GREAT AMERICAN.
INSURANCE GROUP

Great American Insurance Group
Contingent Worker Definition

You have asked to be considered for a Contingent Worker assignment at Great American Insurance Company (GAIC), Great American Financial Resources, Inc (GAFRI) or a subsidiary company. . References to "Great American" include GAIC and GAFRI and subsidiaries. In order for you to be considered, you have to agree to our Contingent Worker Guidelines. Please read all of the information carefully. You will be required to sign acknowledgements in four places.

What is a Contingent Worker at Great American?

What does it mean to be a Contingent Worker (CW) at Great American? It means that you are here for a particular project or job, typically of a limited duration and are not a Great American employee. Some CWs are employees of other companies; others may be independent contractors; and some may be placed here through temporary or other staffing sources.

For legal and policy reasons, it's important that you know you are not a Great American employee. If you feel you are not properly classified as a CW, you need to contact a Corporate Human Resources Representative at 513-369-5052 immediately.

What You Should Know as a Contingent Worker

Since you are a CW, you (i) are not a Great American employee and (ii) are working on a limited, interim basis as a temporary, seasonal, contract, or leased worker.

You are being assigned to work at Great American for one or more of the following reasons:

- To fill in for a Great American employee who is on a leave
- To meet staffing needs (temporary increase in workload)
- To supplement the talent and expertise of the area or work group to which you are assigned
- To assist with the completion or implementation of a new or upgraded project, system or technology

Acknowledged: _____

Name: TATIREDDY THULASIRAM

Date: 28/06/2016

GREAT AMERICAN.
INSURANCE GROUP

Great American Insurance Group
Contingent Worker Guidelines

Your Employer's Responsibilities

If Great American has obtained your services from a company (e.g. temporary staffing, contract labor, consulting company) for whom you are an employee, your employer is responsible to you for the following:

- Hiring and termination processes and procedures, including background, drug, credit, criminal and other reports associated with your employment.
- Management of employment and administrative functions of your work assignments (including final approval for any paid time off).
- Manage all payroll activities for you, including taxes.
- Providing benefits as applicable.
- Conducting your performance evaluations.
- Ensuring you and on-site representatives (where applicable) sign appropriate Great American documentation.
- Providing all employment-related communications to you, except routine day-to-day instructions.
- Meeting all government requirements respecting employment practices.
- Handling all payment issues.
- Assigning your pay level or pay range.
- Recognizing and rewarding outstanding efforts.
- Tracking duration of assignment.
- Participating in your employer's social functions, celebrations and activities.

Independent Contractor

If you are not in an employment situation similar to the one described above, then you are an independent contractor. As such, you are responsible for all of the items list above.

Your Responsibilities

While providing services to Great American as a Contingent Worker, you will:

- Maintain the confidentiality of the work you are doing and the proprietary information you have access to, in accordance with a nondisclosure agreement that either you or your employer has signed. You will still be obligated to maintain this confidentiality after you are finished with your work here. This means that even when you are no longer providing services to Great American, you are still required to hold in confidence the Great American information you viewed or possessed during your assignment with us.
- Be required to read, understand and agree to certain Great American policies that apply to Contingent Workers, which have been or will be provided to you.
- Visibly display your Great American identification badge showing you to be an authorized Contingent Worker.
- Identify yourself in email communications/voicemail greetings as a Contingent Worker or state the name of your employer.
- Represent yourself as a Contingent Worker and will not represent yourself as a GAI employee to anyone internally or externally.
- Sign no documents on behalf of GAI.
- Sign no letters on company letterhead without clearly identifying yourself as a Contingent Worker.

When Your Great American Assignment is Concluded – Exit Procedures

When your Great American assignment is completed, you will be required to:

- Turn in your Great American CW facilities access card to your primary Great American contact while you were a CW.
- Notify the Great American person for whom you were doing the assignment so that your access to all systems can be terminated.
- Return all Great American property to the GAI person for whom you were doing the assignment.
- Maintain the confidentiality of Great American's systems and information even though your assignment has ended.

Workplace Harassment – Great American's "Zero Tolerance" Policy

As a Contingent Work at Great American, you are required to adhere to our Zero Tolerance Policy concerning workplace harassment.

What is Workplace Harassment?

At Great American, **Workplace Harassment** means:

ACTIONS, WORDS OR MATERIALS in the workplace that

(1) **RELATE TO SEX or**

(2) **PUT PEOPLE DOWN OR STEROTYPE THEM BASED ON ANY OF THE PROTECTECTED CLASSIFICATIONS** (described below)

What does "Zero Tolerance" mean?

At Great American, **Zero Tolerance** means NO **Workplace Harassment** will be tolerated.

In other words:
If it relates to sex or if it puts people down or makes them feel uncomfortable based on a **protected classification**, it is not allowed in our workplace.

What are the "Protected Classifications"?

The **Protected Classifications** are easy to remember because they are the same classifications that are protected by federal and state employment discrimination laws.

They are:
(1) **Sex**
(2) **Race**
(3) **Religion**
(4) **Nationality**
(5) **Age (40 or over)**
(6) **Physical and/or Mental Disability**

Workplace Harassment Includes

Based on these definitions, you can see that **Workplace Harassment** includes more than just sexual harassment. It also includes racial and religious harassment and harassment based on nationality, age and disability.

