a personal vehicle to conduct Company business must provide proof of adequate insurance to the local or corporate Human Resources Department. Company vehicles may only be used for authorized Company business. Any employee operating a Company vehicle must do so in a safe manner. Any employee operating a Company vehicle under the influence of drugs or alcohol or in an unsafe or negligent manner will be immediately terminated. The Company has the right to search any Company vehicle at any time. Therefore, employees have no reasonable expectation of privacy with respect to Company vehicles.

Telephone Use

Because a large percentage of our business is conducted over the phone, it is essential to project a professional telephone manner at all times.

Although AGI realizes that there are times when an employee may need to use the telephone for personal reasons, it is expected that good judgment will be used in limiting the length and frequency of such calls. Additionally, no long distance personal calls may be made on Company phones without prior approval from the employee's supervisor.

20. LEGAL CLAIM REPORTING AND LITIGATION HOLD POLICY

Purpose and Summary

Like other large companies, from time to time, AGI becomes involved in legal claims, administrative proceedings, or other kinds of legal disputes, as well as formal requests to produce records by subpoena or otherwise. These events are collectively referred to in this policy as "Claims." Once the Company is placed on notice of an actual or potential Claim, the Company has a legal obligation to preserve potentially relevant evidence.

It is the Company's policy to comply with all laws requiring the preservation of evidence. As part of that policy, the Company requires all AGI Personnel to take certain actions if they become aware of an actual or potential Claim involving the Company. As set forth more fully below, if any AGI Personnel become aware of such a Claim, the employee is required to do the following as soon as reasonably possible:

- a) Report the actual or potential Claim to the Legal Department in the manner set forth below; and
- b) Suspend any routine deletion or purging of Records (as defined below) and preserve all Records that in any way pertain to the actual or potential Claim in the manner set forth below.

Failure to follow any portion of this policy may result in discipline, up to and including termination of employment.

Definitions

The definitions set forth below shall apply to this policy. In applying these definitions, you should construe them broadly so as to err on the side of reporting Claims and preserving records.

Claim: shall mean any actual or potential legal claim, administrative proceeding, or other kind of legal dispute, or a formal request to produce records by subpoena or otherwise.

Records: means all paper records and electronic files, whether created at work or at home, including, but not limited to, any correspondence, electronic communications, e-mails (in your e-mail in-box, sent box, deleted box or folders), e-mail attachments, instant messages, text messages, voicemails, word processing documents, calendars, spreadsheets, PowerPoint presentations, databases, telephone logs, contact manager information, Internet usage files, charts, reports, agreements, memos, letters, records, graphs or tables, photographs, handwritten or typewritten notes, summaries, calendars, diaries, organizers, recordings, photographs, pictures, films, videotapes, telegrams, faxes, or other graphic, symbolic, recorded or written materials of any nature whatsoever. These records may exist in hard copy files, computer hard drives, removable media (e.g., thumb drives, CDs and DVDs), laptop computers, PDAs, servers, or potentially other locations.

Preserved Information: means all Records that may contain information that is potentially relevant to a Claim.

Legal Hold: means a directive to cease destruction of Records and preserve all Preserved Information.

AGI Personnel: means all officers, directors, executives, managers, employees or other agents of the Company.

Procedure for Reporting Actual or Potential Claims

Any AGI Personnel who become aware of an actual or potential Claim, through the receipt of notification, a demand letter, an administrative charge, a formal complaint, or other information

identifying the possibility of legal action, or upon service of a subpoena or other formal request for information, must notify the Director of Human Resources to disclose the Claim as soon as reasonably possible. The Director of Human Resources may be contacted at hdq-hr@cargoforceinc.com. The Legal Department will determine, among other things, how to respond to the Claim, determine whether to initiate a Legal Hold, and identify AGI Personnel who will be subject to the Legal Hold, if one is initiated.

Procedure for Preserving Records

In addition to the reporting obligation set forth in Section 3 above, any AGI Personnel who become aware of an actual or potential Claim must take action to broadly preserve all records that in any way pertain to the Claim as soon as reasonably possible, even before the Legal Department issues a Legal Hold Notice. The actions AGI Personnel must take include the following:

- a) Preserve any and all Records that pertain in any way to the subject matter of the actual or potential Claim;
- b) Suspend any automatic or routine Record deletion or purging practices to the extent necessary to preserve such Records;
- c) Suspend any automatic or routine reformatting, wiping, or deletion of any data storage devices, including, but not limited to, computer hard drives, that contain such Records;
- d) Refrain from altering, moving, copying, or resaving any such Records, as these actions can automatically alter certain parts of the files that may be important; and
- e) Continue safeguarding all such Records, or any new Records created or discovered after you first undertake the preservation efforts required by this policy, until you receive further written instructions from the Legal Department.

