Employee Handbook
**Table of Contents**

**Globe Life And Accident Insurance Company**  
**Globe Marketing Services**  
**Liberty National Life Insurance Company**  
**Torchmark Corporation**  
**United American Insurance Company**

**EMLOYEE HANDBOOK**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOREWORD</td>
<td>1</td>
</tr>
<tr>
<td>TORCHMARK MISSION</td>
<td>3</td>
</tr>
<tr>
<td>TORCHMARK VALUES</td>
<td>3</td>
</tr>
<tr>
<td>INTRODUCTION</td>
<td>5</td>
</tr>
<tr>
<td>EUAL EMPLOYMENT OPPORTUNITY POLICY STATEMENT</td>
<td>5</td>
</tr>
<tr>
<td>NON-DISCRIMINATION AND ANTI-HARASSMENT POLICY</td>
<td>5</td>
</tr>
<tr>
<td>AMERICANS WITH DISABILITIES ACT POLICY STATEMENT</td>
<td>7</td>
</tr>
<tr>
<td>CONFLICT OF INTEREST AND OUTSIDE EMPLOYMENT STATEMENT</td>
<td>8</td>
</tr>
<tr>
<td>CONFIDENTIAL NATURE OF WORK</td>
<td>9</td>
</tr>
<tr>
<td>EMPLOYMENT</td>
<td>10</td>
</tr>
<tr>
<td>INITIAL EMPLOYMENT EVALUATION PERIOD</td>
<td>10</td>
</tr>
<tr>
<td>EMPLOYEE CATEGORIES</td>
<td>10</td>
</tr>
<tr>
<td>TRANSFERS AND PROMOTIONS</td>
<td>11</td>
</tr>
<tr>
<td>DISCIPLINARY ACTIONS</td>
<td>11</td>
</tr>
<tr>
<td>DISMISSALS AND RESIGNATIONS</td>
<td>13</td>
</tr>
<tr>
<td>COMPENSATION</td>
<td>14</td>
</tr>
<tr>
<td>PERFORMANCE MANAGEMENT AND COMPENSATION PROGRAMS</td>
<td>14</td>
</tr>
<tr>
<td>PERFORMANCE MANAGEMENT PROGRAM SCHEDULE</td>
<td>14</td>
</tr>
<tr>
<td>PAYMENT OF SALARY</td>
<td>14</td>
</tr>
<tr>
<td>OVERTIME PAY</td>
<td>15</td>
</tr>
<tr>
<td>TIME RECORDS</td>
<td>15</td>
</tr>
<tr>
<td>EMPLOYEE REFERRAL PROGRAM</td>
<td>15</td>
</tr>
<tr>
<td>PERSONNEL RECORDS</td>
<td>15</td>
</tr>
<tr>
<td>TIME OFF</td>
<td>16</td>
</tr>
<tr>
<td>VACATION</td>
<td>16</td>
</tr>
<tr>
<td>PERSONAL/SICK TIME</td>
<td>17</td>
</tr>
<tr>
<td>HOLIDAYS</td>
<td>17</td>
</tr>
<tr>
<td>JURY DUTY</td>
<td>18</td>
</tr>
<tr>
<td>TIME OFF TO VOTE</td>
<td>18</td>
</tr>
<tr>
<td>SICK LEAVE BENEFIT PLAN</td>
<td>18</td>
</tr>
<tr>
<td>LEAVE OF ABSENCE</td>
<td>19</td>
</tr>
<tr>
<td>LEAVE UNDER THE FAMILY AND MEDICAL LEAVE ACT (“FMLA”)</td>
<td>19</td>
</tr>
<tr>
<td>MILITARY LEAVE</td>
<td>22</td>
</tr>
<tr>
<td>LEAVE OF ABSENCE WITHOUT PAY</td>
<td>24</td>
</tr>
<tr>
<td>RETURNING/NOT RETURNING FROM A LEAVE</td>
<td>24</td>
</tr>
</tbody>
</table>
### EMPLOYEE BENEFITS
- Cafeteria Plan Benefits .......................................................... 25
- Life Insurance and Long Term Disability Coverage .................. 26
- Retirement Benefits ............................................................... 26
- Workers Compensation .......................................................... 26
- Service Recognition Awards .................................................. 26
- Education Assistance ............................................................. 27

### ON THE JOB
- Attendance, Punctuality and Dependability .......................... 28
- Drug-Free Workplace Policy ................................................... 28
- Appearance and Dress Policy ................................................. 30
- Open Door Policy ................................................................. 31
- Internal Complaint Procedures ............................................. 31
- Solicitations, Distributions, and Use of Bulletin Boards ............ 32
- Parking ............................................................................. 33
- Mail Room and Supplies ..................................................... 33
- Employer Information and Property ....................................... 33
- Internal Investigations and Searches ..................................... 33
- Reference Checks ................................................................. 33
- No Smoking Policy .............................................................. 34
- Audio/Video Recording Policy .............................................. 34
- Post Resignation/Termination Procedures ............................. 34

### SAFETY AND SECURITY
- Violence in the Workplace .................................................... 35
- Accidents and Emergencies .................................................. 35
- ID Badges / Visitors in the Workplace .................................... 35

### COMPUTERS AND TECHNOLOGY
- E-Mail and Internet Policy ..................................................... 36
- Personal Electronic Devices ................................................... 38
- Social Media Policy ............................................................. 39
- Telephone and Voicemail Policy .......................................... 39
- Telephone Service Monitoring Practices Notice to Employees ...... 41

### RECEIPT FOR EMPLOYEE HANDBOOK
................................................................................. 43
FOREWORD

This is a description of policies and guidelines for the subsidiaries of Torchmark otherwise known as Torchmark Corporation Affiliates and consists of the following companies: United American Insurance Company, Torchmark Corporation, Globe Life And Accident Insurance Company, Globe Marketing Services Inc., and Liberty National Life Insurance Company hereinafter referred to as “the Company”. In some instances, subsidiary policies and benefits may differ.

Whether you have just joined our staff or have been with the Company for a while, we are confident that you will find our company a dynamic and rewarding place to work and we look forward to a productive and successful association. We consider the employees of the Company to be one of its most valuable assets. This manual has been written to serve as the guide for the employer/employee relationship.

There are several things that are important to keep in mind about this handbook. First, it contains only general information and guidelines. It is not intended to be comprehensive or to address all the possible applications of, or exceptions to, the general policies and procedures described. For that reason, if you have any questions concerning eligibility for a particular benefit, or the applicability of a policy or practice to you, you should address your questions to the Human Resources Department. Neither this handbook nor any other Company document confers any contractual right, either expressed or implied, for you to remain in the Company’s employ. Nor does it guarantee any fixed terms and conditions of your employment. Your employment is not for any specific length of time and may be terminated at will, with or without cause and without prior notice, by the Company or you may resign for any reason at any time. No supervisor or other representative of the Company (except the Chief Executive Officer in consultation with General Counsel) has the authority to enter into any agreement for employment for a specified period of time, or to make any agreement contrary to the above.

Second, the procedures, practices, policies and benefits described herein may be modified or discontinued from time to time. We will make every effort to inform you of any changes as they occur.

Third, this handbook and the information in it should be treated as confidential. No portion of this handbook should be disclosed to others, except Company employees and others affiliated with the Company whose knowledge of the information is required in the normal course of business.

Finally, some of the subjects described herein are covered in detail in official policy documents. Policies may differ by company and/or State laws. You should refer to these documents for specific information since this handbook only briefly summarizes those subjects. In the case of a discrepancy, the terms of the written policy document are controlling.
TORCHMARK MISSION

Our purpose is to help working class families achieve financial protection from adverse circumstances.

TORCHMARK VALUES

We act in accordance with the highest levels of ethics and integrity.

We make decisions prudently in order to advance the long term interests of our policyholders, employees, field representatives, and shareholders.

We strive to have a positive effect within the communities we serve.
INTRODUCTION

EQUAL EMPLOYMENT OPPORTUNITY POLICY STATEMENT

Equal Employment Opportunity has been, and will continue to be, a fundamental principle at the Company. Employment is based upon personal capabilities and qualifications without discrimination because of race, color, national origin, religion, sex, age, disability, marital status, creed, or any other characteristic or class protected by law.

This policy of Equal Employment Opportunity applies to all policies and procedures relating to recruitment and hiring, compensation, benefits, termination and all other terms and conditions of employment.

The Human Resources Department has overall responsibility for this policy and maintains reporting and monitoring procedures. Your questions and/or concerns should be referred to the Human Resources Department.

Appropriate disciplinary action may be taken against any employee willfully violating this policy.

NON-DISCRIMINATION AND ANTI-HARASSMENT POLICY

The Company is committed to a work environment in which all individuals are treated with respect and dignity. Each individual has the right to work in a professional atmosphere that promotes equal employment opportunities and prohibits discriminatory practices, including harassment. Therefore, the Company expects that all relationships among persons in the workplace will be professional and free of bias, prejudice and harassment.

It is the policy of the Company to ensure equal employment opportunity without discrimination or harassment on the basis of race, color, national origin, religion, sex, age, disability, marital status, creed, or any other characteristic or class protected by law. The Company prohibits and will not tolerate any such discrimination or harassment.

Definitions of Sexual Harassment and Other Prohibited Harassment

A. Sexual harassment constitutes discrimination and is illegal under federal, state and local laws. For the purposes of this policy, sexual harassment is defined in the Equal Employment Opportunity Commission Guidelines as unwelcome sexual advances, requests for sexual favors and other verbal or physical conduct of a sexual nature when, for example: (i) submission to such conduct is made either explicitly or implicitly a term or condition of an individual’s employment; (ii) submission to or rejection of such conduct by an individual is used as the basis for employment decisions affecting such individual; or (iii) such conduct has the purpose or effect of unreasonably interfering with an individual’s work performance or creating an intimidating, hostile or offensive working environment.

Sexual harassment may include a range of subtle and not so subtle behaviors and may involve individuals of the same or different gender. Depending on the circumstances, these behaviors may include, but are not limited to:

Unwanted sexual advances or requests for sexual favors; sexual jokes and innuendos; verbal abuse of a sexual nature; commentary about an individual’s body, sexual prowess or sexual deficiencies; leering, catcalls or touching; insulting or obscene comments or gestures; display or circulation in the workplace of sexually suggestive objects or pictures (including through e-mail, texting and social networking); and other physical, verbal or visual conduct of a sexual nature. Sex-based harassment which is harassment not involving sexual activity or language (e.g., male manager yells only at female employees and not males) may also constitute discrimination if it is severe or pervasive and directed at employees because of their sex.

B. Harassment on the basis of any other protected characteristic is also strictly prohibited. Under this policy, harassment is verbal or physical conduct that denigrates or shows hostility or aversion toward an individual because of race, color, national origin, religion, sex, age, disability, marital status, creed, or any other characteristic or class protected by law and that: (i) has the purpose or effect of creating an
intimidating, hostile or offensive work environment; (ii) has the purpose or effect of unreasonably interfering with the individual's work performance; or (iii) otherwise adversely affects the individual's employment opportunities.

C. Harassing conduct includes, but is not limited to: epithets, slurs or negative stereotyping; threatening, intimidating or hostile acts; denigrating jokes; and display or circulation in the workplace of written or graphic material that denigrates or shows hostility or aversion toward an individual or group (including through e-mail).

**Individu**

**als and Conduct Covered**

These policies apply to all applicants and employees and prohibit harassment, discrimination, and retaliation whether engaged in by an employee, a supervisor or manager, or someone not directly connected to the Company (e.g., an outside vendor, consultant or customer).

Conduct prohibited by these policies is unacceptable in the workplace and in any work-related setting outside the workplace, such as during business trips, business meetings and business-related social events.

**Retaliation Is Prohibited**

The Company prohibits retaliation against any individual who reports discrimination or harassment or participates in an investigation of such reports. Retaliation against an individual for reporting harassment or discrimination, or for participating in an investigation of a claim of harassment or discrimination is a serious violation of this policy and, like harassment or discrimination itself, will be subject to disciplinary action.

**Complaint Procedure**

The Company requires the prompt reporting of all incidents of discrimination, harassment or retaliation regardless of the offender’s identity or position. An individual who believes they have experienced conduct that is contrary to the Company’s policy or who has concerns about such matters should file their complaints with the Director of Human Resources or any member of the Human Resources Department, or a designated member of the Legal Department before the conduct becomes severe or pervasive. Individuals are not obligated to file their complaints with their immediate supervisor before bringing the matter to the attention of one of the other Company designated representatives identified above.

Early reporting and intervention have proven to be the most effective method of resolving actual or perceived incidents of harassment. Therefore, while no fixed reporting period has been established, the Company requires prompt reporting of complaints or concerns so that rapid and constructive action can be taken. The Company will make every effort to stop alleged harassment before it becomes severe or pervasive, but can only do so with the cooperation of the staff.

The availability of this complaint procedure does not preclude individuals who believe they are being subjected to harassing conduct from promptly advising the offender that his or her behavior is unwelcome and requesting that it be discontinued.

**The Investigation**

Any reported allegations of harassment, discrimination or retaliation will be investigated promptly, thoroughly and impartially. The investigation may include individual interviews with the parties involved and, where necessary, with individuals who may have observed the alleged conduct or may have other relevant knowledge.

Confidentiality will be maintained throughout the process to the extent consistent with adequate investigation and appropriate corrective action.

**Responsive Action**

Misconduct constituting harassment, discrimination or retaliation will be dealt with promptly and appropriately. Responsive action may include: training; referral to counseling; monitoring of the offender; and/or disciplinary action such as warning, reprimand, withholding of a promotion or pay increase, reduction of wages, demotion, reassignment, temporary suspension without pay or termination.
as the Company believes appropriate under the circumstances. If an employee making a complaint does not agree with its resolution, the employee may appeal to Arvelia Bowie, Vice President of Human Resources, Torchmark.

Individuals who have questions or concerns about these policies should talk to a Human Resources representative.

Finally, these policies should not, and may not, be used as a basis for separating individuals of a particular gender or any other protected characteristic, or for excluding them from participating in business or work-related activities or discussions in order to avoid allegations of harassment. The law and the policies of the Company prohibit disparate treatment on the basis of sex or any other protected characteristic, with regard to terms, conditions, privileges and perquisites of employment. The prohibitions against harassment, discrimination and retaliation are intended to complement and further these policies, not to form the basis of an exception to them.

AMERICANS WITH DISABILITIES ACT POLICY STATEMENT

The Company is committed to complying with all applicable provisions of the Americans With Disabilities Act ("ADA") and the Americans with Disabilities Act Amendments Act of 2008 ("ADAAA"). It is the Company’s policy not to discriminate against any qualified employee or applicant with regard to any terms or conditions of employment because of such individual’s disability or perceived disability so long as the employee can perform the essential functions of the job. Consistent with this policy of nondiscrimination, the Company will provide reasonable accommodations to a qualified individual with a disability, as defined by the ADAAA, who has made the Company aware of his or her disability, provided that such accommodation does not constitute an undue hardship on the Company.

Employees with a disability who believe they need a reasonable accommodation to perform the essential functions of their job should contact the Human Resources Department. The Company encourages individuals with disabilities to come forward and request reasonable accommodation.

Procedure for Requesting an Accommodation

On receipt of an accommodation request, a member of the Human Resources Department and your manager/supervisor will meet with you to discuss and identify the precise limitations resulting from the disability and the potential accommodation that the Company might make to help overcome those limitations.

The Company will determine the feasibility of the requested accommodation. Considerations of various factors will include, but may not be limited to: the nature and cost of the accommodation; the availability of tax credits and deductions; outside funding; and the Company’s overall financial resources and organization. The Company will also consider the accommodation’s impact on the operation of the Company, including its impact on the ability of other employees to perform their duties and on the Company’s ability to conduct business.

The Company will inform the employee of its decision on the accommodation request. If approved, the Company will inform the employee on how it intends to make the accommodation. If the accommodation request is denied, the employee will be advised of his/her right to appeal the decision by submitting a written statement explaining the reasons for the request. If the request on appeal is denied, that decision is final. The ADA does not require the Company to make the best possible accommodation, to reallocate essential job functions, or to provide personal use items (e.g., eyeglasses, hearing aids, wheelchairs etc.).

An employee or job applicant who has questions regarding this policy or believes that he or she has been discriminated against based on a disability should notify the Human Resources Department. All such inquiries or complaints will be treated as confidential to the extent permissible by law.
CONFLICT OF INTEREST AND OUTSIDE EMPLOYMENT STATEMENT

In General

The Company expects its employees to conduct business according to the highest ethical standards of conduct. Employees are expected to devote their best efforts to the interests of the Company. Business dealings that appear to create a conflict between the interests of the Company and an employee are unacceptable. The Company recognizes the right of employees to engage in activities outside of their employment which are of a private nature and unrelated to our business. However, the employee must disclose any possible conflicts so that the Company may assess and prevent potential conflicts of interest from arising. A potential or actual conflict of interest occurs whenever an employee is in a position to influence a decision that may result in a personal gain for the employee or an immediate family member (e.g., spouse or significant other, children, parents, siblings) as a result of the Company’s business dealings.

Although it is not possible to specify every action that might create a conflict of interest, this policy sets forth the ones that most frequently present a problem. If an employee has any question whether an action or proposed course of conduct would create a conflict of interest, he or she should immediately contact the Human Resources Department to obtain advice on the issue. The purpose of this policy is to protect employees from any conflict of interest that might arise.

A violation of this policy will result in immediate and appropriate discipline, up to and including immediate dismissal.

Outside Employment

An employee may engage in outside employment unless the activity conflicts with the Company’s interest. In general, outside work activities are not allowed when they:

- Prevent the employee from fully performing work for which he or she is employed at the Company, including overtime assignments;
- Involve organizations that are doing or seek to do business with the Company, including actual or potential vendors or customers;
- Involve work for or association with competitors of the Company; or
- Violate provisions of law or the Company’s policies or rules.

Financial Interest in Other Business

An employee and his or her immediate family may not own or hold any significant interest in a supplier, customer or competitor of the Company, except where such ownership or interest consists of securities in a publicly owned company and the securities are regularly traded on the open market.

Acceptance of Gifts

The Company’s code of conduct requires that all employees demonstrate our organization’s commitment to treating impartially all people and organizations with which we come into contact or conduct business. Torchmark Affiliate employees demonstrate the highest standards of ethics and conduct. Employees practice and demonstrate equal treatment, unbiased professionalism, and non-discriminatory actions in relation to all vendors, suppliers, customers, employees, potential employees, potential vendors or suppliers, and any other individual or organization.

Work Product Ownership

All employees must be aware that the Company retains legal ownership of the product of their work. No work product created while employed by the Company can be claimed, construed, or presented as property of the individual, even after employment by the Company has been terminated or the relevant project completed. This includes written and electronic documents and files, audio and video recordings, system code, and also any concepts, ideas, or other intellectual property developed for the Company, regardless of whether the intellectual property is actually used by the Company. Although it is acceptable for an employee to display and/or discuss a portion or the whole of certain work
product as an example in certain situations (e.g., on a resume, in a freelancer’s meeting with a prospective client), one must bear in mind that information classified as confidential must remain so even after the end of employment. Supplying certain other entities (for example those in competing or similar business as the company) with certain types of information may constitute a conflict of interest. In any event, it must always be made clear that work product is the sole and exclusive property of the Company. Freelancers and temporary employees must be particularly careful in the course of any work they discuss doing, or actually do, for a competitor of the Company.