Workplace Harassment can take many different forms, including:

ACTIONS: touching, blocking someone's movement or interfering with his or her work, leering, stalking or assault.

WORDS: comments, jokes or slurs; unwelcomed sexual advances.

MATERIALS: emails, cartoons, posters, symbols.

What you HAVE TO DO if You Have a Complaint of Harassment

If you have a complaint of harassment, it is your responsibility to report such conduct immediately. You do not have the option of taking no action.

You are to call the ***confidential toll-free Great American Human Resources hotline at (877) 583-9138***

What Will Happen to Your Report of Harassment

Great American will investigate the circumstances of the complaint and, if an investigation confirms the allegations, the Company will take prompt, corrective action.

The Company will investigate all reports of harassment. The Company does not tolerate any form of harassment of its employees or those working here as a Contingent Worker, nor does it retaliate against those who truthfully report such harassment.

If you have any questions concerning this policy, you are to call the Great American Human Resources Hotline number of (877) 583-9138.

Violations of Zero Tolerance Policy

If you violate the policy, you will be subject to disciplinary action. Depending on the seriousness of the violation, the disciplinary action could include any of the following:

- Verbal counseling
- Written warning
- Suspension
- Reduction in the amount you are paid as a Contingent Worker
- Termination of your assignment as a Contingent Worker at Great American

Questions/Comments

If you have any questions or comments, you are to call the Great American Human Resources Hotline number of (877) 583-9138.

Drug-Free Workplace

Policy Statement

Great American (or the Company) is committed to maintaining a workplace free from the use and abuse of drugs and alcohol and has established the following policy in support of this commitment. Also, drug and alcohol testing practices have been adopted to identify Contingent Workers using drugs and/or alcohol.

Definitions

Illegal Drugs

"Illegal drugs" are drugs or controlled substances that are (i) not legally obtainable, or (ii) legally obtainable, but not obtained in a lawful manner, or (iii) it is a controlled substance.

Controlled Substances

These are chemical substances that are prescribed but not legally obtained or prescribed and not being used for the prescribed purposes.

Violations

Any Contingent Worker involved in any of the following activities at any time while on Company business, premises or using Company property, or at a Company-sponsored event is in violation of Company policy and subject to disciplinary action as defined in this policy:

- Bringing illegal drugs onto Company premises or property (property includes Company owned or leased vehicles) or the Company's agent's or customer's premises.
- Having possession of or being under the influence of illegal drugs.
- Using, consuming, transforming, distributing or attempting to distribute, manufacturing or dispensing illegal drugs.

The Company prohibits the use/being under the influence of alcohol on Company premises or while on personal time during the workday if the Contingent Worker expects to return to work. This includes meal and break times, whether in connection with business or not.

Contingent Workers are expected to practice moderation in the use of alcohol at Company-sponsored events or while on company business with agents, customers or in similar business situations.

A Contingent Worker must not be under the influence of alcohol while driving a Company owned or leased vehicle, whether on Company business or personal time.

A Contingent Worker must cooperate with or submit to questioning, medical or physical tests or examinations when requested or conducted by the Company or its designee, in applying this policy.

The use of Company property, including Company vehicles, or any other Company communication devices (beepers, telephones, etc.) or a Contingent Worker's position within the Company to make, transfer, sell, dispense, or traffic any drugs or alcohol are strictly prohibited.

Testing

The Company asserts its legal right and prerogative to test any Contingent Worker for drug and/or alcohol abuse. A Contingent Worker may be asked to submit to a medical examination and/or submit to urine, saliva, breath, and/or hair testing for drugs or alcohol. Blood tests may be used under post-accident, reasonable suspicion and return-to-duty testing. Any information obtained through such examinations may be retained by the Company and is the property of the Company.

In particular, the Company reserves the right, in its discretion and within the limits of federal and state laws, to examine and test for the presence of drugs and alcohol (as stated above) in situations such as, but not limited to, the following:

Post Assignment Offer - All offers of work assignments to a Contingent Worker will be made subject to the results of a drug test. A Contingent Worker will be required to submit to a test and sign a consent agreement that will release the Company from liability.

Post-Accident - An incident occurring while on Company business that results in injury (requiring medical treatment) to an employee or others and/or damage to Company property may require a drug and/or alcohol test, if allowed by federal and state law. Furthermore, any Contingent Worker involved in an accident while driving a Company owned or leased vehicle, in which the Contingent Worker was cited for a moving traffic violation, will require a drug and/or alcohol test, if allowed by federal and state law. The Contingent Worker may be suspended from his work assignment and will not be permitted to drive the Company owned or leased vehicle, pending the outcome of the test. A Contingent Worker is required to report the incident to his or her Great American contact immediately after the start of the next business day.