If you require assistance completing any of the foregoing requirements in response to an actual or potential Claim, or if you have any questions about these requirements, please contact the Director of Human Resources

Violations

Preservation of evidence is a legal requirement. If the Company unreasonably fails to timely take steps to preserve evidence in response to a Claim, the Company and the individual violating this policy may be subject to sanctions. Accordingly, the requirements of this policy must be implemented as soon as reasonably possible once you become aware of an actual or potential Claim. In addition, failure to comply with any portion of this policy may result in disciplinary action, up to and including termination of employment.

Duration of Legal Hold

Only the Legal Department can determine whether a Legal Hold is no longer necessary and determine when you are authorized to resume your regular routine Record deletion or purging

practices. All Legal Holds, whether initiated by the Legal Department or by you pursuant to this policy, shall remain in effect unless you are notified in writing by the Legal Department that the Legal Hold is no longer necessary.

Superseding Effect/Relation to Other Policies

Once you become aware of an actual or potential Claim, this policy is controlling and you must fully comply with the requirements set forth in this policy as soon as reasonably possible. This policy supersedes any other Company policy, procedure, guideline, rule, or other instruction with respect to the subject matter addressed herein.

Effective Date

This policy is effective immediately and shall apply to any actual or potential Claims about which you may have become aware either before or after the effective date of this policy.

21. REPORTING SUSPECTED VIOLATIONS OF LAW

The Company expects employees to conduct business according to the highest ethical standards of conduct. Any employee who believes that the Company is engaging in any activity that is in violation of a law, rule or regulation should report such concerns to either the COO or Director of Human Resources immediately.

Employee complaints will be thoroughly investigated and will be handled as discreetly as possible. Any person electing to utilize this complaint resolution procedure will be treated courteously, and the complaint will be handled as swiftly as possible. The Company will not retaliate against any employee who makes a good faith complaint. Retaliation will not be tolerated and must be reported to the Human Resources Department and/or the COO.

Employees are required to maintain strict confidentiality and refrain from discussing any information concerning a complaint or an investigation until the Company has completed its investigation. However, nothing precludes an employee from disclosing to any appropriate governmental agency an activity, policy or practice of the Company that is in violation of a law, rule or regulation, or from providing information to or testifying before any appropriate government agency or entity conducting an investigation or inquiry into an alleged violation. **Nothing in this policy is intended to interfere with an employee's rights under Section 7 of the NLRA.**

Further, an employee shall not be held criminally or civilly liable under any federal or state trade secret law for the disclosure of a trade secret that: (1) is made in confidence to a federal, state, or local government official, either directly or indirectly, or to an attorney, and made solely for the purpose of reporting or investigating a suspected violation of law; or (2) is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal. And, an employee who files a lawsuit for retaliation by an employer for reporting a suspected violation of law may disclose the trade secret to the attorney of the employee and use the trade secret information in the court proceeding, if the individual: (A) files any document containing the trade secret under seal; and (B) does not disclose the trade secret, except pursuant to court order.

22. INTERNAL INVESTIGATIONS AND SEARCHES

From time to time, AGI may conduct internal investigations pertaining to security, auditing or work-related matters. Employees are required to cooperate fully with and assist in these investigations if requested to do so, and are required to maintain strict confidentiality and refrain from discussing any information concerning a complaint or an investigation until the Company has completed its investigation. However, nothing in this policy is intended to interfere with an employee's rights under Section 7 of the NLRA.

Whenever necessary, in the Company's discretion, work areas (*i.e.*, desks, file cabinets, etc.) and personal belongings (*i.e.*, briefcases, handbags, clothing (including pockets), etc.) may be subject to a search without notice. Employees are required to cooperate.

The Company will generally try to obtain an employee's consent before conducting a search of work areas or personal belongings, but may not always be able to do so. Employees should expect no right to privacy.

23. ANTI-THEFT POLICY

AGI is committed to providing a safe workplace and to rigorously safeguarding the property of the traveling public, our employees, and our customers. AGI prohibits fraud and theft of any kind, and knowledge of fraud or theft occurring by others must be reported immediately. Fraud and theft harm the Company and employees, not just through monetary or material losses, but also through diminished trust and support.

Fraud, as defined by this policy, is an act of deception or misrepresentation. Examples include, but are not limited to, discount abuse, coupon fraud, misuse of promotion codes, falsification of AGI documents, and forgery.