**Reporting Actual and Potential Conflicts**

An employee must promptly disclose actual or potential conflicts of interest, in writing, to his or her supervisor. Approval will be given unless the relationship interferes with the employee’s duties or will damage the Company.

**CONFIDENTIAL NATURE OF WORK**

All Company records and information relating to the Company or its customers are confidential and employees must treat all matters accordingly. No Company or Company-related information, including, without limitation, documents, notes, files, records, oral information, computer files or similar materials may be removed from the Company’s premises without permission from an officer of the Company (except in the ordinary course of performing duties on behalf of the Company). Additionally, the contents of the Company’s records or information otherwise obtained in regard to business may not be disclosed to anyone, except where required for a business purpose. Employees must not disclose any confidential information, purposefully or inadvertently (for example, through casual conversation), to any unauthorized person inside or outside the Company. Employees who are unsure about the confidential nature of specific information must ask their supervisor for clarification. Employees will be subject to appropriate disciplinary action, up to and including dismissal, for knowingly or unknowingly revealing information of a confidential nature.
EMPLOYMENT

INITIAL EMPLOYMENT EVALUATION PERIOD

Every new employee will go through an initial period of adjustment in order to learn about the Company and about his/her job. During this time the employee will have an opportunity to determine if he/she is suited to, and likes, his/her new position.

Additionally, the initial employment evaluation period gives the employee’s supervisor a reasonable period of time to evaluate his/her performance. The initial evaluation period is 90 days unless otherwise indicated.

During this time, the new employee will be provided with training and guidance from his/her supervisor. He/she may be discharged at any time during this period if his/her supervisor concludes that he/she is not progressing or performing satisfactorily. Under appropriate circumstances, the evaluation period may be extended. Additionally, as is true at all times, employment is not for any specific time and may be terminated at will, with or without cause and without prior notice.

At the end of the initial evaluation period, the employee’s supervisor may discuss the employee’s performance with the employee and provide a work review to him/her. Provided the employee’s job performance is “satisfactory” at the end of the initial employment period, he/she will continue in our employment as an at-will employee.

EMPLOYEE CATEGORIES

Based on the conditions of employment, employees of the Company fall into the following categories:

- Full-Time
- Part-Time
- Temporary Employees
- Seasonal/Occasional Employees

Full-Time

A full time employee is one who works the standard operating hours of the respective Company each week; which may differ by subsidiary.

Exempt employees are classified as such if their job duties are exempt from the overtime provisions of the Federal and State Wage and Hour Laws. Exempt employees are not eligible for overtime pay. Their salaries are calculated on an annual basis.

Non-Exempt salaried and hourly employees receive overtime pay in accordance with our overtime policy.

Part-Time

Part-time employees may be classified as exempt or non-exempt and work a regular schedule but fewer hours than a full-time schedule, as defined by the Company. Part-time employees may receive time off benefits as defined by the respective subsidiary. Part-time employees who work an average of 20-37 hours per week are eligible to receive time off benefits on a pro-rated basis. Employees who work fewer than 20 hours per week will not receive paid time-off benefits.

Temporary Employees

A temporary employee is hired for a specified project or time frame. A temporary employee in a non-exempt position is paid by the hour while a temporary employee in an exempt position is paid according to the terms of hire for that individual. Temporary employees do not receive any additional compensation or benefits from the Company.

Seasonal/Occasional Employees

Occasional employees are those individuals who are employed intermittently and make up a pool of “on-call” workers. Generally, occasional workers may be used to assist with a backlog of production-type work or to fill-in for vacations, etc. Occasional employees are usually former employees. Occasional employees do not qualify for holiday pay or other benefits.
TRANSFERS AND PROMOTIONS

The Company encourages employees to aspire to higher-level positions or lateral transfers for which they qualify. The Company has a job-posting program that offers employees the opportunity to apply for other positions within the Company.

Generally, newly hired employees must be in their job for at least four months before applying for a change in position. In addition, employees who wish to be considered for a transfer to another department must be in good standing in their respective departments, and have a good performance, attendance and punctuality record. An employee on disciplinary action will not be considered for a transfer.

Each employee requesting a transfer will be considered for the new position along with all other applicants. Each transfer is judged on an individual basis, depending on the needs of both departments involved. Management will make all final decisions regarding transfers, in conjunction with the Human Resources Department. Employees should also feel free to discuss their career aspirations with their supervisor/manager or the Human Resources Department at any time.

Employees who wish to apply for a transfer should discuss it first with their supervisor/manager. If it is determined that their skills fit the requirements of the desired job, arrangements will be made to complete a transfer request and any required testing through the Human Resources Department. If an employee scores adequately on the required tests, an exploratory interview with the appropriate manager/supervisor will be arranged.

The Company has a right to deny or postpone the transfer of an employee if it would place an undue hardship on the department or the Company as a whole.

The department manager may handle internal departmental transfers without opening the job to employees of other departments or outside applicants. At the discretion of the department manager, the waiting period may be waived for internal departmental transfers and part-time employees applying for full-time positions.

An employee who applied and is accepted for another job in a different department will not be eligible to apply for another external departmental transfer for a period of one year.

For interest in transfer to an affiliate, all requests must go through the local Human Resources Department. In some instances, company benefits may differ.

DISCIPLINARY ACTIONS

The Company requires order and discipline to succeed and to promote efficiency, productivity and cooperation among its employees. The orderly and efficient operations of the Company require that employees maintain proper standards of conduct at all times. Maintaining cooperative behavior is essential to a productive work environment.

Employees who fail to maintain proper standards of conduct and cooperation 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 discharge.

All instances of misconduct should be referred to Human Resources immediately.

Discipline Other than Immediate Termination

All employees are expected to meet the Company’s standards of work performance. Work performance encompasses many factors, including attendance, punctuality, personal conduct, job proficiency and general compliance with the Company’s policies and procedures.

If an employee does not meet these standards, the Company may, under appropriate circumstances, take corrective action other than immediate dismissal.

The intent of corrective action is to formally document problems while providing the employee with a reasonable time within which to improve performance. The process is designed to encourage development by providing employees with guidance in areas that need improvement, such as poor work performance, attendance problems, personal conduct,
general compliance with the Company’s policies and procedures, and/or other disciplinary problems.

Written Warnings

In most instances, the employee will receive an initial verbal warning regarding his/her violation of company or department guidelines. If the problem is not corrected, the next step is to present the employee with a written warning. This should clearly identify the problem and outline a course of corrective action within a specific time frame along with the consequence (e.g., termination, additional probation, etc.) if the problem is not corrected.

The employee should acknowledge receipt of the warning and include any additional personal comments before signing it. A record of the discussion and the employee’s comments will be placed in the employee file in the Human Resources Department.

Employees under disciplinary review may not be eligible for salary increases, promotions or transfers.

Possible Causes for Immediate Disciplinary Action:

- Willful violation of an established policy or rule
- Insubordination (whether related to a work rule, procedure or a behavior)
- Violation of the Anti-Harassment and/or Equal Employment Opportunity Policy
- Undue and unauthorized absence from duty during regularly scheduled work hours
- Failure to call or directly contact your supervisor when you will be late or absent from work
- Violation of the Company’s Conflict of Interest and/or Confidentiality Policy
- Leaving the work premises without authorization during work hours.
- Sleeping on duty

Any employee whose conduct, actions or performance violates or conflicts with the Company’s policies may be terminated immediately and without warning.

The following are some examples of Grounds for Immediate Dismissal:

- Breach of trust or dishonesty
- Conviction of a felony
- Willful violation of an established policy or rule
- Falsification of company records
- Gross negligence
- Insubordination
- Violation of the Anti-Harassment and/or Equal Employment Opportunity Policy
- Falsification of time records
- Undue and unauthorized absence from duty during regularly scheduled work hours
- Deliberate non-performance of work
- Hiding or disposing of work
- Larceny or unauthorized possession of, or the use of, property belonging to any co-worker, visitor, or customer of the Company
- Possession of dangerous weapons on the premises (specific state law will govern)
- Unauthorized possession, use or copying of any records that are the property of the Company
- Excessive absenteeism or lateness
- Marring, defacing or other willful destruction of any supplies, equipment or property of the Company
- Failure to call or directly contact your supervisor for 3 consecutive days of absence (2 days if employed less than one year)
- Fighting, threatening, harassing, pushing or shoving on company property, including parking lots
DISMISSALS AND RESIGNATIONS

Dismissals

Every employee of the Company has the status of “employee-at-will,” meaning that no one has a contractual right, expressed or implied, to remain in the Company’s employ. The Company may terminate an employee’s employment, or an employee may terminate his/her employment, without cause, and with or without notice, at any time for any reason. No supervisor or other representative of the Company (except the Chief Executive Officer in consultation with General Counsel) has the authority to enter into any agreement for employment for any specified period of time, or to make any employment agreement contrary to the above.

Resignation

When an employee decides to leave the Company for any reason, it is requested that the employee provide the Company with a written two-week advance notice (bear in mind that vacation days, personal days, or company recognized holidays should not be included in the two-week notice period).
COMPENSATION

PERFORMANCE MANAGEMENT AND COMPENSATION PROGRAMS

In order to attract and retain a highly qualified and competent work force, the Company has instituted a performance management program to compensate employees in a fair and equitable manner based upon demonstrated job performance, and in accordance with its Equal Employment Opportunity policy. Through this program, employees will receive constructive work reviews designed to address performance, skill developmental needs, and other interests.

PAYMENT OF SALARY

All paydays are bi-weekly on every other Friday. Payment is current for hourly and salaried employees with the exception of field clerical, part-time, temporary, occasional and hourly employees on a leave-of-absence. Payroll schedules may be viewed on the Company’s intranet Human Resources page.

It is the Company’s policy that employee paychecks will only be given personally to that employee. Arrangements for mailing or pick-up must be made in advance and in writing to Human Resources or Payroll.

If the normal payday falls on a Company-recognized holiday, pay will be distributed one workday prior to the aforementioned schedule. Under no circumstances will the Company release any pay in advance to the schedule.

Employees may be paid by check or through direct deposit of funds to a savings, checking, or a combination of accounts at their financial institution of choice. To activate direct deposit, a Direct Deposit Authorization form may be obtained from Human Resources and/or the Human Resources web page on the affiliate intranet. The completed form must be returned to Payroll or Human Resources. It may take one pay period to activate direct deposit. In the event of a lost paycheck, Payroll or Human Resources must be notified in writing as soon as possible before a replacement check can be issued.

The Company expects all employees to act with the highest level of ethics and integrity in all matters associated with pay. Employees should immediately report all pay discrepancies to their manager or to the appropriate payroll representative. In the event that a payment error occurs, the Company will correct and/or recover earnings paid within a reasonable time frame.

A statement of earnings and deductions is available through the on-line Employee Self Service system (ESS) (for those affiliates with such capability) or is distributed each pay period to employees.

PERFORMANCE MANAGEMENT PROGRAM SCHEDULE

Employees may receive constructive work reviews on the following schedule:

Full-Time and Part-Time Hourly Employees:
- 90 day work review
- Annual work and salary review, based on anniversary of the last start date or predetermined schedule

Full-Time Salaried and Salaried Non-Exempt Employees:
- 90 day work review is optional
- Annual work and salary review, based on predetermined schedule

Temporary and Occasional Employees:
At the discretion of the manager
OVERTIME PAY

Depending on Company work needs, employees will be required to work overtime when requested to do so. Prior approval of a supervisor, however, is required before any non-exempt employee works overtime. **Employees working overtime without approval will be subject to disciplinary action.**

Core administrative office hours are generally from 8:00 a.m. to 5:00 p.m., Monday through Friday. Production hours will vary according to the needs of the Company and department.

Compressed work-week schedules are utilized on a limited basis in some departments where the workload and type of work permit a variance from normal office hours.

**Hours physically worked over the hourly non-exempt employee’s regularly scheduled 40 hours will be paid according to the Federal Labor Standards Act. Vacation, personal/sick, or holiday time will not be counted in the calculation of overtime.**

Each day, the time the employee starts and finishes work must be recorded. The electronic timekeeping system is designed to calculate time worked, overtime, holiday pay, vacation time, personal time and any other approved time adjustments requested by an employee. All hourly employees are required to use the time clock.

Salaried non-exempt employees should use the time clock to calculate any overtime pay.

TIME RECORDS

Attendance for hourly employees is recorded accurately and daily by a time clock. Our attendance records are company records, and care must be exercised in recording the hours worked, the times worked, overtime hours, and absences. Employees are not to clock or sign in or out for other employees. Violations of this policy may result in appropriate disciplinary action, up to and including immediate discharge.

All non-exempt employees must record the time they arrived/departed each day. Each non-exempt employee should use the time clock to record his/her overtime.

Non-exempt overtime is calculated on a weekly basis (see overtime section for further explanation). A non-exempt employee’s supervisor must approve each overtime entry. Individuals working overtime without prior approval will be subject to disciplinary action.

Once an employee clocks in, work is to commence immediately. Failure to do so is considered falsification of timekeeping records.

If an employee forgets to clock in/out or sign in/out, the employee must notify his/her supervisor immediately so the time may be accurately recorded for payroll.

EMPLOYEE REFERRAL PROGRAM

The Company is always looking for qualified employees and appreciates recommendations made by existing employees. Employees are eligible to be paid a recruiting bonus when an applicant they referred to the Company is hired and is still employed by the Company after six months. To be eligible to collect the bonus, the referring employee’s name must appear on the application for employment and the referring employee must still be employed at the end of the six-month period.

The referral program may be changed from time to time depending on the existing market conditions. See your local Human Resources representative for the most current bonus amount and procedures.

PERSONNEL RECORDS

To keep necessary company records up to date, it is extremely important that you notify the Human Resources Department of any personal information changes or update through the on-line Employee Self Service (ESS) when applicable. Examples of personal information that should be kept current include:

- Name and marital status
- Address and telephone number (available through ESS)
- W-4 & State exemptions (available through ESS)
- Person to contact in case of emergency (available through ESS)
VACATION

Time away from work to relax and pursue special interests is important to everyone. All full-time employees who complete six months of continuous employment are eligible for paid vacation. Vacation hours are credited on the anniversary day of each month following the month of accrual (e.g., hire date is June 9, accruals will be credited on the 9th of each month, thereafter).

An employee’s length of service determines the amount of vacation hours accrued. Length of service is calculated based on the adjusted credited service date for an employee who has more than one date of hire. Whether or not an employee has an adjusted credited service date will depend on the length of the original period of employment and length of time elapsed between the date of termination and date of rehire.

Employees are encouraged to utilize all of their allotted vacation time. Except in special circumstances and during the first year of employment, employees will not be permitted to carry over into the following year more than one half the maximum vacation hours that can be accrued. In other words, vacation time not used, is not preserved, and will be forfeited. Where special business necessity requires an exception, the department manager or departmental officer must give prior written approval.

Accrued vacation time may be used after 6 months of employment. The minimum amount of vacation that may be used is 4 hours. Vacation is accrued for Full-time employees according to the following schedule:

<table>
<thead>
<tr>
<th>LENGTH OF SERVICE</th>
<th>MONTHLY ACCRUAL</th>
<th>ANNUAL AMOUNT</th>
<th>MAXIMUM CARRY OVER</th>
<th>MAXIMUM TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 months - 4 years</td>
<td>6.67 hours</td>
<td>80 hours</td>
<td>40 hours</td>
<td>120 hours</td>
</tr>
<tr>
<td>4&gt; years &lt;9 years</td>
<td>8.00 hours</td>
<td>96 hours</td>
<td>48 hours</td>
<td>144 hours</td>
</tr>
<tr>
<td>&gt;9 years +</td>
<td>10 hours</td>
<td>120 hours</td>
<td>60 hours</td>
<td>180 hours</td>
</tr>
</tbody>
</table>

Any hours over the maximum total will not be rolled over into the next year and will be forfeited on anniversary date.

Part-time employees who work an established schedule of 20 hours or more per week will accrue vacation time at one-half the rate of the full-time employees. The maximum accrual rate is also half of the full-time employee.

Temporary employees, occasional workers and part-time employees whose scheduled hours are fewer than 20 hours per week are not entitled to vacation pay.

Vacation hours are not accrued during leaves of absence.

Employees should make their vacation requests as far in advance as possible. The manager/supervisor will determine how much advance notice is required in the department. Approval of vacation time is subject to the department manager. Requests for vacation must be pre-approved and in writing. Based upon department needs, the Company will attempt to grant an employee the vacation dates he/she requests. Hourly employees are not allowed to call in an absence and have it charged to vacation time. Any employee who becomes ill during a scheduled vacation cannot change a vacation day to a sick day; scheduled vacation days count as vacation even if an employee would ordinarily take a sick day.

When a company holiday falls during a scheduled vacation, it is not counted as a vacation day. Pay in lieu of vacation time is not allowed.

Managers must approve vacation requests that extend past 40 hours. Both the officer of the department and the Human Resources Department must pre-approve vacation requests for 80 or more hours. An absence of more than two weeks is considered a Leave of Absence.

Employees who leave the Company after completing one year of service will be paid for all accrued and properly documented unused vacation.
PERSONAL/SICK TIME

Full-time employees occupying an hourly position will accrue personal/sick time at the rate of 4.67 hours per month (i.e., 56 hours per 12 month period from date of employment). To be eligible to use personal/sick time, the employee must have completed four months of service with no absences or tardiness. An absence or tardy within the first four months of employment will automatically postpone eligibility to use personal/sick time for an additional four months. Personal/sick time may be used for the employee’s own illness or the illness of a dependent, doctor’s visits, religious observance, bereavement, moving, etc.

Unused personal/sick time will be accumulated from year to year up to a maximum of 240 hours for full-time hourly employees. Accumulating your personal/sick time is a good way to ensure a full paycheck during a period of illness or unexpected emergency not covered by sick leave benefits or other type of pay. Personal/Sick Time is not to be used in conjunction with or as additional vacation time. Employees who use sick/personal time as soon as it is accrued will risk being disciplined for excessive absences. Under no circumstances will payment in lieu of time off be given. Accrued personal/sick time is forfeited when an employee terminates. Personal/sick time is not accured during leaves of absence.

Part-time employees who work an established schedule of 20 hours or more per week will accrue personal/sick time at a rate of 2.33 hours per month. The maximum personal/sick time a part-time employee may accrue is 120 hours. Temporary employees, occasional workers or part-time employees whose scheduled hours are fewer than 20 hours per week are not entitled to personal/sick time pay.

Personal/sick time is to be used at the employee’s convenience with his/her supervisor’s/manager’s advance approval when possible. The minimum amount of personal/sick time to be used is 1 hour.

Managers will determine the amount of personal/sick time an employee will be allowed to use in one week’s time.

Salaried employees do not accrue personal/sick time. However each employee is expected to maintain acceptable attendance guidelines.

To be eligible for personal/sick pay, employees must telephone their supervisor directly, each day of their absence, as far in advance as possible, but no later than two hours after their scheduled arrival time. Failure to contact your supervisor for three (two if employed for less than one year) consecutive days will be considered a voluntary resignation and employment will be terminated. If the supervisor is not available, the Human Resources Department should be contacted. If an employee is unable to make the call personally, a family member or a friend should contact the supervisor. The supervisor must be contacted each day of absence unless approval is given in advance upon first day of reporting an absence. Appropriate documentation must be provided upon return to work.