Reasonable Suspicion - A Contingent Worker may be asked to submit to a drug and/or alcohol test if reasonable suspicion exists to indicate that his or her health or ability to perform work may be impaired as determined by his or her manager (or other management designee) in consultation with an officer from Human Resources. Although reasonable suspicion testing does not require certainty, mere "hunches" are not sufficient to meet this standard. Therefore, a reasonable suspicion test will only be conducted after careful consideration, based on, but not limited to, the following documented observations that would cause the respective supervisor and the officer-in-charge to conclude that the Contingent Worker may be under the influence of drugs or alcohol:

- Sudden changes in work performance;
- Unexplained and/or frequent absenteeism;
- Personality changes or disorientation;
- Repeated failure to follow instructions or operating procedures;
- Violation of the Company's safety procedures;
- Odor of alcohol and/or residual odor peculiar to some chemical or drug;
- Discovery or presence of drugs or alcohol in a Contingent Worker's possession or near the Contingent Worker's workplace;
- Observable phenomena, such as direct observation of a drug use or possession and/or the physical symptoms of being under the influence;
- A pattern of abnormal conduct or erratic behavior;
- Conviction for violation of a criminal drug or alcohol statute;
- Conviction for a drug-related offense, or the identification of a Contingent Worker as the focus of criminal investigation into illegal drug possession, use or trafficking;
- Information provided either by reliable and credible sources or independently corroborated; or
- Evidence that the Contingent Worker had tampered with a previous drug test.

Any Contingent Worker believed to be under the influence of drugs or alcohol will be taken to the designated collection site and then immediately home. The Contingent Worker will be suspended pending the outcome of the test.

Any Contingent Worker refusing to consent to testing or violating any part of this policy will result in appropriate disciplinary action, up to and including termination of the Contingent Worker's work assignment, depending upon the severity of the situation.

Testing Procedures

The drug test will be performed from urine specimens collected at a qualified site. To determine alcohol levels, for all post-accident, reasonable suspicion and return-to-duty situations, a blood-alcohol test will be performed from blood drawn at the collection site. The collection site will take necessary steps to avoid any dilution or alteration of specimens. However, the test shall be conducted in a professional and sanitary manner with due regard for the individual's privacy, dignity and confidentiality. Proper handling of the specimens will be maintained so that the specimen results can be traced to the proper individual. A

secure, written chain-of-custody process will be implemented from the time of the collection of the specimen until the specimen is disposed of or secured in frozen long-term storage.

The urine or blood specimen will be analyzed by a professional laboratory, certified by the National Institute on Drug Abuse (NIDA), for the following substances:

- Alcohol
- Amphetamines (amphetamine, methamphetamine)
- Cannabinoids (Marijuana)
- Cocaine
- Opiates (codeine, morphine)
- Phencyclidine (PCP)

All urine specimens will undergo an initial Enzyme Multiplied Immunoassay Technique (EMIT) screening. Any positive result from this screen will be confirmed through a Gas Chromatography with Mass Spectrometry (GC/MS) test. Any positive result from this latter test will be reviewed by a Medical Review Officer prior to the result being communicated back to the Company. This will ensure that positive results are not due to factors which the Medical Review Officer feels justifies the presence of drugs.

Any Contingent Worker who is tested will have the right, upon request, to see the results of his or her test. A Contingent Worker whose tests are *confirmed positive by the GC/MS test and verified by the Medical Review Officer* will be notified by the Human Resources representative.

Solicitations

Great American intends to provide employees and others working here, including Contingent Workers, with a work environment free from unauthorized solicitation. Solicitation refers to activities such as the following:

- Ordering merchandise
- Selling tickets or subscriptions
- Requesting contributions or gifts
- Distributing literature
- Procuring memberships for participation in any group
- Signatures or petitions, etc.

The above activities are prohibited on behalf of any person, group, society, labor organization, religious or charitable body, political body, or similar association.

Limitations

Solicitation during work hours is limited to company approved charitable campaigns, such as United Way and Fine Arts Fund drives, or other collections for gifts within a department when approved by the supervisor. Other solicitations, in the absence of specific departmental approval, are prohibited.

Non-employees

Solicitations by non-employees or distributed by non-employees on Great American's premises are strictly prohibited at any time. It is our policy to limit access to our premises to customers, employees and vendors. Anyone else will be considered a trespasser.

Standards of Conduct

Great American has established standards of conduct that it expects all Contingent Workers to follow.

The following are behaviors and actions that Great American considers unacceptable. This list is not all-inclusive but merely indicative of the types of actions considered subject to disciplinary action, up to and including termination of your Contingent Worker assignment, depending on the offense and the circumstances. Great American specifically reserves its right to discipline Contingent Workers for inappropriate behavior of any type, regardless of whether such behavior is listed below.

The following actions are considered to be subject to disciplinary action.