Theft, as defined by this policy, is the unlawful taking of property with the intent to deprive the rightful owner of the property, including but not limited to the misuse or theft of confidential or proprietary information, theft of personal property, theft of services including without limitation airline upgrades, theft of customer property, failure to follow procedures causing loss of revenue to our customer, and theft of work time/wages.

If an employee has knowledge of or a concern regarding suspected fraud or theft activity, the employee must immediately report it to the employee's immediate supervisor, human resource generalist, manager, regional vice president, Company hotline, or Employee Services management at the corporate office. The information reported is to be kept as confidential as possible. An employee who reports theft may be eligible for a \$1,000 reward, depending upon the outcome of an investigation. If AGI later determines that an employee had knowledge of fraud or theft and did not report it, the employee may be subject to disciplinary action, up to and including termination of employment.

All reports of fraud and theft will be promptly investigated. All interviews conducted as part of the investigation will take place in a confidential environment and the individuals conducting the investigation will maintain appropriate confidentiality. An employee suspected of fraud or theft

may be placed on suspension, with or without pay, while the investigation is conducted. If the employee has been found to be in violation of this policy, the employee will not only be subject to disciplinary action, up to and including termination, but could be subject to criminal liability. In addition, AGI reserves the right to take any and all action necessary to recover any losses incurred as a result of the employee's actions, including deductions from the employee's final pay in accordance with and subject to applicable law.

AGI reserves the right to inspect AGI property when investigating reported and/or suspected employee fraud or theft. Employees should have no expectation of privacy in work areas, lockers, desks, or with respect to any property provided by AGI. In addition, AGI reserves the right to search any or all personal property brought onto AGI premises, including but not limited to packages, containers, briefcases, bags/purses, and other belongings in accordance with applicable law. Refusal or failure to cooperate with an AGI inspection or search may result in disciplinary action, up to and including termination of employment.

24. REFERENCE CHECKS

Should an employee receive a written request for a reference, the employee should refer the request to the local or corporate Human Resources Department for handling. No AGI employee may issue a reference letter to any current or former employee without the permission of the local or corporate Human Resources Department. Under no circumstances should any AGI employee release any information about any current or former AGI employee over the telephone. All telephone inquiries regarding any current or former employee of AGI must be referred to the local or corporate Human Resources Department.

We will respond to all reference check inquiries from others, by confirming only dates of employment and positions held. Salary verification will be provided subject to written authorization from the employee that also releases AGI from liability in connection with the furnishing of this information, or unless AGI is required by law to furnish such information. Inquiries must be in writing and will be responded to in writing.

25. NO SMOKING/TOBACCO USE POLICY

Consistent with applicable law, no person may smoke in any enclosed portion of the Company's offices or other enclosed building (including parking garages). This includes, without exception, common work areas, conference and meeting rooms, private offices, dining areas, restrooms, and all other enclosed facilities.

In addition, to protect and enhance our indoor and outdoor air quality and to contribute to the health and well-being of all employees and customers, unless we specifically designate an outdoor smoking area, our physical premises (inside and outside) are entirely smoke free.

This policy precludes the use of all forms of cigarettes or tobacco products, including cigars, pipes and chewing tobacco, on our premises (including the exterior of our premises). Consistent with the recommendation of the American Cancer Society, the American Heart Association, the American Lung Association and the Campaign for Tobacco-Free Kids, the use of e-cigarettes (also called vapor cigarettes) is precluded under this policy in the same manner as tobacco

cigarettes. The Company has implemented this policy due to the increased medical costs correlated with smoking and its concerns regarding employee wellness and productivity.

Employees are protected from retaliatory action or from being subjected to any adverse personal action for exercising or attempting to exercise the employee's rights under this policy. Any violation of this policy should be reported immediately to the local or corporate Human Resources Department. Violation of this policy may result in appropriate corrective action, up to and including suspension without pay and discharge.

26. TAPE RECORDING POLICY

It is a violation of AGI policy to record conversations with a tape recorder or other recording device unless all parties to the conversation give their consent.

The purpose of this policy is to comply with applicable law and to eliminate a chilling effect on the expression of views that may exist when one person is concerned that the employee's conversation with another is being secretly recorded. This concern can inhibit spontaneous and honest dialogue especially when sensitive or confidential matters are being discussed.

Violation of this policy will result in disciplinary action, up to and including suspension without pay and immediate termination of employment.

Nothing in this policy is intended to interfere with an employee's rights under Section 7 of the NLRA.