The Company reserves the right to inquire about the nature or length of an employee’s illness. The Company may request a written certification from a physician or licensed health care professional at any time during an employee’s absence. Such inquiries will be processed through the Human Resources Department.

HOLIDAYS

All full-time and regular part-time employees (including those in initial employment period) are eligible for the following paid holidays:

- New Year’s Day
- Memorial Day
- Independence Day
- Labor Day
- Thanksgiving (2 days)
- Christmas (2 days)

At the end of each year the holiday schedule for the coming year will be posted on the pay calendars. Holiday schedule may vary depending on the subsidiary and department.

In order to be paid for the holiday, employees must work their scheduled day before and after the holiday or the day it will be observed. Full time employees are expected to work at least 6 hours the day before and after a scheduled holiday to have it counted as a full workday.
Part-time employees will be paid for scheduled hours only. Full-time employees who are not regularly scheduled to work on a holiday will be paid 8 hours’ pay that will not count in calculating overtime for the week in which the holiday falls.

JURY DUTY

Upon receipt of the notice to serve jury duty, the employee should immediately notify his/her supervisor, as well as the Human Resources Department. Additionally, a copy of the notice to serve jury duty should be submitted to the Human Resources Department for attendance purposes.

Upon the employee’s return, the employee must notify Human Resources and provide a signed Certificate of Jury Service indicating the number of days served. Full time employees will be paid for the time away from work up to a maximum of two weeks.

TIME OFF TO VOTE

An employee who wishes to vote may request a reasonable amount of time off to go to the polls. An employee may be asked to make up missed time. Employees whose shifts begin 5 hours or more after the polls have opened, or whose shifts end 5 hours or more before the polls close, should not require time off or an adjusted schedule to have ample time to vote.

No employee will be penalized or retaliated against for requesting time off to vote.

SICK LEAVE BENEFIT PLAN

The Sick Leave Benefit Plan (Sick Leave) is wholly funded by the Company to provide benefits during periods of temporary illness or disability. Sick Leave is defined as any period in which you are physically unable to work due to illness or injury and are not entitled to benefits under the Workers’ Compensation law or similar law. Hourly employees who have been continuously employed in a full-time position for at least two years will be eligible to participate in the Sick Leave Benefit Plan.

An employee who applies for sick leave benefits must provide the Company with certification from a licensed physician that supports a determination of disability if the employee is physically unable to work for a period exceeding two weeks.

A short-term disability leave must be certified by a physician or licensed health care professional’s statement identifying the nature of the disability and stating or estimating the date when the employee will be able to return to work. If the employee cannot return on that date, another statement from a physician or licensed health care professional, with a new return date, will be required. Employees will not be able to return to work without submitting to the Human Resources Department a note from a physician or licensed health care professional authorizing the employee’s return.

The Company reserves the right to confirm the necessity for disability leave by requiring the employee to receive a second or third opinion by a doctor of the Company’s choice. The Company will assume any costs for additional examinations that are not paid by the insurance carrier.

Any Family Medical Leave (FML) qualified leave that an employee may be entitled to will run concurrently with time off granted under this policy. In other words, an employee cannot take his/her full short term disability benefits, and then take an additional 12 weeks off under the Family and Medical leave Act (FMLA); any time spent on short term disability counts as part of an employee’s (FML).

An employee who is returning from short-term disability leave will be returned to the same or similar job, at the same salary that the employee held prior to the leave, when possible. Under some circumstances, however, permanent replacement during a leave may be required, or in some instances, staffing requirements may change. Therefore, unless an employee is entitled to return to the same or an equivalent position under the Family and Medical Leave Act, a job cannot be guaranteed when the employee is ready to return to work. In the event the employee is not entitled to return to the same or an equivalent position under the Family and Medical Leave Act and a position is not available, or if the employee chooses not to return to work upon the expiration of the disability leave, employment will be terminated. If an employee does not return from short-term disability leave, the termination date is the last day that the employee
was authorized to return or the date the employee notifies his/her supervisor that he/she is not returning, whichever is sooner. Such employees may be considered for reemployment. An employee who returns to work following a short-term disability leave will be considered as having continuous service.

Payment under the Sick Leave Benefit Plan will begin after the elimination period. The elimination period is the waiting period following the onset of sickness or injury during which an employee is not eligible to receive pay from the Plan.

Sick leave benefits are calculated in a rolling twelve (12) month benefit period, not in a calendar year. A twelve (12) month benefit period begins on the initial day of disabling sickness or injury. Benefits will be paid according to the following schedule:

<table>
<thead>
<tr>
<th>YEARS OF SERVICE</th>
<th>ELIMINATION PERIOD</th>
<th>PAY/ DURATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-3 years</td>
<td>12 weeks</td>
<td>80% base pay up to 14 weeks</td>
</tr>
<tr>
<td>&gt;3-5 years</td>
<td>8 weeks</td>
<td>80% base pay up to 18 weeks</td>
</tr>
<tr>
<td>&gt;5-7 years</td>
<td>4 weeks</td>
<td>80% base pay up to 22 weeks</td>
</tr>
<tr>
<td>&gt;7 + years</td>
<td>2 weeks</td>
<td>80% base pay up to 24 weeks</td>
</tr>
</tbody>
</table>

To qualify for benefits, you must be under the care of a physician and physically disabled in the opinion of the Company. You may be requested to submit an attending physician’s statement at reasonable intervals and may be requested to undergo an independent physical examination. If, in the opinion of the Company, a second opinion is warranted, the second opinion exam will be at the expense of the Company.

Disability due to pregnancy or pregnancy-related illness is covered in the same manner as any other illness. For purposes of administering the Sick Leave Benefit Plan, pregnancy disability is the period of time that an employee is physically unable to perform her normal duties or other duties assigned to her. The period of disability will normally begin on the date of confinement. The Company will allow unpaid maternity leave to be taken in conjunction with Sick Leave if the employee wishes to extend the period of leave in order to prepare for the expected child or care for the newborn prior to making child care arrangements.

Salaried employees who have been continuously employed for one year or more may be eligible to full salary during periods of illness for a maximum of 26 weeks in a twelve (12) month period. Required documentation must be presented to Human Resources within the required time frame for approval.

It is necessary to contact the Human Resources Department at least one week prior to the end of the leave. Failure to return to work promptly when leave ends, refusing a job transfer or accepting other employment while on leave will be considered as a voluntarily resignation and employment will be terminated immediately.

**LEAVE OF ABSENCE**

An employee who anticipates an absence of ten or more workdays will need to apply for a Leave of Absence (LOA). An employee’s length of service will determine if the LOA is paid or unpaid. Paid time-off benefits (Vacation, Sick/Personal) do not accrue during periods of LOA. If a holiday falls during a period when an employee is on leave, the holiday will not be paid. Absences less than 10 days may be considered Family Medical Leave if absence is due to a serious health condition. See your local Human Resources Department for further clarification.

**LEAVE UNDER THE FAMILY AND MEDICAL LEAVE ACT (“FMLA”)**

The Family and Medical Leave Act (FMLA) provides eligible employees with up to 12 weeks of unpaid leave for certain family and medical reasons during a 12-month period. During this leave, an eligible employee is entitled to continued group health plan coverage as if the employee had continued to work. At the conclusion of the leave, subject to some exceptions, an employee generally has a right to return to the same or an equivalent position.
How Much Family and Medical Leave May Be Taken

The 12-Month Period

An eligible employee is entitled to up to 12 weeks of unpaid leave during a 12-month period for any FMLA qualifying reason(s). The 12-month period is a rolling 12-month period measured backward from the date an employee first uses any FMLA leave.

Limitations on Family and Medical Leave

- Leave to care for a newborn or for a newly placed child must conclude within 12 months after the birth or placement of the child.
- When the Company employs both spouses, they are together entitled to a combined total of 12 weeks of FML within the designated 12-month period. Leave will be for the birth, adoption or foster care placement of a child with the employee, for aftercare of the newborn or newly placed child, to care for a parent (but not in-law) with a serious health condition.
- Each spouse may be entitled to additional FML for other FMLA qualifying reasons (i.e., the difference between the leave taken individually for any of the above reasons and 12 weeks, but not more than a total of 12 weeks per person).
- For example, if each spouse took 6 weeks of leave to care for a newborn child, each could later use an additional 6 weeks due to his/her own serious health condition or to care for a child with a serious health condition.

Intermittent or Reduced Work Schedule Leave

“Intermittent leave” is leave taken in separate blocks of time. A “reduced work schedule leave” is a leave schedule that reduces an employee’s usual number of hours per week or hours per workday.

Leave to care for a newborn or for a newly placed child or leave because of an employee’s own serious health condition, or to care for an employee’s spouse, child or parent with a serious health condition, may be taken all at once or, where medically necessary, intermittently or on a reduced work schedule.
If an employee takes leave intermittently or on a reduced work schedule basis, the employee must, when requested, attempt to schedule the leave so as not to unduly disrupt the Company’s operations. When an employee takes intermittent or reduced work schedule leave for foreseeable planned medical treatment, the Company may temporarily transfer the employee to an alternative position with equivalent pay and benefits for which the employee is qualified and which better accommodates recurring periods of leave.

Requests for Family and Medical Leave

An employee should request FML by completing the Employer’s Request for Leave form and submitting it to the Human Resources Department.

When leave is foreseeable for childbirth, placement of a child or planned medical treatment for the employee’s or family member’s serious health condition, the employee must provide the Company with at least 30 days advance notice, or such shorter notice as is practical. When the timing of the leave is not foreseeable, the employee must provide the Company with notice of the need for leave as soon as practicable (i.e., within 1 or 2 business days of learning of the need for the leave).

Required Documentation

When leave is taken to care for a family member, the Company may require the employee to provide documentation or statement of family relationship (e.g., birth certificate or court document).

An employee will be required to submit medical certification from a health care provider to support a request for FML for the employee’s or a family member’s serious health condition. Medical certification forms are available from the Human Resources Department.

The Company may: (i) with the employee’s permission, have a designated health care provider contact the employee’s health care provider in an effort to clarify or authenticate the initial certification; and/or (ii) require the employee to obtain a second opinion by an independent health care provider designated by the Company and at the Company’s expense. If the initial and second certifications differ, the Company may, at its own expense, require the employee to obtain a third, final and binding certification from a jointly selected health care provider.

During FML, the Company may request that the employee provide re-certification of a serious health condition at intervals in accordance with the FMLA. In addition, during FML, the employee must provide the Company with periodic reports regarding the employee’s status and intent to return to work. If the employee’s anticipated return to work date changes and it becomes necessary for the employee to take more or less leave than originally anticipated, the employee must provide the Company with reasonable notice (i.e., within 2 business days) of the employee’s changed circumstances and new return to work date. If the employee gives the Company notice of the employee’s intent not to return to work, the employee will be considered to have voluntarily resigned.

The employee will be required to submit a fitness for duty certification from the employee’s health care provider before the employee returns to work from FML for the employee’s own serious health condition, with respect to the condition for which the leave was taken, stating that the employee is able to resume work.

FML or return to work may be delayed or denied if the appropriate documentation is not provided in a timely manner. A failure to provide requested documentation of the reason for an absence from work may lead to termination of employment.

Use of Paid and Unpaid Leave

FMLA provides eligible employees with up to 12 weeks of unpaid leave. If an employee has accrued paid leave (e.g., vacation, sick leave, and/or personal leave) the employee must use any qualifying paid leave first. “Qualifying paid leave” is leave that would otherwise be available to the employee for the purpose for which FML is taken. The remainder of the 12 weeks of leave, if any, will be unpaid. Any paid leave used for a FMLA qualifying reason will be charged against an employee’s entitlement to FML. The substitution of paid leave for unpaid leave does not extend the 12-week leave period allowed under the Family Medical Leave Act.
**Designation of Leave**

The Company will notify the employee that leave has been designated as FML. The Company may provisionally designate the employee's leave as FML if the Company has not received medical certification or has not otherwise been able to confirm that the employee's leave qualifies as FML. If the employee has not notified the Company of the reason for the leave, and the employee desires that leave be counted as FML, the employee must notify the Human Resources Department within 2 business days of the employee's return to work. Appropriate documentation will be required.

**Maintenance of Health Benefits**

During FML, an employee is entitled to continued group health plan coverage under the same conditions as if the employee had continued to work. To the extent that an employee's FML is paid, the employee's portion of health insurance premiums will be deducted from the employee's salary. For the portion of FML that is unpaid, the employee's portion of health insurance premiums must be paid directly to the Company on the same schedule as payments under COBRA. If the employee's payment of health insurance premiums is more than 30 days late, the Company may discontinue health insurance coverage upon notice to the employee.

**Return from Family and Medical Leave**

Upon return from FML, the Company will place the employee in the same position the employee held before the leave or an equivalent position with equivalent pay, benefits and other employment terms.

**Limitations on Reinstatement**

An employee is entitled to reinstatement only if he/she would have continued to be employed had FML not been taken. Thus, an employee is not entitled to reinstatement if the employee would not be employed with the Company at the time job restoration is sought due to layoffs, reduction in force, or any other reasons employment would have ended during the period of leave.

The Company reserves the right to deny reinstatement to salaried, eligible employees who are among the highest paid 10 percent of the Company's employees employed within 75 miles of the worksite ("key employees") if such denial is necessary to prevent substantial and grievous economic injury to the Company's operations.

**Additional Information**

For further information or clarification about Family and Medical leave, please contact the Human Resources Department.

**MILITARY LEAVE**

An employee who is a member of the United States Army, Navy, Air Force, Marines, Coast Guard, National Guard, Reserves or Public Health Service will be granted a leave of absence for military service, training or related obligations in accordance with applicable law. Employees on military leave may substitute their accrued paid leave time for unpaid leave. At the conclusion of the leave, upon the satisfaction of certain conditions outlined in the Uniformed Services Employment and Reemployment Rights Act (USERRA), an employee generally has a right to return to the same position he or she held prior to the leave or to a position with like seniority, status and pay that the employee is qualified to perform.

**Continuation of Health Benefits**

During a military leave of fewer than 31 days, an employee is entitled to continued group health plan coverage under the same conditions as if the employee had continued to work. For military leaves of more than 30 days, an employee may elect to continue health coverage for up to 18 months of uniformed service at the COBRA rate.

**Requests for Leave**

**Leave for Active or Reserve Duty**

Upon receipt of orders for active or reserve duty, an employee should submit a copy of the military orders...
to his/her department manager and to the Human Resources Department (unless because of military necessity it is impossible or unreasonable).

**Leave for Training and Other Related Obligations**
(e.g., fitness for service examinations)

Employees will also be granted unpaid time off for military training (normally 14 days plus travel time) and other related obligations, such as for an examination to determine fitness to perform service. Employees should advise their supervisor and/or department head of their training schedule and/or other related obligations as far in advance as possible.

**Exigency Leave**

Leave benefits may also be granted under military exigency: 1) qualifying exigency leave under which eligible employees may take up to 12 weeks of FMLA leave for reasons related to the call to active duty of covered service member spouses, children, or parents; and 2) military caregiver leave, which gives employees up to 26 weeks of leave in a single 12-month period to care for a seriously injured or ill, covered service member.

Employees seeking qualifying exigency leave must give reasonable and practicable notice if the exigency is foreseeable. The notice must inform the Company that a family member is on active duty or called to active duty status, cite a listed reason for leave, and give the anticipated length of absence. Family members generally are defined broadly. A son or daughter on active duty, for example, includes an employee's biological, adopted, or foster child, stepchild, legal ward, or one for whom the employee stood in loco parentis, regardless of age.

Please contact a Human Resources representative for information and forms necessary for Military leave.

**Return from Military Leave**

**Notice Required**

Upon return from military service, an employee must provide notice of or submit an application for reemployment in accordance with the following schedule:

- An employee who served for fewer than 31 days or who reported for a fitness to serve examination, must provide notice of reemployment at the beginning of the first full regular scheduled work period that starts at least eight hours after the employee has returned from the location of service.

- An employee who served for more than 30 days, but fewer than 181 days, must submit an application for reemployment no later than 14 days after completing his/her period of service, or, if this deadline is impossible or is unreasonable through no fault of the employee, then on the next calendar day when submission becomes possible.

- An employee who served for more than 180 days must submit an application for reemployment no later than 90 days after the completion of the uniformed service.

- An employee who has been hospitalized or is recovering from an injury or illness incurred or aggravated while serving must report to the Human Resources Department (if the service was fewer than 31 days), or submit an application for reemployment (if the service was greater than 30 days), at the end of the necessary recovery period (not to exceed two years).

**Required Documentation**

An employee whose military service was for more than 30 days must provide documentation within two weeks of his/her return (unless such documentation does not yet exist or is not readily available) showing the following: (i) the application for reemployment is timely (i.e., submitted within the required time period); (ii) the period of service has not exceeded five years; and (iii) the employee received an honorable or general discharge.
LEAVE OF ABSENCE WITHOUT PAY

Should a situation arise that temporarily prevents an employee from working, he/she may be eligible for a personal leave of absence without pay. However, employees must be employed for at least six (6) months prior to the requested leave.

Any request for a leave of absence without pay must be submitted in writing as far in advance as possible. The request will be reviewed on a case-by-case basis by the employee’s supervisor/manager and Human Resources. The decision to approve or disapprove is based on the circumstances, the length of time requested, the employee’s job performance, attendance and punctuality record, the reasons for the leave, and, the most importantly, the effect the employee’s absence will have on the work in the department.

Leaves of absence will be considered only after all vacation and personal time have been exhausted.

See your Human Resources representative for details.

RETURNING/NOT RETURNING FROM A LEAVE

Due to the nature of our business, the Company cannot guarantee either that an employee’s job will remain available or that a comparable position will exist when returning from an unpaid leave. When an employee is ready to return from a leave of absence without pay, the Company will attempt to reinstate the employee to his/her former position or to one with similar responsibilities.

If the position or a similar position is not available, the employee will be terminated.

An employee, who returns to work following an unpaid leave, depending upon the length of the leave, generally will be considered as having continuous service. If an employee does not return from an unpaid leave of absence, the termination date is the last day of the authorized leave period or the date the employee notifies his/her supervisor/manager that he/she is not returning, whichever is sooner.
EMPLOYEE BENEFITS

The Company has established a variety of employee benefit programs designed to assist you and your eligible dependents in meeting the financial burdens that can result from illness and disability, and to help you plan for retirement. This portion of the Employee Handbook lists the possible benefits to which you may be entitled as an employee of the Company. Your rights can be determined only by referring to the full Summary Plan Description of the official plan documents, which are available from Human Resources.

The Company reserves the right, in its sole and absolute discretion, to amend, modify or terminate, in whole or in part, any or all of the provisions of the benefit plans described herein, including any health benefits that may be extended to retirees and their dependents. Further, the Company reserves the exclusive right, power and authority, in its sole and absolute discretion, to administer, apply and interpret the benefit plans described herein, and to decide all matters arising in connection with the operation or administration of such plans.

For more complete information regarding any of our benefit programs, please refer to the Employee Benefit Guides or the Summary Plan Descriptions.

CAFETERIA PLAN BENEFITS

Salary Tax Reduction Plan

The Salary Tax Reduction Plan (STRP) operates as a cafeteria plan under Section 125 of the Internal Revenue Code.