- Absenteeism from contingent work assignment—excessive
- Accepting gifts or kickbacks in violation of Company policy
- Breach of security
- Bribery
- Carrying or concealing weapons/dangerous ordnance that is not registered with and approved by the Company
- Causing general dissention and unrest among employees, including malicious gossip or false accusation
- Conflict of interest - undisclosed/unapproved
- Criminal acts or convictions
- Damaging Company property or the property of an employee or another Contingent Worker
- Deception or fraudulent acts
- Defamation of character of an employee or another Contingent Worker
- Discrimination against an employee or another Contingent Worker
- Dishonesty
- Disloyalty to Company
- Disorderly conduct
- Embezzlement
- Extortion
- Failure to cooperate with a Company investigation
- Failure to follow quality specifications
- Falsifying billed hours or other documentation
- Fighting and/or assault
- Gambling - other than office pools and raffles
- Harassment—including sexual harassment and inappropriate displays of anger
- Insubordination
- Interference with production
- Intoxication—under the influence of drugs or alcohol while on duty or on-call. (No alcoholic beverages or controlled substances other than prescription medication are allowed on the premises.)
- Misappropriation of funds—failure to handle cash in accordance with the Company guidelines, reporting personal expenses as business expenses, or misuse of corporate funds or credit cards.
- Misuse of Company resources, including misuse of telephone, email, internet, computers (as set forth in the Information Asset Security Policy, below) and company credit cards.
- Profanity or abusive language
- Release of confidential information— unauthorized disclosure of information critical to the Company's success or of a confidential nature
- Safety rule violations
- Sleeping on the job
- Solicitation or distribution of non-Company products or services (unauthorized)
- Stealing
- Tardiness—excessive
- Unprofessional or abusive conduct
- Unsatisfactory performance of assignments
- Violations of Company policy

Violation of Company rules or policies as set forth in these Contingent Worker Guidelines

Tobacco Usage in the Workplace

Tobacco usage is prohibited in all Great American offices and locations. Also, many local governments restrict and control tobacco usage out of doors. You are required to know and comply with all local regulations controlling tobacco usage.

Weapons Policy

Great American's policy, in accordance with state law, prohibits the possession, transfer, sale or use of weapons on Company property. Company property includes, but is not limited to, facilities owned, leased or managed by the Company and Company-owned and leased vehicles. Contingent Workers are further prohibited from carrying weapons while on Company business and at Company-sponsored events.

"Weapons" include, but are not limited to, any form of gun, illegal knife or other dangerous ordnance.

This policy applies to everyone who is on Company property, including all Company employees, Contingent Workers or those conducting business on Great American's property, regardless of whether they are licensed to carry a concealed weapon.

The only exceptions to this policy are law enforcement officers on official business or security officers engaged by the Company.

Any employee who has reason to believe someone is in violation of this policy or has questions about the policy is to contact AFG Corporate Security at 513-579-2586.

Safety and Building Evacuation

You are to become fully acquainted with emergency procedures for your work location. Each floor or area at Great American has someone identified as the Fire Warden. This person will make sure all people have either exited the area or are in a designated waiting area should the building be evacuated. You are to find the Fire Warden for your area, learn the exit routes (also posted on all floors) and find out any other information needed for your participation in an orderly, safe building evacuation.

Additional information is normally found in bulletins or booklets specific to office sites. They include guidance on evacuation, earthquake, fire, medical emergency and other urgent safety situations. If written procedures are unavailable for your office, you should request a personal orientation from a member of management. The Loss Prevention department can provide direction as needed.

Accidents are preventable in the sense that had someone in the chain of events done something differently (exercising more safety), the accident could have been prevented. You must take responsibility for your own safety, and are expected to help look out for the safety of others. Any suggestions for safety improvements, or requests for safety assistance, should be promptly communicated to management or the local Loss Prevention department.

Immigration Compliance Policy

Great American complies with all laws relating to using legally eligible Contingent Workers – including citizens, nationals and aliens authorized to work in the United States. We do not knowingly engage anyone as a Contingent Worker who is not authorized to work in the United States.

Business Attire Policy

Those who work at a Great American location are expected to dress in a manner that is appropriate for the business to be conducted each day. Depending on the nature of the day's work, it may be appropriate to wear more traditional, formal business attire. On other days, business casual attire might be suitable. A Contingent Worker has the responsibility to wear what is appropriate each day in the business setting. All questions concerning the appropriateness of what to wear are to be directed to the Great American employee for whom you are doing your continent work.

Other Agreement

If you have an independent consulting agreement or other agreement with Great American whereby you are to do work or provide services as a non-employee and any of the terms and conditions of such agreement are in conflict with or different from these Contingent Worker Guidelines, then the agreement you signed is controlling with respect to the conflict.

Acknowledged: _____

Name Date

GREAT AMERICAN.
INSURANCE GROUP

Information Asset Security Policy

It is the policy of the Great American Insurance Company ("Company") to protect the Company's Information Assets. All information and systems used by the Company and its subsidiaries are considered assets and must be appropriately protected. Maintaining the confidentiality, integrity, and accessibility of Information Assets is the responsibility of all Company employees, contractors, consultants, Contingent Workers and other third parties who have access to Company Information Assets. This Information Asset Security Policy is implemented in accordance with and subject to the Company's Code of Ethics/Conflict of

Interest.

Introduction

Scope

The scope of this Information Asset Security Policy ("Policy") covers the use and protection of all **Company Information Assets** by employees and third parties (which includes Contingent Workers). Company Information Assets include Company data as well as Company systems that store or process that data.

Company Information. This Policy covers data in all forms and media that is controlled, owned by, or under the custody of the Company, including but not limited to:

- Electronic data - data that is stored, captured or processed using telephonic or electronic systems (e.g., emails, voicemails, websites, files, documents, databases, and archived and back-up information);
- Non-electronic data (e.g., hard copies of files, meeting minutes, manuals, policy documents, claims documents, hand-written documents, and management reports);
- Data contained in products;
- Data pertaining to systems or applications;
- Data about functional or departmental operations;
- Contractual agreements with third parties;
- Company business plans;
- Personal data collected from or otherwise regarding Company employees, agents, contractors or customers;
- Trade secrets or inventions and other Company confidential and proprietary data.

Company Systems. This Policy also covers computer systems and other non-electronic equipment that process or store Company Information. Such systems include:

- Computer systems (e.g., desktop computers, portable hard drives, handhelds, printers, fax machines, servers, tapes, telephone systems, scanners, networks, software application, mainframes, floppy disks, CDs, CD-ROMs, DVDs, or USB thumb drives);
- Non-electronic equipment (e.g., file cabinets, file folders, desk drawers, boxes or file rooms).

Users. This Policy applies to all *Users* of Company Information Assets. Users include:

- Employees;
- External Parties (business partners, independent contractors, agents, suppliers, Contingent Workers and third parties who have access to Company Information Assets).

Remote Access. This Policy applies to the use of Company Information assets at any location, whether at the User's home, at work or at another site, and at any time.

Compliance

All Users of Company Information Assets must comply with this Policy. This Policy is to be construed in accordance with, and subject to, the Company's Code of Ethics/Conflict of Interest [link to AFGLink for policy] and GAI Records Retention Program Manual [link to AFGLink for policy]. Non-compliance with this Policy can jeopardize the integrity and value of Company Information, and may subject the Company to unnecessary risk including legal action. Anyone who violates this Policy is subject to disciplinary action up to and including termination of employment or other affiliation with the Company. Noncompliance by an External Party may subject the External Party to legal exposure and could jeopardize the relationship with the Company.

Security

General Access

Access to Company Information Assets is restricted to those Users who have a legitimate business need to utilize Company Information Assets. Users may be granted access to some, but not necessarily all Company Information Assets. Regardless, all Users are responsible for protecting Company Information Assets for which they have been granted use and access. Controls for accessing Company Information Assets are implemented based on the location of the asset, the value of the affected Company Information, and any risks that may be mitigated by such controls.

Company Information

Users who are granted access to Company Information Assets may use the asset for legitimate purposes only in accordance with this Policy. Company Information Assets must be returned to the Company immediately upon termination of employment or termination as an authorized external party.

All Users, including remote access Users, must protect the confidentiality, integrity, and availability/accessibility of Company Information Assets at all times from unauthorized or accidental disclosure, use, modification, copying, publication, damage, or destruction, and must not release Company Information without appropriate authorization.

Some examples of protecting Company Information Assets include the following:

- Company Information accessed from a laptop hard drive, thumb drive, or other peripheral device must be returned to Company computer systems;
- Laptops must be secured in the trunk of an employee's vehicle rather than on the back seat, while the vehicle is unattended;
- Confidential paper documents and files must be kept in a secure location to protect against loss, theft, or unauthorized viewing.

To the extent a User has knowledge of Company Information, the confidentiality obligations survive the termination of any access to the Company Information Asset where the information resides or is located.

Company Computer Systems

Identification and Authentication

The Company assigns each User of Company computer systems a unique user id/account. Users must authenticate their identity with a password or authentication token (e.g., digital certificate and dual-factor authentication) before gaining electronic access to the Company computer system. The Company prohibits Users from having multiple user id's/accounts with different permissions on the same system, except in limited situations as approved by the Company on an individual basis. Likewise, the Company also prohibits shared or group user id's/accounts, although certain exceptions may be allowed depending on the application.

Passwords

Passwords provide the primary level of access, accountability and control for the Company's Information Assets. All Users of Company Information Assets must maintain complete confidentiality of their passwords. Users are not permitted to divulge a password to another User or any other individual unless permitted by an authorized Company representative. In rare situations access to a system is required for support purposes, in which case the User shall either create a new temporary password for support personnel's use, or immediately change the existing password once it has been compromised. Users are required to change their password every 90 days. Additionally, the Company also utilizes software to ensure that the password selected by the User meets minimum password complexity.

Internet Usage and Monitoring

Public communications networks (e.g., Internet, Extranets, etc.) are generally unsecured and unregulated. Public networks can also provide a gateway through which any individual can gain unauthorized access to the Company's electronic data and applications. Users have no expectation of privacy in accessing any website using the Company's computer or network systems. The Company reserves the right to restrict access to Internet usage to ensure that the computer systems are not being misused. Subject to applicable law, the Company also reserves the right to monitor, review and record all access to and usage of the Internet by those using the Company's computers or network systems. Monitoring may include: (1) User identification, (2) web pages visited, (3) date and time, and (4) bandwidth usage (See sub-section below on Bandwidth Usage).

Users may be allowed to use the Company's public network systems to access the Internet or Company Intranet for business-related purposes. Incidental and occasional personal use of the Internet through the Company's computer systems is permitted, but such use must otherwise comply with this Policy, and is not to distract or prevent Users from fulfilling their functions and duties.