The following benefits are included in the Company’s cafeteria plan benefits and are offered with pre-tax deductions:

Health Insurance

The Company currently offers health insurance for full-time employees and their dependents after 30 days of continuous employment. If elected, coverage begins on the first of the month following 30 days of continuous employment.

The point-of-service plan provides comprehensive hospital and major medical insurance coverage. Under the point-of-service plan, participants may choose in-network or out-of-network providers at any point in time. To assist employees in managing their health care costs, the Company offers choices in levels of coverage.

Health Savings Account

A pre-tax Health Spending Account (HSA) is offered to those who enroll in the High Deductible Health Plan. The HSA allows you to pay for many of the health care expenses not covered by your medical plan including deductibles. You may contribute up to the maximum limit allowed by the Internal Revenue Service and the amounts may change from year to year. The HSA account balances carry over at year end. A small administration fee may apply from the managing financial institution. If enrolled in an HSA, a Flexible Spending Account (FSA) cannot be used for reimbursement of medical expenses.

Dental Insurance

The Company offers a choice of two dental plans for regular full-time employees and their eligible dependents. Employees who enroll will be covered on the first of the month following 30 days of continuous employment.

Vision Insurance

A separate vision plan allows for coverage of eye exams, spectacle lenses co-pay, contact lens evaluation/fitting, and follow-up care co-pay.
**Flexible Spending Accounts**

A Flexible Spending Account (FSA) is an employee benefit that allows money to be deducted from your paycheck on a pre-tax basis to pay for qualifying health care, dependent care, and transportation expenses.

There are three types of FSAs:

**Medical/Health Care Spending Account** – allows the employee to pay for many of the health care expenses not covered by your medical, dental and vision coverage, including deductibles and co-pays. An FSA cannot be used for medical expense if enrolled in the Health Savings Account (HSA), but the FSA can still be used for vision and dental expenses.

**Dependent Care Spending Account** – Allows the employee to pay certain dependent care expenses, such as day care, with pre-tax funds.

**Transportation Spending Account** – an employee can pay certain transportation expenses, including parking, mass transit, vanpool, etc, with pre-tax funds.

For a complete description and limits, see the Flexible Spending Account Benefit Guide supplied by your Human Resources Department.

**LIFE INSURANCE AND LONG TERM DISABILITY COVERAGE**

The Employer Group Life (Life) and Long Term Disability (LTD) plans provide participating employees of the Company with life insurance and disability benefits for their security and the security of their families. Full time employees are eligible to enroll in the plans during the first 30 days of employment. If the employee declines coverage during the initial enrollment period, the employee will be able to apply at a later date but will be subject to evidence of good health in order to enroll.

**RETIREMENT BENEFITS**

The Company provides various sources of income for retirement.

1. A pension plan (Either Defined Benefit or Defined contribution) plan;
2. The Savings and Investment Plan is a 401k benefit that provides employees additional income for retirement if he/she enrolls and contributes; and,
3. Social Security and Medicare benefits which are contributed equally through payroll FICA taxes.

**WORKERS COMPENSATION**

Employees at all facilities are covered by Worker’s Compensation insurance. The name of the insurer at your location is posted on the bulletin board and/or can be obtained from Human Resources. The Company complies in all respects with the various state Workers Compensation laws.

**SERVICE RECOGNITION AWARDS**

The Company recognizes the value of loyal service by its employees. As an expression of appreciation, a service award is presented to employees who complete five years of service and each five years thereafter. Prior to your anniversary you will be given the opportunity to select a service award from the program currently in place. When an employee has more than one date of hire the service award level is determined according to the credited service date.
EDUCATION ASSISTANCE

The Company supports employees who wish to continue their education to secure increased responsibility and growth within their professional careers. In keeping with this philosophy, the company has established a reimbursement program for expenses incurred through approved institutions of learning. If you are a full-time regular employee and have completed six months of service, you are eligible for participation in this program as long as the courses are job-related. (See Education Assistance Policy and Procedure for additional details)

LOMA Education

Fellow, Life Management Institute Program (FLMI) is a 10-course, professional development program that provides a comprehensive business education in the context of the financial services industry. This program will provide a solid instruction to industry terms, functional areas, processes and more. Each course successfully completed will pay a bonus and when FLMI designation is reached an additional bonus is paid.

Continuing Education

The company will reimburse costs (up to a designated maximum amount per year) incurred by an employee for continuing education through an accredited college or curriculum that offers growth in an area related to his or her current position. This can include college credit courses, continuing education unit courses, seminars and certification tests. You must secure a passing grade of “B” or its equivalent or obtain a certification to receive any reimbursement and the program must be approved prior to enrolling. Expenses must be validated by receipts and a copy of the final grade card or certification must be presented to show hours or certification received. Courses must be approved prior to enrolling in order to receive reimbursement.
ON THE JOB

ATTENDANCE, PUNCTUALITY AND DEPENDABILITY

Because the Company depends heavily upon its employees, it is important that employees attend work as scheduled. Dependability, attendance, punctuality, and a commitment to do the job right are essential at all times. As such, employees are expected at work on all scheduled workdays and during all scheduled work hours and to report to work on time. Moreover, an employee must notify his/her supervisor as far in advance as possible, but not later than two hours after his/her scheduled starting time if he/she expects to be late or absent. This policy applies for each day of his/her absence. A careful record of absenteeism and tardiness is kept by the Company and becomes part of the employee’s personnel record. To the extent permitted by law, absenteeism and tardiness lessen an employee’s chances for advancement and may result in dismissal. An employee who fails to contact his/her immediate supervisor may be considered as having voluntarily resigned. Failure to contact your supervisor for three consecutive days (two consecutive days if employed for less than one year) will be considered a voluntary resignation and employment will be terminated. If the supervisor is not available, Human Resources should be contacted. If an employee is unable to make the call personally, a family member or a friend should contact the supervisor. The supervisor must be contacted each day of absence unless approval is given upon the first day of reporting an absence. Appropriate documentation must be provided upon return to work.

To keep the business and each department running smoothly and efficiently, it is important that every employee be on the job on time regularly. For this reason, careful attention is given to promptness, absence record and overall dependability.

All full-time hourly employees who are unable to perform their jobs due to illness or injury are eligible for personal/sick time, subject to the conditions previously discussed in this Handbook. Sick leave benefits are intended to provide income protection in the event of injury or personal illness. Managers will determine the absenteeism rate acceptable in each Department. Generally, an absence rate of more than five (5%) percent of scheduled work time during any rolling 90-day calendar period is considered excessive.

The Company reserves the right to inquire about the nature or length of an employee’s absence.

DRUG-FREE WORKPLACE POLICY

The Company is committed to providing a safe and productive workplace free from the effects of alcohol and substance abuse. The Drug-Free Workplace policy is in place to ensure a safe, healthy and productive work environment for all employees of United American, Globe Life and Accident, Globe Marketing Services and affiliated Torchmark Companies “the Company”, to protect the Company’s property and assets, and to ensure the efficient operation of the Company.

Rules of Conduct

The Company will enforce the following rules uniformly with respect to all employees:

1. Employees are prohibited from using or being under the influence of alcohol or illegal drugs during working hours.

2. Employees are prohibited from selling, possessing, transferring or purchasing illegal drugs on the Company’s property or while performing the Company’s business. The use, sale, transfer or possession of an illegal drug while on duty is cause for immediate termination.

3. No alcoholic beverage will be brought or consumed on the Company’s premises except in connection with company-authorized events.

4. No prescription drug will be brought on the Company premises by any person other than the one for whom it is prescribed. Prescription drugs may be used only in the manner, combination and quantity prescribed.

5. For purposes of this policy, an “illegal drug” is any drug or controlled substance in which the sale or consumption is illegal. A “prescription drug” is any substance prescribed for individual consumption by a licensed medical practitioner. “Alcohol” or “an
alcoholic beverage” is any beverage that may be legally sold and consumed and has an alcoholic content in excess of 3% by volume.

Drug Testing Procedures

The following procedures will be followed with regard to any testing for the presence of alcohol or illegal drugs:

Persons Subject to Testing

All applicants and all employees are subject to drug and alcohol testing.

Applicant Testing

Upon a conditional offer of employment, the Company will request each job applicant for positions (which in the sole discretion of the Company are subject to testing) to undergo pre-employment drug and alcohol testing. The applicant’s refusal to undergo testing or a confirmed positive test result may be used as the basis for refusing to hire the applicant.

Circumstances When Drug and Alcohol Testing May Be Requested or Required of Employees

1. Reasonable Suspicion Testing. If the Company has a reasonable suspicion that an employee has violated the Company’s policy prohibiting employees from using or being under the influence of alcohol and illegal drugs during work hours, the Company may request or require testing. A reasonable suspicion determination may be based upon observable actions/behaviors such as physical symptoms of being under the influence of a drug or alcohol while at work or on duty, or the direct observation of drug or alcohol use while at work or on duty. The Company may also determine that reasonable suspicion of a violation exists based on an independently corroborated reliable report of drug or alcohol use while at work or on duty, evidence that an individual has tampered with a drug or alcohol test in connection with employment with the Company, or evidence that an employee is involved in the use, possession, sale, solicitation or transfer of drugs or alcohol while on duty or while on the Company’s premises or operating the Company’s vehicles, machinery or equipment.

2. Post-Accident Testing. The Company may require an employee to undergo drug or alcohol testing. Each location’s policy will be guided by state laws and local jurisdiction for all post-accident testing of drug and alcohol. For purposes of workers’ compensation or unemployment compensation, no employee who tests positive for the presence of alcohol, illegal drugs, or illegally used chemicals shall be eligible for such compensation unless the employee proves by a preponderance of the evidence that the substances, alcohol, illegal drugs, or illegally used chemicals were not the proximate cause of the injury or accident.

3. Random Testing. The Company may request or require an employee to undergo testing on a random selection basis. The Company will select employees for random testing in such a way that there is an equal probability that any employee from a group of employees subject to selection will be selected. The Company will not waive the testing of any employee selected under the random testing mechanism.

4. Scheduled Periodic Testing. The Company may request or require an employee to undergo testing conducted as a part of routinely scheduled employee fitness-for-duty medical examinations or scheduled routinely for all members of an employment classification or group.

5. Post-Rehabilitation Testing. The Company may request or require an employee to undergo testing without prior notice for a period of up to two years commencing with the employee’s return to work following a confirmed positive test or following participation in a drug or alcohol dependency treatment program.
Identification of the Substances Which May Be Tested

The Company may request or require an applicant or employee to be tested for the following substances but not limited to: alcohol, marijuana, opiates, synthetic narcotics, cocaine, phencyclidine (PCP), amphetamines, barbiturates, benzodiazepines, methaqualone, or a metabolite of any of the substances listed herein.

Testing Methods and Collection Procedures to Be Used

1. **Time of testing.** For current employees, testing will occur during or immediately after their regular work period. Testing will be considered work time for purposes of compensation and benefits for current employees.

2. **Costs.** The Company will pay for the cost of the testing, including confirmation tests and the cost of transportation if the testing of a current employee is conducted at a place other than the workplace. Any individual who requests a retest of a sample in order to challenge the results of a positive test, however, must pay all costs of the retest, unless the retest reverses the findings of a challenged positive test, in which event the Company will reimburse the individual for the cost of the retest.

3. **Sample collection procedures.** Samples will be collected and tested by individuals qualified by the State Board of Health. The collection of samples will be performed under reasonable and sanitary conditions and in sufficient quantity for splitting into two separate specimens. Sample collection will be documented, and the employee or applicant will be provided an opportunity to provide confidentially any information relevant to the test, including identification of currently or recently used prescription or non-prescription drugs.

Maintenance and Confidentiality of Records and Information

The Company will maintain all test results and related information as confidential records separate and apart from personnel records. The records are the property of the Company, but upon the request of the applicant or employee tested, the Company will make the records available for review.

Disciplinary Action

A positive test result is grounds for disciplinary action, including termination of employment. No disciplinary action, except for a temporary suspension or a temporary transfer to another position, will be taken by the Company against an employee based on a positive test result unless the test result has been confirmed by a second test. The Company may also take disciplinary action (including discharge) against any employee who refuses to undergo testing conducted pursuant to this policy. Any employee discharged on the basis of a refusal to undergo testing or a confirmed positive test conducted in accordance with this policy will be considered to have been discharged for misconduct for purposes of unemployment compensation benefits.

Conduct of Searches

Any employee may be required, upon the Company’s request, to submit to a search of any vehicle brought onto Company premises, to submit to a search of any pocket, package, purse, briefcase, toolbox, lunchbox or other container brought onto the Company’s premises, and to submit to a search of any desk, file locker or other container provided by the Company.

**APPEARANCE AND DRESS POLICY**

Employees are expected to be suitably attired and groomed during working hours or when representing the Company. Employees should appear neat and professional at all times with clothing appropriate for any unscheduled meeting with clients, vendors, or other professionals.
Business casual clothing is acceptable for our work environment. However, when conducting a customer meeting or attending another business function, wear traditional business clothing unless business casual is otherwise agreed upon.

Print Shop and other particular employee groups should take into consideration any job specific safety concerns when determining what attire is appropriate. For example, employees who regularly work with machinery or lifting heavy material should wear slip resistant closed-toe shoes. While casual dress is appropriate in this environment, employees are still expected to maintain a neat and professional appearance. Ripped, frayed or disheveled clothing and athletic wear is inappropriate.

Listed below is a general overview of acceptable business casual attire as well as a listing of some of the more common items that are not appropriate for our work environment. Neither listing is intended to be all inclusive. Rather, these items should help set the general parameters for proper business casual attire and allow you to make intelligent judgment about items that are not specifically addressed.

Acceptable – Polo shirts, golf shirts, sweaters, knit tops and casual pants, slacks and Capri pants that are longer than mid-calf. Unacceptable – Shorts, t-shirts, athletic shoes, sweat pants, sweat shirts, tops with spaghetti straps, cargo pants, tank tops, and flip flops.

Denim is acceptable attire only on Casual Fridays.

Perfume, scented lotion, cologne and aftershave lotion should be used in moderation, as some individuals may be sensitive to strong fragrances.

Any clothing, jewelry, or tattoo that conveys a negative statement toward a race, gender, sexual orientation, age, religion, disability, or is otherwise considered harassing or offensive is prohibited.

Your supervisor or department manager is responsible for ensuring adherence to this policy. If your supervisor considers your personal appearance inappropriate, you may be asked to leave the workplace and return properly dressed or groomed. Under such circumstance, you will not be compensated for the time away from work.

Disregarding or failing to comply with this standard of dress code could lead to disciplinary action, up to and including termination of employment. Consult your supervisor or Human Resources if you have questions as to what constitutes appropriate appearance.

Where possible, reasonable accommodation may be made to a person with a disability or to accommodate a person’s religious beliefs.

**OPEN DOOR POLICY**

The Company promotes an atmosphere whereby employees may talk freely with members of the management staff. Employees are encouraged to openly discuss with their supervisor or manager any work related problems so that appropriate action, may be taken. If this is not feasible, you are encouraged to go to the Company officer responsible for your department. If neither is of assistance, or if you do not feel comfortable with either alternative, please feel free to voice your concerns to Human Resources. When taking advantage of this policy please be mindful of other responsibilities borne by the supervisors, managers and officers. Always try to schedule time in advance rather than just showing up at the door.

**INTERNAL COMPLAINT PROCEDURES**

To foster sound employee-employer relations through communication and reconciliation of work-related problems, the Company provides employees with an established procedure for expressing employment related concerns.

In situations where employees feel a complaint is in order, the following steps should be taken:

- If an employee believes that he/she has a legitimate work-related complaint, the employee is encouraged to first attempt to resolve the issue(s) through discussions with his/her immediate supervisor.
● If the situation is not resolved within five working days from the time the complaint is discussed with the employee’s immediate supervisor, barring extenuating circumstances, it should be brought to the attention of the next-level supervisor or a representative in the Human Resources Department with written documentation. The Company will attempt to resolve the complaint within a reasonable period of time while preserving the confidentiality and privacy of those involved to the extent feasible.

Any employee of Torchmark or its affiliates may submit a good faith complaint regarding accounting or auditing matters to the management of the Company without fear of dismissal or retaliation of any kind. The Company is committed to achieving compliance with all applicable securities laws and regulations, accounting standards, accounting controls and audit practices. For further clarification the policy, Employee Complaint Procedures for Accounting and Auditing Matters and the Employee Notice-Whistleblower Hotline can be found on the Torchmark Corporation web site.

SOLICITATIONS, DISTRIBUTIONS, AND USE OF BULLETIN BOARDS

Solicitations and Distributions

No sales or solicitations are to take place on company premises without the review and approval of Human Resources.

Unless specifically authorized, selling, soliciting, collecting and similar activities are prohibited on the Company’s premises in work areas during work time. Types of activities prohibited include the following:

● Sales of any kind, including sales of food, clothing, cosmetics, household items, hand-made items, novelties, and catalog items
● Sales of tickets by hand or e-mail, including raffle tickets
● Soliciting contributions for organizations or individuals by hand or e-mail
● Soliciting support or memberships in clubs or other organizations by hand or e-mail

● Distributing advertising materials by hand or e-mail, handbills or other literature

Work time consists of all time when an employee’s duties require that he or she be engaged in work tasks, but does not include the time before and after work or during lunch and break times. Employees may conduct sales efforts and solicitations during non-work time in the break room. However, such efforts are to be conducted in such a manner as not to be objectionable to fellow employees or to be an interruption of the Company’s business. Even though a solicitation may be authorized, there is never an obligation to participate.

Employees may not solicit any other employee during work time, nor may employees distribute unauthorized 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 work time. This includes electronic solicitation by e-mail.

Persons not employed by the Company may not solicit employees for any purposes on the Company’s premises without prior approval from Human Resources.

Bulletin Boards

Human Resources must approve any information placed on the Company’s bulletin boards.

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

● Notices containing matters directly concerning company business;
● Announcements of a business nature which are equally applicable and of interest to all employees;
● Other notices as approved by Human Resources.

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.
INTERNAL INVESTIGATIONS AND SEARCHES

From time to time, the Company may conduct internal investigations pertaining to security, auditing or work-related matters. Employees are required to cooperate fully and assist in these investigations if requested to do so.

When necessary, in the Company’s discretion, work areas and personal belongings (e.g., desks, file cabinets, brief cases, handbags, etc.) may be subject to a search without notice. Employees are required to cooperate with such searches.

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.

REFERENCE CHECKS

All inquiries regarding a current or former Company employee must be referred to Human Resources.

Should an employee receive a written request for a reference, he/she should refer the request to Human Resources for handling. No employee may issue a reference letter to any current or former employee without the permission of Human Resources.

Under no circumstances should any company employee release any information about any current or former employee over the telephone. All telephone inquiries regarding any current or former employee of the Company must be referred to Human Resources.

In response to an outside request for information regarding a current or former company employee, the Human Resources Department will furnish or verify only an employee’s name, dates of employment, job title and department. No other data or information regarding any current or former employee, or his/her employment with the Company will be furnished unless the employee authorizes the Company to furnish this information in writing that also releases the Company from liability in connection with the furnishing of this information or the Company is required by law to furnish such information.

MAIL ROOM AND SUPPLIES

Because of the enormous volume of incoming mail, personal mail should not be sent to you at the office. Company letterhead and envelopes are provided for the Company’s business only. Do not use the Company’s stationery or envelopes for personal correspondence.