Bandwidth Usage

Users should also refrain from accessing sites that require excessive bandwidth usage. For example, accessing sites that utilize streaming video creates additional costs to the Company, and strain the capacity of the Company's computer systems, often resulting in unusually slow data transmission for ongoing business needs (e.g., slow email retrieval or Internet access).

Because bandwidth usage presents unique problems, the Company may send an initial electronic or other notice to a User whose Internet bandwidth usage exceeds acceptable limits, requesting that the User discontinue accessing the relevant

website. The User's manager will receive a copy of the initial notice. If the excessive bandwidth usage continues during an eight-day period following the initial notice, the Company will send the User's manager a notice requesting that the manager take appropriate action. Human Resources will receive copies of all such notices sent to the User and the User's manager.

Electronic Mail Usage

Company electronic mail systems are the property of the Company and should be used for business related purposes. Electronic mail messages, whether business or personal, containing derogatory statements, abusive or offensive language, and which are in any manner racist, sexist or discriminatory are inappropriate and are not sanctioned by the Company. Using Company computer systems to create, distribute or print messages of this type is prohibited.

Incidental and occasional personal use of the Company electronic mail systems is permitted, but the Company is not to incur any external costs for the processing of personal messages, and such personal messages is not to distract or prevent Users from fulfilling their functions and duties. Users have no expectation of privacy in accessing or using the Company's electronic mail messaging systems for sending or receiving either business or personal emails.

Subject to applicable law, the Company reserves the right to monitor, review and record all electronic messages created, sent or received by those using the Company's computers systems to ensure that the Company's electronic mail systems are not being misused.

Telephonic Systems Usage

The Company's telephonic systems are the property of the Company and should be used for Company business. Information stored, transmitted, carried by and created on telephonic systems is considered property of the Company. Telephonic communications and recordings containing derogatory statements, abusive or offensive language, or which are in any manner racist, sexist or discriminatory are inappropriate and are not sanctioned by the Company.

Incidental and occasional personal use of the Company's telephonic systems is permitted within the Company, but the Company is not to incur any external costs for the use of these systems, and such personal use is not to distract or prevent Users from fulfilling their functions and duties. Personal use is subject to the same guidelines as other communications as stated above.

Subject to applicable law, the Company reserves the right to restrict access to, monitor, review, and record all inbound and outbound telephone calls on any Company telephonic system. Users have no expectation of privacy in sending or receiving either business or personal telephonic communications.

Company Computers and Software

Company computers contain software and various applications, which fall under strict licensing agreements between GAIC and third party vendors. Many of these agreements prohibit the use of the specific software and/or applications by non-employees of the Company. Therefore, terminated employees and Contingent Workers whose GAIC assignments have ended are responsible for returning their computers to their manager and/or immediate supervisor or GAIC contact. The manager of a terminated employee or GAIC contact for a Contingent Worker is also responsible for promptly ensuring and confirming that the Company owned computer has been returned or remains with the Company.

Software that is developed in-house or licensed through a third party is subject to copyright and other intellectual property laws. Users are prohibited from unauthorized copying of such software for any purpose. Additionally, no personal software may be installed on Company information systems, unless it is necessary for the performance of the User's job duties. Users are to refer to the Company's Code of Ethics/Conflict of Interest for more information on copyright restrictions and license agreements pertaining to software.

Peripheral Devices

A peripheral device is any external hardware that can be attached to a computer either directly, or via wire or wireless connection. Some peripheral devices are portable and can store, process, or transmit data. These include BlackBerry® and other handheld (PDA) devices, floppy disks, CDs, CD-ROMs, DVDs, and USB thumb drives.

Company Information that is downloaded to, stored on, or processed using a peripheral device nonetheless remains the property of the Company. All Users who utilize a peripheral device for business purposes must ensure that the Company Information residing on the peripheral device is backed up or moved to Company computer systems as soon as practical.

The Company reserves the right to inspect at any time all peripheral devices that are used to transmit, store, or process Company Information, whether the device is Company-owned or User-owned. Therefore, Users who utilize their own peripheral device for business purposes have no expectation of privacy to the extent that the peripheral device contains Company Information.

Cameras and Videotapes

Company Information is never be downloaded to, stored on, or processed using any type of camera or video recorder, unless necessary for the User's job function. Accordingly, any photographing and videotaping on Company premises should be done in a manner in which Company Information is not captured. External Parties are prohibited from using any type of camera or video recorder while on Company premises without approval from the appropriate Company manager.

Personally Owned Equipment

The Company strongly discourages Users from storing Company Information on any personally owned equipment. As with peripheral devices, Users who store Company Information on their personally owned equipment must backup or move the Company Information to Company computer systems as soon as practical. Likewise, Users who utilize their personally owned equipment for business purposes have no expectation of privacy to the extent that their personally owned equipment contains Company Information.

Personally Identifiable Information

The Company defines Personally Identifiable Information ("PII") as information that is protected by applicable privacy statutes and regulations. Examples of PII include, but are not limited to the following:

- Social Security Number
- Credit Card Number
- Bank Account or Routing Number
- Federal Tax Identification Number

Users should refrain from transmitting any PII about any individual through any unsecured means, including but not limited to email, facsimile, internet, and text messaging via PDA, except as may be necessary as part of the User's job function. Additionally, Users are not to scan and/or copy documents that contain PII unless it is absolutely necessary for the User to do so as part of the User's job duties. Additionally, PII are not to be sent from one department/division of GAI to another using unsecured interoffice mail.