EMPLOYER INFORMATION AND PROPERTY

The protection of the Company’s business information, property and assets are vital to the interests and success of the Company. No company related information or property, including, without limitation, documents, files, records, computer files, equipment, office supplies or similar materials may be removed from the Company’s premises (except in the ordinary course of performing duties on behalf of the Company). Violation of this policy is a serious offense and will result in appropriate disciplinary action, up to and including discharge.

In addition, when an employee leaves the Company, then he/she must return all Company-related information and property that the employee has in his/her possession, including without limitation, documents, files, records, manuals, information stored on a personal computer, computer disc, personal cell phone or other personal electronic device, company supplies, equipment or office supplies.

PARKING

Employees must not park in handicap parking without authorization. Parking in reserved and visitor parking is prohibited at any time. The Company assumes no responsibility for theft or damage to automobiles parked on the Company’s property or other parking facilities. Employees should never speed and should always be courteous to other employees when driving in the parking lot. For security purposes, the Company may have video monitoring of parking areas.
NO SMOKING POLICY

In order to comply with government regulations, the Company has prohibited smoking throughout its workplace. Smoking is allowed only in designated areas of the facilities.

Employees are protected from retaliatory action or from being subjected to any adverse personal action for exercising or attempting to exercise his/her rights under the no smoking policy. Any violation of this policy may result in appropriate corrective disciplinary action, up to and including discharge.

Any questions regarding the no smoking policy should be directed to the Human Resources Department.

AUDIO/VIDEO RECORDING POLICY

It is a violation of the Company policy to record conversations with a tape recorder or other recording device unless prior approval is received from a member of senior management and all parties to the conversation give their consent.

The purpose of this policy is to eliminate a chilling effect on the expression of views that may exist when one person is concerned that his or her 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 immediate termination.

POST RESIGNATION/TERMINATION PROCEDURES

Exit Interview

Human Resources is responsible for scheduling an exit interview with a terminating employee on the employee’s last day of employment and for arranging the return of company property including:

- Company Security Card
- Picture Identification Card
- Office keys
- Company-issued credit card(s)
- Company manuals
- Any additional company-owned or issued property

Benefits

An employee may be eligible to continue Medical, Dental, and Vision Benefits in accordance with the Consolidated Omnibus Budget Reconciliation Act (“COBRA”). Specific information will be provided using the postal service. Employees are responsible for enrollment and payment of COBRA.

An employee vested in retirement benefits will receive specific information in regards to such benefits. All questions can be directed to the Human Resources Department.

Final Paycheck

An employee’s final paycheck will be paid in a timely manner and in accordance to the applicable state law. If there are unpaid obligations to the Company, the final paycheck will reflect the appropriate deductions. Specific instructions can be sent to the Company’s Payroll Department or your local Human Resources Department.
SAFETY AND SECURITY

VIOLENCE IN THE WORKPLACE

The Company strongly believes that all employees should be treated with dignity and respect. Acts of violence including, but not limited to, behavior toward others or company property by employee or non-employees will not be tolerated. Any instances or suggestions of violence must be reported to the employee’s supervisor and/or Human Resources. 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 immediate discharge.

ACCIDENTS AND EMERGENCIES

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

All employees will be provided care, first-aid and emergency service, as required, for injuries or illnesses while on the Company’s premises. In the event of an accident or emergency employees should contact their supervisor, the nearest supervisor, Human Resources and the front desk.

Failure to report accidents is a serious matter as it may preclude the employee’s ability to obtain medical care under the Company’s worker’s compensation insurance.

ID BADGES / VISITORS IN THE WORKPLACE

All employees are to wear company issued photo identification badges while on company premises. Identification badges serve the dual purpose of readily identifying company employees and other authorized personnel, while providing measured protections against unauthorized personnel and intruders from entering secured work areas. In most instances, identification badges will be printed on proximity cards, in which case each card will have a unique code and will provide access through particular doors and other controlled areas on an as-needed basis. Because it holds permission to gain access to particular doors, the identification badge must be protected from use by non-authorized persons. If an identification badge is lost, the employee should notify Human Resources immediately.

Identification badges are the property of the Company. On a terminating or retiring employees’ last workday, the employee should surrender the identification badge to the supervisor or Human Resources Department.

All visitors and contractors are required to sign in at specified location. They will be required to wear an appropriate visitor or temporary badge and, in most instances, should be escorted to their destination. All visitors and contractors should return the identification badge to the security desk and sign out.

All employees must observe the following rules for identification badges and building security:

- Do not lend your identification badge to anyone;
- Do not allow people to follow you into the building without knowing them or checking their identification;
- Do not hold or prop doors open;
- Do not leave doors open after you leave;
- Notify security if you observe any non-authorized personnel without identification.
E-MAIL AND INTERNET POLICY

E-mail Use Policy

Every employee of the Company who has access to electronic mail is charged with being responsible for using the system properly and in accordance with this policy. Any questions about this policy should be addressed to the Information Technology Department or the Human Resources Department.

The e-mail system is the property of the Company. It has been provided for use in conducting company business. All communications and information transmitted by, received from, or stored in this system are company records and property of the Company.

Employees have no right of personal privacy in any matter stored in, created, received, or sent over the Company mail system including written or electronic mail.

Even though the Company has the right to retrieve and read any e-mail messages, those messages should still be treated as confidential by other employees and accessed only by the intended recipient. Employees are not authorized to retrieve or read any e-mail messages that are not sent to them. Any exception to this policy must receive the prior approval of management.

The Company’s policies against sexual or other harassment apply fully to the e-mail system, and any violation of those policies is grounds for discipline up to and including discharge. Therefore, no e-mail messages should be created, sent, or received if they contain intimidating, hostile, or offensive material concerning race, color, national origin, religion, sex, age, disability, marital status, creed, or any other characteristic or class protected by law.

The e-mail system may not be used to solicit, promote or denigrate religious or political causes, commercial enterprises, outside organizations, or other non-job related solicitations.

The e-mail system shall not be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior authorization from the Company’s management. Employees, if uncertain about whether certain information is copyrighted, proprietary, or otherwise inappropriate for transfer, should resolve all doubts in favor of not transferring the information.

Avoid making disparaging statements in any e-mail record and computer file

Any employee who discovers misuse of the e-mail system should immediately contact the offending employee’s supervisor or Human Resources.

Violations of the Company’s e-mail policy may result in disciplinary action up to and including discharge.

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

Please review the Company’s Policies and Procedures Regarding Security and Use of Company Equipment for further details. This policy may be found on the Company’s intranet or see your local Human Resources Department.

Internet Use Policy

Certain employees may be provided with access to the Internet to assist them in performing their jobs. The Internet can be a valuable source of information and research. Use of the Internet, however, must be tempered with common sense and good judgment.

Although the Company recognizes that the Internet may have useful applications to the Company’s business, employees may not engage in Internet use without prior approval from the most senior officer of the department, and unless a specific business purpose requires such use. Absent such approval, employees may not access the Internet using the Company’s computer systems, at any time or for any reason. “Surfing the Net” is not a legitimate business activity.
If you abuse your right to use the Internet, it will be taken away from you. In addition, you may be subject to disciplinary action, including possible termination, civil and criminal liability.

This policy and the e-mail policy govern your use of the Internet.

**No Expectation of Privacy**

The computers and computer accounts given to employees are to assist them in performance of their jobs. Employees should not have an expectation of privacy in anything they create, store, send, or receive on the computer system. The computer system belongs to the Company and may only be used for business purposes.

**Monitoring Computer Usage**

The Company has the right, but not the duty, to monitor any and all of the aspects of its computer system, including, but not limited to, monitoring sites visited by employees on the Internet, monitoring chat groups and news groups, reviewing material downloaded or uploaded by users to the Internet, and reviewing e-mail sent and received by users.

**Blocking Of Inappropriate Content**

The Company may use software to identify inappropriate or sexually explicit Internet sites. Such sites may be blocked from access by Company networks. In the event you nonetheless encounter inappropriate or sexually explicit material while browsing on the Internet, immediately disconnect from the site, regardless of whether the site was subject to company blocking software.

**Prohibited Activities**

Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful, inappropriate, offensive (including offensive material concerning race, color, national origin, religion, sex, age, disability, marital status, creed, or any other characteristic or class protected by law), or which violates the policies of the Company’s Equal Employment Opportunity policy and its policies against sexual or other harassment may not be downloaded from the Internet or displayed or stored in the Company’s computers. Employees encountering or receiving this kind of material should immediately report the incident to their supervisor or Human Resources. The Company’s Equal Employment Opportunity policy and its policies against sexual or other harassment apply fully to the use of the Internet and any violation of those policies is grounds for discipline up to and including discharge.

Employees may not use the Company’s Internet connection to download games or other entertainment software, including wallpaper and screen savers, or to play games over the Internet.

Employees may not illegally copy material protected under copyright law or make that material available to others for copying. You are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material you wish to download or copy. You may not agree to a license or download any material for which a registration fee is charged without first obtaining the express written permission of your immediate supervisor.

To ensure security and to avoid the spread of computer 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 is strictly prohibited unless the computer you are using is not connected to the Company’s network.

Files obtained from sources outside the Company may contain dangerous computer viruses that may damage the Company’s computer network. These include: 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. Employees should never download files from the Internet, accept e-mail attachments from outsiders, or use disks from non-Company sources, without first seeking approval from Information Technology. Only Information Technology approved software may be loaded. If you suspect that a virus has been introduced into the Company’s network, notify the Help Desk immediately.
This policy may be amended or revised from time to time as the need arises. Users will be provided with copies of all amendments and revisions.

Violations of this policy will be taken seriously and may result in disciplinary action, including possible termination, civil and criminal liability.

Use of the Internet via the Company's computer system constitutes consent by the user to all of the terms and conditions of this policy.

**PERSONAL ELECTRONIC DEVICES**

Managers will determine the appropriate use of personal electronic devices within each department. Employees may be allowed the use of personal electronic devices only with the approval of the department manager.

At the Company’s discretion, the Company may consent to allow certain of its employees direct access to the Company’s email system via the use of electronic mobile devices, including but not limited to cell phones, iPhones, iPads, tablets, and/or laptops. Employees may not access any company system other than the Company’s email system, for any purpose whatsoever, absent express, written authorization from the Company. The Company’s email system contains electronically stored data belonging to the Company, including but not limited to, contacts, calendars, and Company documents in any format. Notwithstanding any decision to allow certain employees access to the Company’s email system, employees shall not be permitted to copy or save any of the Company’s electronically stored data to any electronic mobile device, or transfer such electronically stored data from an electronic mobile device to another electronic device or storage apparatus. Any electronic mobile device used to directly access the Company’s email system must be password-protected.

As a condition to any employee request for direct access to the Company’s email system via a mobile device, the requesting employee must authorize the Company to install software on the device that will allow the Company to “remotely” wipe (i.e., remove) the Company’s electronically stored data from the device in the event that the device is lost or stolen, or in the event the Company is not afforded the opportunity to remove such data from the device due to termination of employment or for any other reason.

Any employee who uses an electronic mobile device, whether company-owned or personal, to gain direct access to the Company’s email system, and thereby obtain electronically stored data belonging to the Company, acknowledges and irrevocably consents to the Company’s accessing any such device for the purpose of monitoring, deleting, or retrieving the Company’s electronically stored data.

In the event of termination of employment, whether voluntary or involuntary, any employee possessing a mobile device that contains any of the Company’s electronically stored data shall deliver each such device to the Company to allow the Company to remove all company data from the device. In the event of the loss or theft of a mobile device containing any of the Company’s electronically stored data, an employee must immediately report such loss or theft to the Company to enable the Company to remotely wipe all such data from the device.

Any employee who uses a mobile device to gain direct access to the Company’s email system acknowledges that the removal of the Company’s electronically stored data may result in the partial or total removal of personal data from said device. By using a mobile device to gain direct access to the Company’s email system, and the Company’s electronically stored data contained therein, each employee waives and releases any and all claims for any loss, damage, or destruction of such mobile device or the personal contents thereon by the Company.
SOCIAL MEDIA POLICY

Torchmark and its affiliates take no position on your decision to start or maintain a blog or participate in other social networking activities. However, it is the right and duty of the Company to protect itself from unauthorized disclosure of information. Torchmark’s social media policy includes rules and guidelines for company-authorized social networking and personal social networking.

General Provisions

Blogging or other forms of social media or technology include but are not limited to video or wiki postings, sites such as Facebook and Twitter, chat rooms, personal blogs or other similar forms of online journals, diaries or personal newsletters not related to any Torchmark Affiliate.

Unless specifically instructed, employees are not authorized, and therefore restricted, to speak on behalf of any Torchmark Affiliate. Employees may not publicly discuss clients, products, employees or any work-related matters, whether confidential or not, outside company-authorized communications. Employees are expected to protect the privacy of Torchmark, its subsidiaries, its employees and clients are prohibited from disclosing personal employee and nonemployee information and any other proprietary and nonpublic information to which employees have access. Such information includes but is not limited to customer information, trade secrets, financial information and strategic business plans.

Employer Monitoring

Employees are cautioned that they should have no expectation of privacy while using the Internet. Your postings can be reviewed by anyone, including your coworkers, department manager, supervisors, and others associated with the Company. Torchmark reserves the right to monitor comments or discussions about the Company, its employees, clients and the industry, including products and competitors, posted on the Internet by anyone, including employees and non-employees. Employees are cautioned that they should have no expectation of privacy while using company equipment or facilities for any purpose, including authorized blogging.

Reporting Violations

The Company requests and strongly urges employees to report any violations, perceived violations or possible violations to supervisors, managers or Human Resources. Violations include discussions of any Torchmark affiliate and its employees and clients, any discussion of proprietary information and any unlawful activity related to blogging or social networking.

Discipline for Violations

The Company investigates and responds to all reports of violations of the social networking policy and other related policies. Violation of the Company’s social media policy will result in disciplinary action up to and including immediate termination. Discipline or termination will be determined based on the nature and factors of any blog or social networking post.

TELEPHONE AND VOICEMAIL POLICY

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 the Company 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. Anyone making personal long distance calls will be required to reimburse the Company. Therefore, the use of calling cards is encouraged.

Cell phones and other personal electronic devices are prohibited from being used in the work area during working hours unless previously approved by the department manager.
Voice Mail Policy

Every employee with access to the voice mail system is responsible for using it properly and in accordance with this policy. Any questions about this policy should be addressed to Information Technology Department or Human Resources Department.

The voice mail system is the property of the Company. It has been provided by the Company for use in conducting company business. All communications and information transmitted by, received from, or stored in this system are company records and property of the Company. The voice mail system is to be used for company purposes only. Use of the voice mail system for personal purposes is prohibited.

Employees have no right of personal privacy in any matter stored in, created, received, or sent over the Company’s voice mail system.

The Company, in its discretion as owner of the voice mail system, reserves and may exercise the right to monitor, access, retrieve, and delete any matter stored in, created, received, or sent over the voice mail system, for any reason without the permission of any employee and without notice.

Even if employees use a password to access the voice mail system, the confidentiality of any message stored in, created, received, or sent from the Company’s voice mail system still cannot be assured. Use of passwords or other security measures does not in any way diminish the Company’s rights to access materials on its system, or create any privacy rights of employees in the messages and files on the system. Any password used by employees must be revealed to the Company as Voice Mail messages may need to be accessed by the Company in an employee’s absence.

The Company’s policies against sexual or other harassment apply fully to the voice mail system, and any violation of those policies is grounds for discipline up to and including discharge. Therefore, no Voice Mail messages should be created, sent, or received if they contain intimidating, hostile, or offensive material concerning race, color, national origin, religion, sex, age, disability, marital status, creed, or any other characteristic or class protected by law.

The voice mail system may not be used to solicit for religious or political causes, commercial enterprises, outside organizations, or other non-job related solicitations.

Users should routinely delete outdated or otherwise unnecessary voice mails. These deletions will help keep the system running smoothly and effectively, as well as minimize maintenance costs.

Employees should also use professional and courteous greetings on their voice mail boxes so as to properly represent the Company to outside callers.

Avoid making any disparaging comment in any voice mail record and message.

Any employee who discovers misuse of the voice mail system should immediately contact Human Resources or Information Technology.

Violations of the Company’s voice mail policy may result in disciplinary action up to and including discharge.

The Company reserves the right to modify this policy at any time, with or without notice.
TELEPHONE SERVICE MONITORING PRACTICES NOTICE TO EMPLOYEES

Call Center representatives who have telephone conversations with consumers either in the incoming or outgoing business lines will be monitored and/or recorded from time to time for training, quality control, and other business purposes. This notice provides information to employees about monitoring and recording practices.

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 employees receive calls on the outside line are not to be used for personal calls by Call Center employees 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. Supervisors who conduct service monitoring should use judgment and disconnect when monitoring an employee’s call that may for any reason seem to be personal or confidential in nature.
I acknowledge that I have received the August 2012 edition of the Company’s Employee Handbook (the “Handbook”). I understand that it is my responsibility to read and comply with the policies contained in this Handbook and any revisions made to it. I agree that if there is any policy or provision in the Handbook that I do not understand, I will seek clarification from Human Resources.

I understand that the Company is an “at will” employer and as such, employment with the Company is not for a fixed term or definite period and may be terminated at the will of either party, with or without cause, and without prior notice. No supervisor or other representative of the Company (except the Chief Executive Officer in consultation with the General Counsel) has the authority to enter into any agreement for employment for any specified period of time, or to make any agreement contrary to the above. In addition, I understand that this Handbook states the Company’s policies and practices in effect on the date of publication.

I understand that nothing contained in the Handbook may be construed as creating a promise of future benefits or a binding contract with the Company for benefits or for any other purpose. I also understand that these policies and procedures are continually evaluated and may be amended, modified or terminated at any time without notice.

Please sign and date this receipt and return it to Human Resources.

Date: _______________________________

Signature: ___________________________

Print Name: __________________________
Message from the Co-Chief Executive Officers

As each of us works to meet individual and Company-wide business goals here at Torchmark, we must all ensure that the work we perform and the business each of us conducts is done with integrity and in accordance with the highest ethical standards. Torchmark and its subsidiaries (the Company) are committed to maintaining a business atmosphere and working environment based on honesty, fair dealing and sound business ethics.

This Code of Conduct expresses the standards of integrity and business conduct that every Company employee, contractor, officer and director must uphold and follow. The Code is being provided to you to help you understand what the Company expects of you and should be read carefully. While this Code cannot address all questionable situations, it provides procedures for you to obtain guidance from your supervisors or the legal department.

Adherence to honesty and integrity in all our actions will only further enhance the Company’s good business reputation and result in benefit to you, the Company, its policyholders and shareholders.