Clean Desk

The Company must protect its information and that of its employees, customers and third parties from unauthorized disclosure or theft. All Users are to secure all Company confidential paper documents and files containing confidential and restricted information in drawers and filing cabinets whenever leaving their work area and at the end of the day. Additionally, Users should clear their work areas from all paper, files and media that may contain sensitive and proprietary Company Information prior to leaving the area. Users should also log off from their computers at the end of the day and use the computer screen saver with password protection when stepping away from their desk during the workday.

Access for Contractors/External Parties

External parties, including Contingent Workers, will not be granted access to Company Information Assets unless the external User first agrees in writing to adhere to this Policy, which will be provided or made available online at the beginning of the business relationship. External parties who are granted access to Company Information Assets must also agree to comply with the Company's appropriate non-disclosure requirements. Each Company department and/or business unit is responsible for authorizing and terminating any External Party's access to and use of Company Information Assets.

Ownership & Responsibilities

Prohibited Activities

Users are expected to use good judgment in accessing and utilizing Company Information Assets, and must not use these Assets to engage in activities that are illegal, immoral, or that may expose the Company to legal liability or otherwise harm the Company's business interests or reputation. Without limiting the foregoing, Users are prohibited from engaging in the following activities using Company Information Assets:

- Conducting outside business ventures or engaging in other activities in violation of the Company's Code of Ethics/Conflict of Interest.
- Posting or disseminating information in any manner, including blogs and other Internet postings, that is inconsistent with the Company's Privacy Notice.
- Posting or disseminating material that is intended to, or has the effect of, harassing or discriminating against any individual or group.
- Accessing any website that contains or displays offensive, derogatory, obscene, pornographic, violent or sexually explicit materials, or that might contribute to a hostile work environment, based on gender, age, race, national origin, religion, or disability.

- Penetrating or attempting to penetrate the Company's computer systems, physically or electronically (either on-site or remotely), or that of any third party, or accessing any other person's computer, email or voicemail accounts, or equipment without authorization.
- Downloading or installing any software or online tools without authorization. Such applications may contain harmful computer viruses and codes that may adversely affect the operation and function of the Company's computer systems.

Any Contingent Worker who engages in prohibited activities may be subject to legal exposure, and the Company may also terminate the relationship.

Reporting Breaches and Suspicious Activities

If a User becomes aware of or suspects a security breach involving Company Information Assets or any violation of this Policy, then that User must report the breach and/or their suspicions to at least one of the following:

- User's Manager and/or Immediate Supervisor or Company contact
- AFG Investigative Services Anonymous Hotline [1-800-748-7848]
- IT Security Operations and Enablement (If IT related)
- Customer Care Center (If IT related)
- GAI Legal Department

Once contacted and made aware of the incident, the Company will take appropriate action to address the situation.

Acknowledged: _____

Name Date

GREAT AMERICAN.
INSURANCE GROUP

FOREIGN CORRUPT PRACTICES ACT ANTI-CORRUPTION POLICY

Purpose

The purpose of this Foreign Corrupt Practices Act Anti-Corruption Policy ("Policy") is to ensure that all contingent workers comply with the Foreign Corrupt Practices Act of 1977, as amended ("FCPA") and related laws of other countries in which Great American does or intends to do business. Great American reserves the right to amend, rescind or replace this Policy at any time.

What is the FCPA?

The FCPA makes it illegal for U.S. persons to bribe foreign public officials. U.S. persons include U.S. companies and their subsidiaries, officers, directors, employees and agents. Therefore, the fact that business is conducted only in the U.S. does

not mean that you are not dealing with a foreign official. **A foreign official could be an officer, employee or a third party agent of a government owned business operating within the U.S. or overseas.**

Applicability

This Policy extends to all of Great American's domestic and foreign operations, including operations conducted by any departments, divisions, subsidiaries, agents, consultants, or other representatives. The Policy contains information explaining the key provisions of the FCPA and is intended to prevent corruption and bribery from occurring in Great American's activities. **Great American strictly prohibits all forms of bribery and corruption** and will take all necessary steps to ensure that it does not occur in its business activities.

Prohibited Payments

Contingent workers are prohibited from directly or indirectly making, promising, authorizing or offering Anything of Value to a foreign government official on behalf of Great American to secure an improper advantage, obtain or retain business, or direct business to any other person or entity. Payments to third parties are prohibited if undertaken with actual or implicit knowledge that such payments may be used in an illegal manner.

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

(i) Gifts.

(ii) Travel, meals, lodging, entertainment, gift cards.

(iii) Loans, non-arm's length transactions.

(iv) Charitable donations.

(b) **Foreign Government Official** broadly includes:

(i) Officers or employees of a foreign 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 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) Foreign political parties or officials thereof.

(v) Candidates for political office.

The term also includes spouses or other immediate family members of Foreign Government Officials and agents of Foreign Government Officials.