Gary L. Coleman
Co-Chief Executive Officer

Larry M. Hutchison
Co-Chief Executive Officer
Torchmark Corporation
Code of Business Conduct and Ethics
# TABLE OF CONTENTS

- **INTRODUCTION** ................................................................................................................... 1
- **1. COMPLIANCE WITH LAWS, RULES AND REGULATIONS** ............................................ 2
- **2. CONFLICTS OF INTEREST** ............................................................................................ 2
- **3. INSIDER TRADING** .......................................................................................................... 2
- **4. CORPORATE OPPORTUNITIES** ....................................................................................... 3
- **5. COMPETITION AND FAIR DEALING** ............................................................................. 4
- **6. EQUAL EMPLOYMENT OPPORTUNITY** .......................................................................... 4
- **7. HEALTH AND SAFETY** ................................................................................................ 4
- **8. PUBLIC COMPANY REPORTING** ................................................................................... 5
- **9. RECORD-KEEPING** ........................................................................................................ 5
- **10. CONFIDENTIALITY** ...................................................................................................... 5
- **11. PROTECTION AND PROPER USE OF COMPANY ASSETS** ......................................... 6
- **12. PAYMENTS TO GOVERNMENT PERSONNEL** .............................................................. 6
- **13. REPORTING ILLEGAL OR UNETHICAL BEHAVIOR; NON-RETALIATION** ................. 6
- **14. AMENDMENT, MODIFICATION AND WAIVER OF THE CODE** ................................. 7
- **15. COMPLIANCE PROCEDURES** .................................................................................... 7
- **ACKNOWLEDGEMENT OF CODE OF BUSINESS CONDUCT AND ETHICS** ............. 8
Introduction

This Code of Business Conduct and Ethics sets out the guiding principles by which we operate Torchmark and its subsidiaries (the “Company”) and conduct our daily business with our shareholders, policyholders, suppliers, regulatory authorities and with each other. These principles apply to all of the directors, officers, employees and contractors of the Company. Accordingly, this Code has been formally adopted by the Boards of Directors of Torchmark and each of its subsidiaries.

While this Code carries a wide range of business practices and procedures, it does not include all of the policies and procedures of the Company. It does not cover every issue that may arise, but sets out basic principles to guide all employees, officers, directors and contractors of the Company in making sound judgments regarding compliance with the law and ethical business conduct.

It is your responsibility to carefully read this Code and conduct yourself in accordance with it. You should seek to avoid even the appearance of improper behavior. If a law conflicts with a policy in this Code, you must comply with the law. You should seek guidance from your supervisor or the Legal Department if you have any questions about this Code or about a situation in which you are unsure about how to proceed.

Additionally, if you are aware of an event or action that could in any way be a violation of law or this Code, it is your responsibility to report it immediately to your supervisor or the General Counsel or his designee. The Company will investigate the reported violation. Anyone who in good faith reports a possible violation of law, this Code or Company policies will be protected from retaliation. Violations of this Code, including retaliation against an employee who reports a suspected illegal or improper action, will constitute grounds for corrective action, up to and including termination of employment.

After reading this Code, every employee, officer, director and contractor will be asked to execute an acknowledgement that you have received, read and understand your obligation to comply with the principles, policies and laws outlined in the Code.
1. Compliance with Laws, Rules and Regulations

All directors, officers, employees and contractors of the Company are expected to understand, respect and comply, in letter and spirit, with all of the laws, rules and regulations that apply to them in their respective positions at the Company. Although not all such persons are expected to know the details of these laws, rules and regulations, it is important to know enough to determine when to seek additional information, training or advice from supervisors, managers and other appropriate personnel.

2. Conflicts of Interest

All directors, officers, employees and contractors of the Company should be scrupulous in avoiding any action or interest that conflicts or gives the appearance of a conflict with the Company’s interests. A “conflict of interest” exists whenever an individual’s private interests interfere or conflict in any way (or even appear to interfere or conflict) with the interests of the Company. A conflict situation can arise when an employee, officer, director or contractor takes actions or has interests that may make it difficult to perform his or her work for the company objectively and effectively. Conflicts of interest may also arise when a director, officer, employee or contractor or member of his or her family receives improper personal benefits as a result of his or her position with the Company, whether from a third party or from the Company. It is almost always a conflict of interest for a Company employee to work simultaneously for a competitor, customer or service provider. You are not allowed to work for a competitor as a consultant or board member. It is best to avoid any direct or indirect business connection with our customers, service providers or competitors except on the Company’s behalf.

Conflicts of interest are prohibited as a matter of Company policy, except under guidelines approved by the Torchmark Board of Directors in an October 2002 Board resolution. These guidelines also have been separately adopted by the Boards of Directors of Torchmark’s subsidiaries. Pursuant to that resolution, annually all directors, officers and certain employees of Torchmark and its subsidiaries will complete and submit a Conflict of Interest Questionnaire.

Conflicts of interest may not always be clear-cut, so if you have a question you should obtain a copy of the Board resolution from the Legal Department and/or consult with higher levels of management or the Company’s Legal Department. Any employee, officer, director or contractor who becomes aware of a conflict or potential conflict should bring it to the attention of the Legal Department, a supervisor, manager or other appropriate personnel.

3. Insider Trading

Directors, officers, employees and contractors who have access to confidential information are not permitted to use or share that information for stock trading purposes or for any other purpose except the conduct of our business. All non-public information about the Company should be considered confidential information. To use non-public information for personal financial benefit or to “tip” others who might make an investment decision on the basis of this information is not only unethical but also illegal.

In order to assist with compliance with laws against insider trading, the Company has adopted a separate policy governing trading in securities of Torchmark. If you have any questions concerning this policy, you should contact either the General Counsel or the Corporate Secretary.
The following is a summary of the principal terms of the policy:

A. Directors, officers, employees and contractors who know any “material” information about the Company which has not been disclosed (made widely available) to the public (“insider information”) may not buy or sell Torchmark's stock until a reasonable time has passed after the information has been made public. Information is “material” if a reasonable investor would consider it to be important in deciding whether or not to buy, sell or retain Torchmark securities. Examples of material inside information include knowledge of new products; forecasts of revenue or income; unpublished sales; earnings figures; new contracts with customers or suppliers; changes in key personnel; acquisitions; mergers; and sales of businesses.

B. In addition, directors, officers, employees and contractors can be legally liable if someone outside of the Company trades in Torchmark stock based on a “tip” of inside information given by an employee. Company policy forbids giving confidential information about the Company to outsiders except under limited circumstances approved by legal counsel.

C. Specific additional legal restrictions on Torchmark stock trading and transaction reporting apply to corporate directors and certain officers (“Section 16 insiders”), who have been furnished with detailed explanations of these restrictions.

D. Trading in the stock of outside concerns while in possession of material inside information is also prohibited. Examples of material inside information which might be obtained as a result of your position with the Company include proposed acquisitions of outside concerns or awards of important contracts to suppliers of the Company.

Only authorized spokespersons are permitted to disclose material information and to speak on behalf of the Company. If you get calls from the media, investment analysts, stockbrokers, or others looking for information about the Company, you should not answer and direct the call to the Vice President, Investor Relations or his designee.

If you mistakenly disclose or if you discover that someone else has disclosed material nonpublic information about the Company, you must immediately contact the General Counsel.

4. Corporate Opportunities

Employees, officers, directors and contractors are prohibited from taking for themselves personally opportunities that are discovered through the use of corporate property, information or position without the consent of the Board of Directors. No employee, officer, director or contractor may use corporate property, information, or position for personal gain, and no employee, officer, director or contractor may compete with the Company directly or indirectly. Employees, officers, directors and contractors owe a duty to the Company to advance its legitimate interests when the opportunity to do so arises.
5. Competition and Fair Dealing

We seek to outperform our competition fairly and honestly. The Company seeks competitive advantages through superior performance, never through unethical or illegal business practices. Stealing proprietary information, possessing trade secret information that was obtained without the owner’s consent, or inducing such disclosures by past or present employees of other companies is prohibited. You should endeavor to respect the rights of and deal fairly with the Company’s customers, suppliers, competitors and employees. You should not take unfair advantage of anyone through manipulation, concealment, abuse of privileged information, misrepresentation of material facts, or any other intentional unfair-dealing practice.

Business entertainment and gifts in a work-related setting should only be used to create good will and sound working relationships, not to gain an unfair advantage over actual or potential competitors or with customers or suppliers. No gift or entertainment should ever be offered, given, provided or accepted by any Company employee, family member of an employee or agent unless it: (1) is not a cash gift, (2) is consistent with customary business practices, (3) is not excessive in value, (4) cannot be construed as a bribe or payoff and (5) does not violate any laws or regulations. Please discuss with your supervisor any gifts or proposed gifts to give or receive which you are not certain are appropriate.

6. Equal Employment Opportunity

The Company has a policy of equal opportunity with respect to race, sex, marital status, age, color, religion, creed, national origin, handicapped, veteran or other protected status. Consistent with this principle, it is also the Company’s policy not to discriminate in hiring and or promotion based on sexual orientation, gender identity or gender expression. The Company is committed to providing an inclusive and welcoming environment for all members of our community and to ensuring that employment and promotion decisions are based on the individual's abilities and qualifications. The Company is morally and legally committed to give all persons an equal opportunity for employment and promotion based solely on their individual qualifications and the valid requirements of the position. Such a policy ensures that only relevant factors are considered and that equitable and consistent standards of conduct and performance are applied. Additional information on the Company’s employment policies and procedures can be found in your employee handbook or obtained from your Human Resources Department.

7. Health and Safety

The Company strives to provide a safe and healthy work environment. Each of us has a responsibility for maintaining a safe and healthy workplace for everyone by following safety and health rules and practices and reporting accidents, injuries and unsafe equipment, practices or conditions.

Violence and threatening behavior are not permitted. You should report to work in condition to perform your duties, free from the influence of illegal drugs or alcohol. The use of illegal drugs in the workplace will not be tolerated.
8. Public Company Reporting

As a public company, it is of critical importance that Torchmark’s filings with the Securities and Exchange Commission be accurate and timely. Depending on your position with the Company, as an employee, officer, director or contractor, you may be called upon to provide necessary information to assure that the Company’s public reports are complete, fair and understandable. Torchmark expects employees, officers, directors and contractors to take this responsibility very seriously and to provide prompt accurate answers to inquiries related to the Company’s public disclosure requirements. Torchmark will not permit its employees, officers, directors or contractors to improperly influence the audit process or the accuracy of the Company’s financial statements, which are part of the Company’s public reports.

9. Record-Keeping

The Company requires honest and accurate recording and reporting of all information in order to make responsible business decisions. For example, only the true and actual number of hours worked should be reported for compensation purposes and use of business expense accounts should be documented and recorded accurately.

All of the Company’s books, records, accounts and financial statements must be maintained in reasonable detail, must appropriately reflect the Company’s transactions and must conform both to applicable legal requirements and to the Company’s system of internal controls. Unrecorded or “off the books” funds or assets should not be maintained unless permitted by applicable law or regulation.

Business records and communications often become public, and you should avoid exaggeration, derogatory remarks, guesswork, or inappropriate characterizations of people and companies that can be misunderstood. This applies equally to e-mail, internal memos, and formal reports. Records should always be retained or destroyed according to the Company’s record retention policies. In accordance with those policies in the event of litigation or governmental investigation, please consult the Company’s Legal Department.

10. Confidentiality

Directors, officers, employees and contractors must maintain the confidentiality of confidential information entrusted to them by the Company or its suppliers or customers, except when disclosure is specifically authorized by the Legal Department or required by laws, regulations or legal proceedings. Confidential information includes all non-public information that might be of use to our competitors or harmful to the Company, its customers or employees, if disclosed. It also includes information that suppliers and customers have entrusted to us. The obligation to preserve confidential information continues even after employment ends.
11. Protection and Proper Use of Company Assets

All directors, officers, employees and contractors should endeavor to protect the Company's assets and ensure their efficient use. Theft, carelessness, and waste have a direct impact on the Company's profitability. Any suspected incident of fraud or theft should be immediately reported for investigation. Company equipment should not be used for non-Company business, though incidental personal use may be permitted.

Your obligation to protect the Company's assets includes its proprietary information. Proprietary information includes intellectual property such as trade secrets, trademarks and service marks, as well as business, marketing and service plans, databases, records, salary information and any unpublished financial data and reports. Unauthorized use or distribution of this information violates Company policy. It may also be illegal and may result in civil or even criminal penalties.

12. Payments to Government Personnel

The U.S. Foreign Corrupt Practices Act prohibits giving anything of value, directly or indirectly, to officials of foreign governments or foreign political candidates in order to obtain or retain business. It is strictly prohibited to make illegal payments to government officials of any country.

In addition, the U.S. government has a number of laws and regulations regarding business gratuities which may be accepted by U.S. government personnel, as well as gifts or payments to political parties or political candidates. The promise, offer or delivery to an official or employee of the U.S. government of a gift, favor or other gratuity in violation of these rules not only violates Company policy but could also be a criminal offense. State and local governments, as well as foreign governments, may have similar rules. The Company's Legal Department can provide guidance to you in this area.

13. Reporting Illegal or Unethical Behavior; Non-Retaliation

Employees, officers, directors and contractors who suspect or know of violations of this Code or illegal or unethical business or workplace conduct by employees, officers, directors or contractors have an obligation to contact either their supervisor or superiors or the appropriate contact in the Company's Legal Department. If the individual to whom such information is conveyed is not responsive, or if there is reason to believe that reporting to such individuals is inappropriate in particular cases, then the employee, officer, director or contractor may contact the General Counsel of the Company. Such communications will be kept confidential to the extent feasible. If you are still not satisfied with the response, you may contact the Audit Committee of the Board of Directors of the Company by telephoning a toll-free number (1-877-854-0033) that is monitored by an independent, third party reporting service. If concerns or complaints require confidentiality, then this confidentiality will be protected to the extent feasible, subject to applicable law.

You should read the Company's Employee Complaint Procedures for Accounting and Auditing Matters, located on the Torchmark website at the Investor Relations page under Employee Complaint Procedures or obtain a written copy from the Corporate Secretary's Office at Torchmark. It describes the Company's procedures for the receipt, retention and treatment of complaints received by the Company regarding accounting, internal accounting controls or auditing matters. You may submit a good faith concern regarding questionable accounting or auditing matters under this policy without fear of dismissal or retaliation.
The Company prohibits retaliation of any kind against individuals who have made good faith reports or complaints of violations of this Code or other known or suspected illegal or unethical conduct. You are expected to cooperate in internal investigations of misconduct.

14. Amendment, Modification and Waiver of the Code

This Code may be amended or modified by the board of Directors of Torchmark Corporation. Waivers of this Code may only be granted by the Board of Directors or a committee of the Board with specific delegated authority. Waivers will be disclosed to shareholders as required by the Securities and Exchange Act of 1934 and the rules thereunder and the applicable rules of the New York Stock Exchange.

15. Compliance Procedures

We must all work to ensure prompt and consistent action against violations of this Code. However, in some situations it is difficult to know if a violation has occurred.

Since we cannot anticipate every situation that will arise, it is important that we have a way to approach a new question or problem. These are the steps to keep in mind:

- **Make sure you have all the facts.** In order to reach the right solutions, we must be as fully informed as possible.

- **Ask yourself:** What specifically am I being asked to do? Does it seem unethical or improper? This will enable you to focus on the specific question you are faced with, and the alternatives you have. Use your judgment and common sense; if something seems unethical or improper, it probably is.

- **Clarify your responsibility and role.** In most situations, there is shared responsibility. Are your colleagues informed? It may help to get others involved and discuss the problem.

- **Discuss the problem with your supervisor.** This is the basic guidance for all situations. In many cases, your supervisor will be more knowledgeable about the question, and will appreciate being brought into the decision-making process. Remember that it is your supervisor’s responsibility to help solve problems.

- **Seek help from Company resources.** In the rare case where it may not be appropriate to discuss an issue with your supervisor, or where you do not feel comfortable approaching your supervisor with your question, discuss it with your Human Resources manager, the General Counsel or his designee.

- **You may report ethical violations in confidence and without fear of retaliation.** If your situation requires that your identity be kept secret, your anonymity will be protected. The Company does not permit retaliation of any kind against employees for good faith reports of ethical violations.

- **Always ask first, act later.** If you are unsure of what to do in any situation, seek guidance before you act.
Acknowledgement of Code of Business Conduct and Ethics

I acknowledge that I have received and read the Torchmark Corporation Code of Business Conduct and Ethics and understand my obligations as an employee, officer, contractor and/or director of Torchmark and its subsidiaries to comply with the principles, policies and laws outlined in this Code.

If I am an employee of Torchmark or any of its subsidiaries, I understand that my agreement to comply with the Code of Business and Ethics Conduct does not constitute a contract of employment and does nothing to alter my status of “employment at will” with Torchmark or its subsidiaries.

Signature: _____________________________   Date: ________________________________

Please print your name: _______________________________________________________________

Title: ____________________________________    Company: ________________________________

Check:   ☐ Director   ☐ Employee   ☐ Officer   ☐ Contractor
Torchmark Corporation
Information Security Policies
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>COVERED TORCHMARK AFFILIATES</td>
<td>1</td>
</tr>
<tr>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>BUILDING &amp; AREA SECURITY &amp; SYSTEMS</td>
<td>2</td>
</tr>
<tr>
<td>INFORMATION SECURITY RESPONSIBILITIES</td>
<td>3</td>
</tr>
<tr>
<td>INFORMATION SENSITIVITY CLASSIFICATION</td>
<td>5</td>
</tr>
<tr>
<td>ACCESS CONTROL</td>
<td>6</td>
</tr>
<tr>
<td>FIXED PASSWORD MANAGEMENT</td>
<td>8</td>
</tr>
<tr>
<td>PRIVACY</td>
<td>8</td>
</tr>
<tr>
<td>THIRD-PARTY DISCLOSURES</td>
<td>9</td>
</tr>
<tr>
<td>ACCEPTABLE USE OF THE INTERNET</td>
<td>9</td>
</tr>
<tr>
<td>ESTABLISHING NETWORK CONNECTIONS</td>
<td>11</td>
</tr>
<tr>
<td>THIRD-PARTY ACCESS</td>
<td>11</td>
</tr>
<tr>
<td>ENCRYPTION</td>
<td>12</td>
</tr>
<tr>
<td>ELECTRONIC MAIL</td>
<td>12</td>
</tr>
<tr>
<td>PRINTING, COPYING AND FAX TRANSMISSION</td>
<td>14</td>
</tr>
<tr>
<td>MOBILE COMPUTING AND WORK AT HOME</td>
<td>15</td>
</tr>
<tr>
<td>VIRUSES, MALICIOUS SOFTWARE, AND CHANGE CONTROL</td>
<td>17</td>
</tr>
<tr>
<td>USE OF REMOVABLE MEDIA</td>
<td>17</td>
</tr>
<tr>
<td>DISPOSAL OF EQUIPMENT, COMPUTER COMPONENTS &amp; MEDIA</td>
<td>18</td>
</tr>
<tr>
<td>PERSONAL USE OF INFORMATION SYSTEMS</td>
<td>19</td>
</tr>
<tr>
<td>INTELLECTUAL PROPERTY RIGHTS</td>
<td>19</td>
</tr>
<tr>
<td>CORPORATE SOFTWARE POLICY</td>
<td>20</td>
</tr>
<tr>
<td>SYSTEMS DEVELOPMENT</td>
<td>21</td>
</tr>
<tr>
<td>REPORTING PROBLEMS</td>
<td>22</td>
</tr>
<tr>
<td>NON-COMPLIANCE SITUATIONS</td>
<td>22</td>
</tr>
</tbody>
</table>
COVERED TORCHMARK AFFILIATES

American Income Life Insurance Company
First United American Life Insurance Company
Globe Life & Accident Insurance Company
Globe Marketing Services
Liberty National Life Insurance Company
National Income Life Insurance Company
United American Insurance Company
United Investors Life Insurance Company

INTRODUCTION

Purpose

Information is one of the most important assets of our company. Management and employees are responsible for ensuring that company information is complete, accurate, and confidential. Additionally, this information should only be used for authorized business purposes.