Permitted Payments

These are limited exceptions to the prohibition of payments:

(a) **Facilitating Payments.** Permitted if, and only if, they are 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.

(b) **Promotional Hospitality and Marketing Expenses.** Great American may pay for the reasonable cost of a foreign 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 Great American's products or services, or the execution of a contract with a foreign government or agency.

(c) **Promotional Gifts.** Promotional gifts of nominal value may be given as a courtesy in recognition of services rendered or to promote goodwill. Such nominally valued gifts should generally bear the service mark of Great American.

Political Contributions

Contributions to candidates for foreign political office are prohibited unless preapproved in writing by the General Counsel.

Record Keeping

All expenses involving foreign government officials must be recorded accurately, providing the purpose and amount of the expenditure.

Cash Payments

Cash payments of any kind to a third party, other than documented petty cash disbursements or other valid and approved payments, are prohibited. Great American's checks shall not be written to "cash," "bearer" or anyone other than the party entitled to payment except to replenish properly used petty cash funds.

Representatives

All third party representatives including agents of Great American must fully comply with the FCPA and all other applicable laws.

Penalties

Penalties for violation of this law are severe: Great American can be fined up to $2,000,000, and individuals can be fined up to $250,000 and imprisoned for up to 5 years. The FCPA does not contain any "materiality" standard; all violations, regardless of the sum of money involved, are considered equally serious. Violations of the FCPA can also result in violations of other US laws, including anti-money laundering laws, mail and wire fraud and conspiracy. Aside from the FCPA, Great American and contingent workers may also be subject to other foreign anti-corruption laws.

Compliance

Great American expects contingent workers to be familiar with and perform their duties according to the requirements set out in this Policy. Individuals with supervisory responsibilities over others will be responsible for the failure to exercise proper supervision in detecting and reporting violations of this Policy by their direct reports. Individuals who violate this Policy are subject to disciplinary action, up to and including dismissal. Third-party representatives who violate this Policy may be subject to termination of all commercial relationships with Great American.

If you suspect that this Policy may have been violated, immediately notify Great American as specified in section entitled "Reporting Policy Violations" below. Any person 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, Great American requires that you seek additional guidance before taking any action that may subject Great American to potential FCPA liability.

Duty to Cooperate

Great American may at times undertake a more detailed review of certain transactions. You must cooperate with Great American, outside legal counsel, outside auditors or other similar parties. Failure to cooperate in an internal review is a breach of obligation to Great American. A failure to cooperate may result in disciplinary action up to and including termination and may require a report to a governmental authority.

Reporting Policy Violations

To report potential violations of this Policy, immediately notify your supervisor or if you feel uncomfortable or otherwise believe it is inappropriate to discuss such matter with your immediate supervisor, you may follow the procedures found on the AFGLink website under "Report a Fraud."

Questions About the Policy

If you have any questions about the FCPA, or whether a payment or gift is permitted under the FCPA, contact Corporate Legal for guidance at clegal@gaic.com or call Eve Rosen, General Counsel, Great American Insurance Company.

FCPA Acknowledgment

I have received and read a copy of Great American's Anti-Corruption Policy and understand its contents. I understand that Great American expressly reserves the right to change, modify or delete its provisions without notice.

Acknowledged:

Name TATIREDDY THULACIRAM

Date 28/06/2016

GREAT AMERICAN.
INSURANCE GROUP

Contingent Worker Acknowledgment and Agreement

I acknowledge that I have read, understand and agree to the Great American Contingent Worker Guidelines. I also understand that I am required to comply with certain other Company policies that have been covered or that may be presented to me if I become a Great American Contingent Worker.

I understand that Great American policies and rules that would apply to me as a Contingent Worker may change from time to time, and I will comply with those in effect throughout the time I remain a Great American Contingent Worker.

I further certify that all the information submitted by me to Great American is true and complete to the best of my knowledge, and I understand that any false information, omissions or misrepresentations of facts may result in Great American ending my Contingent Worker assignment. I understand that this certification does not create a contract of employment and my status is that of a Contingent Worker as defined in the Great American Contingent Worker Guidelines.

Also, in consideration of my work assignments for Great American and in accordance with the nondisclosure agreement that either I or my employer has signed, I agree not to use, publish or otherwise disclose to any third party, except as the Company may direct, either during or after my work assignment at Great American, any confidential or proprietary information of Great American, or any information or data of others which Great American is obligated to maintain in confidence. I understand that any information, ideas or inventions made or conceived by me in furtherance of my work responsibilities while a Contingent Worker at Great American are the sole property of Great American.

I understand that if I am unsure what information is considered proprietary or confidential, or if I am unsure of my obligations to Great American, I will ask my primary Great American contact for clarification.

When my status as a Contingent Worker ends, I agree to promptly return to Great American all items that belong to the Company, including, without limitation, all confidential or proprietary materials, computer equipment and other property in my possession or under my control that belongs to the Company.

I agree to report any policy concerns to the AFG Investigative Services Anonymous Hotline at (800)-748-7848.

Thulasi Ram
Signature

JAITREDDY THULASI RAM
Name (First, MI, Last Name)

28/06/2016
Date