All equipment (Servers, Printers, Computers, etc.) and all software, electronic documents, files, and e-mail are property of the company. Security policies and procedures help ensure the protection of company information assets. Unless appropriate measures are taken, information on PCs or terminals can easily be accessed.

Compliance with PC policies and procedures will result in keeping information stored on network computer systems and on employees’ PC hard disks and other storage media secure. Additionally, following policies and procedures in regards to proper e-mail and Internet usage will help prevent abuse and waste of company resources. The policies and procedures contained herein apply to all full-time employees, part-time employees, temporary employees, consultants, and contract labor.

Critical Business Function

Information and information systems are necessary for the performance of just about every essential activity at Torchmark. If there were to be a serious security problem with this information or these information systems, Torchmark Corporation could suffer serious consequences including lost customers, regulatory fines or penalties, customer expenses, litigation, reduced revenues, and degraded reputation. As a result, information security now must be a critical part of the Torchmark Corporation business environment.

Consistent Compliance Essential

A single unauthorized exception to security measures can jeopardize other users, the entire organization, and even outside organizations such as business partners. The interconnected nature of information systems requires that all workers observe a minimum level of security. This document defines that minimum level of due care. Senior Management has decided that the minimum requirements defined in this document are appropriate for all workers at Torchmark Corporation and its affiliates. As a condition of continued employment, all workers, employees, contractors, consultants, and temporaries, must consistently observe the requirements set forth in this document.

Personal Computers and Other Hardware

The following guidelines should be followed regarding PCs and related equipment.

- Never attempt to move a PC or related equipment.
- Never install non-company devices or software.
- Do not set food or liquids on or near your PC.
- Do not place any magnetic items on or near your PC.
Unattended Workstations

Employees must secure their PCs and their workspace when leaving their area by use of the following methods:

- Secure your workstation before walking away, <Ctrl+Alt+Delete> then <Enter> or <Windows key + L>, will lock your machine.
- Lock sensitive documents and computer media in drawers or filing cabinets
- Physically secure laptops with security cables or secure in locked cabinet.
- When leaving for the day, the PC should be “Shut Down”, unless there is a business reason for leaving the PC on, in which case, you must lock the machine with a secured password.

Employee ID

Every Torchmark employee is issued a Picture ID badge. This badge has a dual purpose. It is used to identify Torchmark employees and contains a card key module that allows access to secured doors and areas. Employees should have their badges visible on their person anytime they are in Torchmark facilities. ID badges should never be loaned out or used to allow access to others. If you lose or forget your badge, go to the main entrance, where you can be escorted to HR for a replacement or temporary badge.

Secured Areas & Doors

Restricted areas have been established at the different Torchmark Affiliate Sites. These include Human Resources, Data Centers, File Storage Areas, Maintenance Closets and Wiring Closets. Access to these areas is restricted via Key or ID Badge (card key). If access is required to a restricted area place a request through your authorized approver to HR for the additional access needed. Never prop open doors leading to restricted areas. If you find a restricted area door propped open, please close it and notify Security.

Workspace Clearance

It is crucial to protect sensitive information from disclosure. Office space is frequented by visitors, consultants, vendors, cleaning crews, maintenance and fellow employees. Please keep your workspace neat. If it is messy, you may not notice when something is missing.

Never post sensitive information or documents around you work area. Examples include: User IDs & Passwords, IP addresses, Contracts, Account numbers, Client lists, Intellectual property, Employee/Customer records or anything you wouldn't want disclosed.

At the end of the day, take a moment to tidy up and secure sensitive material, Lock drawers, file cabinets and offices, secure expensive equipment (laptops, PDAs, etc.), and shut down your system to conserve power and the life of the machine.

Visitor Escort

Upon arrival, visitors must sign the visitor log at the security desk and receive a visitor’s badge. Security will phone employees to inform them of a visitor’s presence. All visitors will remain in the waiting area until an escort arrives. Visitors must be escorted at all times. If you need to step away, ensure that someone else accepts responsibility for watching the visitor. This includes escorting visitors back to the security desk. Frequent visitors must not receive special treatment. Instruct visitors to wear their visitor badges so that they can be easily identified. At no time will a visitor be given access to the company network without formal authorization from IT Operations. Never let visitors (or anyone else) borrow your access card. Tours of restricted areas are prohibited without proper authorization. Visits should be confined to normal business hours. If a visitor needs to come in early or leave late, security must be notified, and all other procedures apply. If you see an unescorted person wearing a visitor’s badge, ask “may I help you”. Find out where they are going and make sure they get there. Report any suspicious activity to building security. Never let non-employees into Torchmark Facilities. Simply point them to the main entrance where they can speak with Security.
INFORMATION SECURITY RESPONSIBILITIES

Information Owners

Middle-level managers in user departments must be designated as the Owners of all types of information used for regular business activities. Each type of “production system information” must have an Owner. When information Owners are not clearly implied by organizational design, the Chief Information Officer will make the designation. Information Owners do not legally own the information. They are instead members of the Torchmark Corporation management team who make decisions on behalf of the organization. Information Owners or their delegates must make the following decisions and perform the following activities:

- Approve information-oriented access control privileges for specific job profiles.
- Approve information-oriented access control requests that do not fall within the scope of existing job profiles.
- Select a data retention period for their information, relying on advice from the Legal department.
- Designate an original source for information from which all management reports will be derived.
- Select special controls needed to protect information, such as additional input validation checks or more frequent backup procedures.
- Define acceptable limits on the quality of their information, such as accuracy, timeliness, and time from capture to usage.
- Approve all new and different uses of their information.
- Approve all new or substantially-enhanced application systems that use their information before these systems are moved into production operational status.
- Review reports about system intrusions and other events that are relevant to their information.
- Review and correct reports that indicate the current production uses of their information.
- Review and correct reports that indicate the job profiles that currently have access to their information.
- Select a sensitivity classification category relevant to their information, and review this classification every five years for possible downgrading.
- Select a criticality category relevant to their information so that appropriate contingency planning can be performed.

Information Owners must designate a back-up person to act if they are absent or unavailable. Owners may not delegate ownership responsibilities to third-party organizations such as outsourcing organizations, or to any individual who is not a Torchmark employee. When both the Owner and the Back-up Owner are unavailable, Immediate Owner decisions may be made by the department manager who ordinarily handles the information.

Worker’s Manager

Owners do not approve ordinary access control requests. Instead, a worker’s approved requestor must approve a request for system access based on existing job profiles. If a job profile does not exist, it is the manager’s responsibility to create the profile, obtain the approval of relevant Owners, and inform Information Security. When a worker leaves Torchmark Corporation, it is the responsibility of the worker’s immediate manager to promptly inform Information Security that the privileges associated with the worker’s user ID must be revoked. User IDs are specific to individuals, and must not be reassigned to, or used by, others. Shortly after separation from Torchmark Corporation, a worker’s manager is additionally responsible for reassigning the involved duties and files to other workers.
Information Custodians

Custodians are in physical or logical possession of information and information systems. Like Owners, Custodians are specifically designated for different types of information. In many cases, a manager in the Infrastructure Technology Group will act as the Custodian. If a Custodian is not clear, based on existing information systems operational arrangements, then the Chief Information Officer will designate a Custodian. Custodians follow the instructions of Owners, operate systems on behalf of Owners, but also serve users authorized by Owners. Custodians must define the technical options, such as information criticality categories, and permit Owners to select the appropriate option for their information. Custodians also define information systems architectures and provide technical consulting assistance to Owners so that information systems can be built and run to best meet business objectives. If requested, Custodians additionally provide reports to Owners about information system operations and information security problems. Custodians are responsible for safeguarding the information in their possession, including implementing access control systems to prevent inappropriate disclosure, and developing, documenting, and testing information systems contingency plans.

Information Users

Users are not specifically designated, but are broadly defined as any worker with access to internal information or internal information systems. Users are required to follow all security requirements defined by Owners, implemented by Custodians, or established by Information Security. Users must familiarize themselves with, and act in accordance with, all Torchmark corporate information security requirements. Users also must participate in information security training and awareness efforts. Users must request access from their approved requestor, and report all suspicious activity and security problems.

Information Security

Information Security is the central point of contact for all information security matters at Torchmark Corporation. Acting as internal technical consultants, it is this department’s responsibility to create workable information security solutions that take into consideration the needs of users, Custodians, Owners, and selected third parties. Reflecting these compromises, this department defines information security standards, procedures, policies, and other requirements applicable to the entire organization. Information Security must handle all access control administration activities, monitor the security of Torchmark Corporation information systems, and provide information security training and awareness programs to Torchmark Corporation workers. The department is responsible for periodically providing management with reports about the current state of information security at Torchmark Corporation. While information systems contingency planning is the responsibility of information Custodians, Information Security must provide technical consulting assistance related to emergency response procedures and disaster recovery. Information Security is also responsible for organizing a computer emergency response team to promptly respond to virus infections, hacker break-ins, and similar information security problems.

Internal Audit Department

The Torchmark Corporation Internal Audit department periodically performs compliance checks to ensure that all parties are performing their assigned duties, and to ensure that other information security requirements are being consistently observed. Internal Audit acts as the eyes and ears of Senior Management at Torchmark Corporation, ensuring that internal controls, including those related to information security, are consistent with both Senior Management expectations and organizational goals.
INFORMATION
SENSITIVITY CLASSIFICATION

Reasons For Classification

To assist in the appropriate handling of information, a sensitivity classification hierarchy must be used throughout Torchmark Corporation. This hierarchy provides a shorthand way of referring to sensitivity, and can be used to simplify information security decisions and minimize information security costs. One important intention of a sensitivity classification system is to provide consistent handling of the information, no matter what form it takes, where it goes, or who possesses it. For this reason, it is important to maintain the labels reflecting sensitivity classification categories. Torchmark Corporation uses four sensitivity classification categories:

1. HIGHLY RESTRICTED (SECRET) - This classification label applies to the most sensitive business information that is intended for use strictly within the Company. Its unauthorized disclosure could seriously and adversely impact the Company, its customers, its business partners, and/or its suppliers. Examples may include merger and acquisition documents, corporate level strategic plans, litigation strategy memos, reports on breakthrough new product research, and Trade Secrets.

2. CONFIDENTIAL - This classification label applies to less-sensitive business information that is intended for use within the Company. Its unauthorized disclosure could adversely impact the Company and/or its customers, suppliers, business partners, or employees. Information that some people would consider to be private is included in this classification. Examples may include employee performance evaluations, private customer information (e.g., NPI), customer transaction data, unpublished internally-generated market research, computer passwords, and internal audit reports.

3. FOR INTERNAL USE ONLY - This classification label applies to all other information that does not clearly fit into the previous two classifications. While its unauthorized disclosure is against policy, it is not expected to seriously or adversely impact the Company or its employees, suppliers, business partners, or its customers. Examples may include the Company telephone directory, dial-up computer access numbers, new employee training materials, and internal policy manuals.

4. PUBLIC - This classification applies to information that has been approved by Company management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be disseminated without potential harm. Examples may include product and service brochures, advertisements, job opening announcements, and press releases.

Default Category

If information does not fall into one of these categories, it will default into the Internal Use Only category. If information falls into the Internal Use Only category, it is not necessary to apply a sensitivity label. Information that falls into the Confidential or Secret categories is designated Sensitive.

Labeling

The Owner or creator of information must designate an appropriate label, and the user or recipient of this information must consistently maintain an assigned label. Labels for sensitive information in email can be accomplished either by marking the email message sensitive or by using a label in the subject field of the email message. Labels for sensitive information must appear on the outside of floppy disks, magnetic tape reels, CD-ROMs, audiocassettes, and other storage media. If a storage volume such as a floppy disk contains information with multiple classifications, the most sensitive category should appear on the outside label. Likewise, when creating a collection of information from sources with various classifications, the collection must be classified at the highest sensitivity level of the source information.
Handling Instructions

All users must observe the requirements for handling information based on its sensitivity. Owners may designate additional controls to further restrict access to, or to further protect their information.

Storage

All areas that contain data that has been classified, whether electronic or not, should be kept in secure areas. There should be limited access to these areas and they should be protected by Key or Card Key. These areas should not be in main traffic areas and any guests should be escorted at all times.

ACCESS CONTROL

Access Philosophy

Access to Public and Internal Use Only information is not restricted with access controls that discriminate by specific user. For example, Public information is available at the Torchmark Corporation web site, and Internal Use Only information is available on the Torchmark Corporation intranet. Access to Confidential or Secret information must be granted only when a legitimate business need has been demonstrated and access has been approved in advance by the information Owner. Access to special hardware and software must be restricted based on business need.

Access Approval Process

A worker’s authorized approver must initiate the access control approval process, and the privileges granted remain in effect until the worker’s job changes or the worker leaves Torchmark Corporation. If either of these two events occurs, the manager must notify the Support Technical Operations Center immediately. All non-employees, contractors, consultants, temporaries, and outsourcing organizations must also go through a similar access control request and authorization process initiated by the project manager. The privileges of these non-employees must be immediately revoked by the Support Technical Operations Center when the project is complete, or when the non-employees stop working with Torchmark Corporation.

Default Access

By default, all users must be granted basic information systems services such as electronic mail and word processing facilities. These basic facilities will vary by job title and be determined jointly by Information Security and Support Technical Operations Center. All other system capabilities must be provided through job profiles or by special request directed to the Owner of the involved information. The existence of certain access privileges does not, in and of itself, mean that an individual is authorized to use these privileges. If users have any questions about access control privileges, they must direct these questions to Information Security.

Restricted Access

Access to the Mainframe Systems, PC Network Systems and VPN (Remote Access) will not be routinely provided to all employees. Employees who have a need to use one of these online systems will be granted access with proper management approval. The appropriate request should be completed listing specific transactions or resource needed and approved by the authorized approver for that system or user and then forwarded to the Support Technical Operations Center’s ticketing system. (Refer to Contact Information Matrix at the end of this document).

3rd Party, Business Partners & Vendor Access

Vendors, business partners or 3rd parties will be encouraged to use e-mail or the Secure FTP site for exchanging data. Access to the Secure FTP site is controlled via passwords. In the rare case where a business party will need additional access to the network, the business party will be required to complete a Non-Disclosure Agreement and a Business Associate Agreement with Torchmark and any of the information that they may access while working with Torchmark will be kept confidential and secured in an appropriate system for data type.

Departures From Torchmark Corporation

When a user leaves Torchmark Corporation, all system privileges and access to Torchmark Corporation information must cease immediately. For example, departed users must not be permitted to continue to
maintain an electronic mail account with Torchmark Corporation. At this point, all Torchmark Corporation information disclosed to users must be returned or destroyed. For example, customer contact lists must remain with Torchmark Corporation. All work done by users for Torchmark Corporation is Torchmark Corporation property, and it too must remain with Torchmark Corporation when users depart. For example, a computer program written by a member of the Information Technology department while employed by Torchmark Corporation is Torchmark Corporation property and must remain with Torchmark Corporation. When Human Resources marks any employee record as terminated, Information Systems and Network Support will be notified so that the employee's access to the network and/or mainframe can be removed. At this time a checklist is performed to ensure return of all company assets and removal of all company data from personal equipment including mobile devices, phones and PDA's.

Movement of Employees within the Corporation

Managers must ensure that employees return all phone, computer, software, documentation, and removable media when they leave a department transferring to a different department or affiliate company.

Unique User IDs

Each user must be assigned their own unique user ID. This user ID follows an individual as they move through the organization. It must be permanently decommissioned when a user leaves Torchmark Corporation. Re-use of user IDs is not permitted. Every Torchmark Corporation user ID and related password is intended for the exclusive use of a specific individual. While user IDs can be shared in electronic mail messages and in other places, passwords must never be shared with anyone. Information systems technicians have all the privileges they need to do their job, and must never obtain a user's password. User IDs are linked to specific people, and are not associated with computer terminals, departments, or job titles. With the exception of Internet pages, intranet pages, and other places where anonymous interaction is both generally understood and expected, anonymous and guest user IDs are not permitted unless approved in advance by Information Security.

Privilege Deactivation

After a period of no activity defined in minutes by Information Security, online sessions with multi-user machines must be terminated automatically. Users must be sure to log-off from multi-user computers when they leave their desks for any more than a few minutes. Dormant user IDs on multi-user computers that have no any activity for a period defined in weeks by Information Security must have their privileges automatically revoked and the related files archived. Users who return from an extended vacation or a leave of absence must have their manager contact the Support Technical Operations Center to reestablish their privileges.

User Authentication

All production information system user IDs must have a linked password or a stronger mechanism such as a dynamic password token, to ensure that only the authorized user is able to utilize the user ID. Users are responsible for all activity that takes place with their user ID and password or other authentication mechanism. A user must change their password immediately if they suspect that it has been discovered or used by another person. Users must notify Information Security if other access control mechanisms are broken or if they suspect that these mechanisms have been compromised.
FIXED PASSWORD MANAGEMENT

Choosing Passwords

Users must choose complex passwords. Fixed passwords must not be found in the dictionary and must not be a reflection of the user’s name. All fixed passwords must be at least 6 characters, and this minimum length must be enforced automatically where systems support it. Users must choose fixed passwords that include both Upper and Lower case alphabetic and numeric characters.

Changing Passwords

User-chosen fixed passwords must not be reused or recycled for 3 change periods. Where systems support it, fixed passwords must be required to change every 45 days and passwords must be changed the first time they are used. If a user suspects that somebody else may know his or her password, the password must be changed immediately. The Support Technical Operations Center will not reset user passwords unless a user is identified. Keep in mind that passwords on the network are case sensitive, so if you type a new password in upper and lower case, it must be entered at sign-on in the same upper and lower case pattern. If you forget your password, please reset your password using the self service password reset website.

Protecting Passwords

Users must not share a fixed password with anyone, including managers and co-workers. Users must employ authorized mechanisms to share information such as local server shared directories, electronic mail, intranet pages, or floppy disks. Users must not store fixed passwords in any computer files, such as logon scripts or computer programs, unless the passwords have been encrypted with authorized encryption software. Passwords must not be written down unless a transformation process has concealed them, or they are physically secured, such as placed in a locked file cabinet. All fixed passwords set by default by the hardware or software vendor must be changed before the involved system can be used for Torchmark Corporation business activities.

Passwords are Never to be Used

Use of startup batch and macro files to automatically log on to network/mainframe resources is prohibited. Use of a CMOS password (a password that must be entered for your PC before it will boot) is discouraged; as such a password cannot simply be reset if it is forgotten. This is true for both local workstation and automated batch processing.

PRIVACY

Expectations Of Privacy

Users must have no expectation of privacy when using information systems at Torchmark Corporation. To manage systems and enforce security, Torchmark Corporation may log, review, and otherwise utilize any information stored on or passing through its systems. Torchmark Corporation may capture user activity such as telephone numbers dialed and web sites visited.

Collecting Information

Torchmark Corporation does not collect information that is unnecessary for business purposes. Torchmark Corporation does not collect information from third parties such as customers unless these parties are notified about the collection activities before they occur.

Third-Party Information Privacy

A wide variety of third parties have entrusted their information to Torchmark Corporation for business purposes, and all workers at Torchmark Corporation must do their best to safeguard the privacy and security of this information. Customer account data is Confidential and access must be strictly limited based on business need for such access. Customer account information must not be distributed to third parties without advance authorization by the customer. Exceptions will be made in the case of customer incapacitation or death.
THIRD-PARTY DISCLOSURES

Pre-authorization For Public Statements
All workers who will be delivering speeches, writing papers, or otherwise disclosing information about Torchmark Corporation or its business must obtain preauthorization from the Public Relations department. Only designated individuals are authorized to be spokespersons for Torchmark Corporation. Unless a worker is one of these designated spokespersons, all inquiries from the media must be directed to Public Relations.

Torchmark Corporation Non-Disclosure Agreements
Whenever communications with third parties necessitate the release of sensitive Torchmark information, a standard non-disclosure agreement (NDA) must be signed by the third party. Information released to these third parties must be limited to the topics directly related to the involved project or business relationship, and the disclosure must be approved in advance by the involved information Owner.

Third-Party Non-Disclosure Agreements
In some instances, before discussions can be commenced, third parties must require that workers at Torchmark Corporation sign their non-disclosure agreements (NDAs). Recipients of third-party NDAs must forward these agreements to the Legal department. Third-party NDAs must be signed only by members of the Torchmark Corporation’s Legal department.

ACCEPTABLE USE OF THE INTERNET

Internet Access
Use of the Internet will not be routinely provided to all employees. Employees who have a need to use the Internet will be granted access with proper management approval. The appropriate request should be completed and approved by management for access to the Internet, and forwarded to Network Support.

All Internet usage is recorded and reported on to management. If management suspects inappropriate usage of the Internet, they can request that a detailed report on an employee’s usage

Internet Use
The Internet should be used only for valid business purposes. There are many offensive or inappropriate sites on the Internet, which must be strictly avoided. An employee caught using an inappropriate site faces disciplinary action from the company. Employees should not stay connected to a web site that provides constant or periodic feedback (for example, stock ticker information, ads that update or constant changing content), as this needlessly uses and ties up bandwidth, which could contribute to slower Internet response.

Not A Fringe Benefit
Internet access beyond electronic mail must be provided only if necessary to perform a worker’s job. If a user needs additional access to Internet facilities, a request must be directed to the user’s approved requestor, who must contact the Support Technical Operations Center though it’s automated system.

Information Reliability
All information acquired from the Internet must be considered suspect until confirmed by separate information from another source. Users must not rely on the alleged identity of a correspondent through the Internet unless the identity of this person is confirmed through methods approved by Information Security such as digital certificates or digital signatures.
Posting Information To Public Discussion Groups

Users must not post to public discussion groups, “blogs”, chat rooms, or other public forums on the Internet unless they have been preauthorized by the Public Relations department to make this type of representation on behalf of Torchmark Corporation. Management reserves the right to remove any Internet posting by a worker at Torchmark that it deems inappropriate and potentially damaging to the organization’s reputation.

Setting Up Extra Services

Subscription to real-time automatic information distribution services on the Internet must be approved by the Support Technical Operations Center. Subscription to electronic mail distribution lists is permissible without this approval. The establishment of any network connection with a third party is forbidden unless Information Security has approved the controls associated with this connection. Users must not establish web pages, electronic bulletin boards, or other mechanisms that provide public access to information about Torchmark Corporation without management approval. The establishment of electronic data interchange and other electronic business system arrangements is prohibited unless approved by both corporate management and Network Operations.

User Anonymity

Users must not misrepresent, obscure, suppress, or replace their own or another user’s identity on the Internet or on any other Torchmark information system. In all instances, the user name, electronic mail address, organizational affiliation, and related contact information must reflect the actual originator of a message or posting. The use of anonymous re-mailers or other identity-hiding mechanisms is forbidden. The use of web browsers, anonymous FTP logons, and other methods established with the expectation that users do not need to identify themselves is permissible.

False Security Reports

All users in receipt of information about system vulnerabilities must forward this information to the Support Technical Operations Center who will relay to Information Security, which will determine what action is appropriate. Users must not redistribute system vulnerability information.

Sensitive Information

Users must not send any sensitive information such as credit card numbers, ePHI, telephone calling card numbers, fixed passwords, or customer account numbers through the Internet unless the connection is authorized and encrypted. Users must not include sensitive parameters in electronic mail messages sent through the Internet unless these messages are encrypted with software approved by Information Security. It is not sufficient for a user to employ a virtual private network (VPN) to connect with Torchmark computers, even though the result is that the communications link between a remote computer and Torchmark computers is encrypted. Security parameters must not be sent through electronic mail to outside parties unless end-to-end encryption is employed.

International Transfer Of Data

The movement of private information such as human resources records across international borders in some countries is illegal. Before transferring any private information across a border, users must check with Information Security to ensure that laws are not violated.
ESTABLISHING NETWORK CONNECTIONS

Connection Approval Required

Torchmark Corporation computers or networks may be connected to third-party computers or networks only after Information Security has determined that the combined systems will be in compliance with Torchmark corporate security requirements. Real-time connections between two or more in-house Torchmark Corporation computer systems must not be established unless Information Security has determined that such connections will not jeopardize information security. Connections of internal Torchmark computers to the Torchmark internal network do not require such permissions, unless the involved systems store sensitive information. Connections to the Internet through Torchmark Corporation firewalls do not require such permissions.

VPN / Dial-Up Access

With the exception of approved computers and telecommuting computers, the use of modems directly attached to, or integrated into, personal computers to establish communication sessions with Torchmark Corporation computers or networks is prohibited. All dial-up connections with Torchmark Corporation computers and networks must be routed through a modem pool that includes an extended user authentication security system approved by Information Security.

THIRD-PARTY ACCESS

Written Approval Required

Before third-party users are permitted to reach Torchmark Corporation internal systems through real-time computer connections, specific written approval of the Information Security manager must be obtained. These third parties include information providers such as outsourcing organizations, business partners, contractors, and consultants working on special projects.

Access Restrictions

Third-party information system vendors must be given only in-bound connection privileges when the applicable system manager determines that they have a legitimate business need. These privileges must be enabled only for the time period required to accomplish previously-defined and approved tasks. Third-party vendor access that will last longer than one day must be approved by Information Security.

Only Public Information Posted

Unless the relevant information Owner has approved in advance, workers must not place anything other than Torchmark Corporation public information in a directory, on a server, or in any other location where unknown parties could readily access it.
Third Party Security Requirements

As a condition of gaining access to the Torchmark Corporation computer network, every third party must secure its own connected systems in a manner consistent with Torchmark corporate requirements. Torchmark Corporation must reserve the right to audit the security measures in effect on third party-connected systems without prior warning. Torchmark also must reserve the right to immediately terminate network connections with all third-party systems not meeting such requirements.

Encryption

Default Protection Not Provided

Torchmark Corporation networks and the Internet and other public networks are not protected from wiretapping by default. In all but a few rare instances, if information is to be protected, then the user must take specific action to enable encryption facilities. Users who employ cellular or mobile phones must not discuss Confidential or Secret information unless they have taken steps to encrypt the call. Video conferences must not involve discussion of sensitive information unless encryption facilities are known to be enabled.

When To Use Encryption

Whenever Confidential or Secret information is sent over a public computer network like the Internet, encryption methods authorized by Information Security must be used to protect it. Whenever Secret information is stored in a computer, this storage must be achieved with similar authorized encryption methods.

Key Selection

Many encryption routines require that the user provide a seed or a key as input. Users must protect these security parameters from unauthorized disclosure, just as they would protect passwords from unauthorized disclosure. Rules for choosing strong seeds or keys must follow all rules for choosing strong passwords.

Laptop Computers

All laptop computers are required to have encrypted disks. This is to protect Torchmark in the event the laptop is lost or stolen. The laptop must be configured to encrypt using Torchmark’s Centralized Encryption Solution. This allows us to ensure all sensitive information is encrypted and the ability to prove the laptop is encrypted using our reporting and compliance package.

Electronic Mail

Proper E-Mail Use

E-mail should be used primarily for business correspondence. Employees should limit their use of e-mail for sending personal messages. E-mail can be monitored by management if it is thought an employee is misusing this corporate resource. While employees cannot keep others from sending them junk mail, employees should not forward junk mail, and such mail should be deleted immediately.

Attachments

Use common sense regarding attachments to e-mail. E-mail attachments can contain viruses, take up needed server hard drive space, and consume network bandwidth when they are sent. However, rather than creating a large, long-text e-mail, it is better to create a text document using Word and attach it to an e-mail. This is especially preferable if the document contains sensitive information, since the e-mail can be deleted after the document has been moved to local or network storage.

Mailbox Cleaning

E-mail can quickly accumulate and take up space. Therefore, e-mail should be deleted as soon as it is practical. Any e-mail that should not be deleted should be kept in a directory on the hard drive of the employee’s PC. Email space on our mail server is limited and effort must be taken to stay within assigned limits.
Default Protection

Users must be careful about the inclusion of sensitive information in electronic mail messages that are not protected by encryption. Users must employ encryption facilities approved by Information Security if sending any sensitive information outside the company.

Message Recording

Users are responsible for saving important messages that might be needed at a future date. Electronic mail systems must not be used for message storage. Users must move important messages from electronic mail systems into other storage places such as word processing documents.

Contents Of Messages

Users must not use profanity, obscenities, or derogatory remarks in any electronic mail messages discussing employees, customers, competitors, or others involved with Torchmark Corporation business. Such remarks may create legal problems such as trade libel and defamation of character. Special caution is warranted because backup and archival copies of electronic mail made by third parties may actually be more permanent and more readily accessible than traditional paper communications.

Harassing Or Offensive Messages

Torchmark Corporation information systems must not be used for the exercise of a user’s right to free speech. Sexual, ethnic, and racial harassment, including unwanted telephone calls, electronic mail, and internal mail, is strictly prohibited. Users should reply directly to the originator of offensive electronic mail messages, telephone calls, or other communications asking them to stop. If the originator does not promptly stop sending offensive messages, workers must report the communications to their manager and the Human Resources department.

Examples of acceptable e-mail include the following:

- Business messages.
- Messages about company sponsored events.
- Short personal messages deemed necessary (for example, meeting someone for lunch or after work) when calling or physically visiting would take more time.

Examples of unacceptable e-mail include the following:

- Messages interfering with the normal conduct of business.
- Messages involving solicitation or for-profit business activities.
- Sending chain letters, electronic art, or jokes.
- Long personal messages.

Sharing And Forwarding

Electronic mail accounts, like user IDs, are for specific individuals and must not be shared. If a user goes on vacation or is otherwise unable to check their mail for extended periods, mail can be forwarded to another Torchmark worker. Notices can be established that will automatically inform correspondents that the recipient will not be responding for a certain period of time. Upon departure from Torchmark Corporation, a user’s electronic mail account must be terminated. No forwarding of electronic mail to addresses outside Torchmark Corporation is permitted. If an electronic mail message contains sensitive information, users must not forward it to another recipient unless the other recipient is known to be authorized to view the information, or the originator approves the forwarding. Broadcast electronic mail message facilities must not be employed unless department manager approval is obtained, but the use of selected distribution lists is both advisable and permissible without such approval.

- Business messages.
- Messages about company sponsored events.
Legal Implications

There are legal implications regarding the use of e-mail, in that e-mail and other forms of electronic communications are potentially discoverable in litigation involving the company. Certain words, phrases, and messages, often seemingly harmless in e-mail, could be misinterpreted or lead to accusations of slander, defamation or discrimination. E-mail messages can and have been used as evidence in recent and varied legal cases. When using e-mail, express facts clearly and be careful when expressing opinions. Avoid sending messages laced with anger, humor, or irony, which can easily be misunderstood.

The views expressed in e-mail by individuals are not necessarily the views of the company. Your e-mail address has the name “Torchmark” or a form of your company name in it, so care should be taken as to where you send e-mail. You should not participate in posting information to forums or inappropriate sites where a negative association could be made with the Torchmark name or your company name.

Handling of Sensitive Messages: Sensitive messages should be deleted from your Inbox as soon as possible. Also, any sensitive message you send will remain in your Sent Items folder unless deleted. After deleting messages from either of these folders, they should be purged from your Deleted Items folder as soon as possible, as deleting a message from your Inbox or Sent Items folder does not necessarily mean the message is gone. If you do not delete messages from your Deleted Items folder, they could remain on the E-mail server.

Note: The foregoing is subject to any requests by the Legal Department to retain such information (e.g., Document Preservation Notice.

Corporate Rights: Torchmark does not routinely monitor internal e-mail messages for misconduct. However, managers who suspect an employee is using e-mail in an unacceptable manner can request that the employee’s e-mail be monitored. All email coming into the company is scanned for virus and content.

PRINTING, COPYING AND FAX TRANSMISSION

Destruction Of Waste Copies

If a printer, copier, or fax machine jams or malfunctions when printing Confidential or Secret information, the involved users must not leave the machine until all copies of the sensitive information are removed or are no longer legible. All paper copies of sensitive information must be disposed of by shredding or other methods approved by Information Security.

Faxing Precautions

Sensitive materials must not be faxed unless an authorized staff member is on-hand at the time of transmission to properly handle the materials at the receiving site, the fax is sent to a locked room to which only authorized workers have access, or a password-protected fax mailbox is used to restrict release to an authorized recipient. Sensitive information must not be faxed through un-trusted intermediaries such as hotel staff or rented mailbox service staff. Secret information may be faxed only if the connection is protected with encryption systems approved by Information Security. The receipt of sensitive information by fax must be confirmed promptly. All faxes must employ a standard cover page that includes language approved by the Torchmark Corporation Legal department. If faxing from a multi-functions device make sure any scan copy or image of sensitive documents are erased.

Printer Precautions

When printing sensitive information, the user must be present at the printer at the time of printing to prevent the information from being revealed to unauthorized parties, or direct the output to a printer inside an area where only authorized workers are permitted to go. Do not store images of sensitive documents on internal storage of a printer or multi-function device.
Copy Machine Precautions

Unless permission from the copyright Owner is obtained, making multiple copies of material from magazines, journals, newsletters, and other publications is forbidden unless this is both reasonable and customary.

Repair Services

The repair of fax machines, printers, and copy machines must be performed only by third-party vendors who have signed a Torchmark Corporation non-disclosure agreement.

MOBILE COMPUTING AND WORK AT HOME

Approval For Remote Access

Remote access to Torchmark Corporation computers must be granted only to those users who have a demonstrable business need for such access.

Location Independence

All security requirements apply at remote locations, although they may be implemented in different ways. For example, paper-based Confidential or Secret information must be locked up when not in active use. In Torchmark Corporation offices, a file cabinet might be used, but on the road, a locking briefcase might be employed.

Access Control Packages

All portable and remote computers that are under the control of Torchmark Corporation workers and that are used to process Torchmark Corporation business information must be protected with an access control package approved by Information Security. These access control packages must prevent unauthorized use of the machines and unauthorized access to Torchmark Corporation information. These access control packages must prevent virus infections and other types of damage from malicious software.

Handling Of Sensitive Information

Where possible, sensitive (Confidential or Secret) information should not leave Torchmark Corporation offices. If it is necessary to remove computer-readable sensitive information from Torchmark Corporation offices, this information must be protected with encryption facilities approved by Information Security. If sensitive information is transmitted over public computer networks such as the Internet, this transmission must take place with encryption facilities approved by Information Security. All portable and remote systems storing sensitive Torchmark Corporation information must also employ hard disk encryption systems.

Authentication Of Remote Users

Remote access to Torchmark Corporation computers and networks requires that all users be definitively authenticated with dynamic passwords or other identification systems approved by Information Security. All remote users must connect to Torchmark Corporation computers and internal networks through authorized communications systems such as a firewall. Inbound or outbound connection to Torchmark Corporation computers or networks through an office desktop modem is prohibited unless specific approval has been obtained from Information Security. Leaving modems in auto-answer mode is prohibited.

Theft Of Equipment

If information systems equipment used to handle Torchmark Corporation information is not stored in a locked area, users must employ anti-theft equipment approved by Information Security. Users must not store passwords, user IDs, or any other access information in portable or remote systems. Dynamic password tokens or other access control mechanisms employed for remote access must not be stored in the same case as portable computers.
Remote Office Security

Before approval for working at home or telecommuting is granted, a user's manager must review the security environment of the proposed working environment. If the user works with sensitive information, a shredder must be employed or issued by Torchmark Corporation. If sensitive information will be stored in paper form, locking furniture or a safe must be available or provided by Torchmark Corporation. Users must ensure that their files will be remotely backed-up over the network, or that they will have appropriate remote systems to perform their own backups.

Travel Considerations

Users must be careful not to discuss sensitive information when in public places like hotel lobbies, restaurants, and elevators. Viewing sensitive information on a computer screen or hardcopy report is discouraged when a user is in a public place such as seated on an airplane. Users must be careful not to provide sensitive information in voice mail messages or alphanumeric pager messages.

Mobile Devices

A "Mobile Device" is defined as a PDA, Cellular Phone, Tablet, Smart Phone or any small portable device that can be used to connect into Torchmark systems using over the air technology.

Supported mobile device list contains the OS version of mobile devices that are allowed to connect to Torchmark systems. Additionally, these are devices IT will support in connecting to our systems; not hardware or software phone support. That must be obtained from phone vendor. All mobile devices connecting into corporate resources must be configured to do so using corporate management solution.

Corporate Owned Mobile Devices: Collect phone at time of departure, per Human Resources terminating employee procedures. If phone is lost remote wipe the phone using the corporate management solution.

Non-Corporate Mobile Devices: An agreement must be on file in HR listing corporate rights and proper use rules of any non-company acquired device connecting into Torchmark systems. This signed agreement must be in place before a user can connect a mobile device into company systems. This agreement will specify Torchmark rights to wipe corporate data off of mobile device if phone is lost or stolen.

All users must request access for their mobile device through procurement and IT ticketing systems, as a device license must be obtained. Additionally, depending on mobile device ownership a Mobile Device Agreement must be signed by the user.

Supported Mobile Device Operating Systems: Please contact Tech Operations Center to see if your device is supported by our systems.

Laptops

Laptops are for easy removal from the office, putting them at risk of loss or theft. Always secure laptops to prevent theft or damage. All laptops should be locked up when leaving for the day. Additionally, when traveling with a laptop, keep it with your person at all times, (i.e., carry it onto planes with you). All Home Office laptops should have encryption package installed from Central Corporate Encryption Management Solution.
VIRUSES, MALICIOUS SOFTWARE, AND CHANGE CONTROL

Virus Checking Required

Virus-checking systems approved by Information Security must be in place on all personal computers and servers with operating systems susceptible to viruses, on all firewalls with external network connections, and on all electronic mail servers. All files coming from external sources must be checked before execution or usage. If encryption or data compression has been used, these processes must be reversed before the virus-checking process takes place. Users must not turn off or disable virus-checking systems.

If A Virus Is Detected

If users obtain virus alerts, they must immediately disconnect from all networks and cease further use of the affected computer, and contact the Support Technical Operations Center for technical assistance. Users must not remove viruses on their own. If users believe they may have been the victim of other malicious software, they must immediately contact the Support Technical Operations Center to minimize the damage. User possession or development of viruses or other malicious software is prohibited.

Viruses Avoidance

It is the responsibility of each employee to protect against computer viruses on the network. E-mail should only be opened if it comes from a trusted source and pertains to business. E-mail attachments are particularly dangerous and should only be opened when they are expected. If you have the need to frequently deal with data from outside Torchmark (especially files downloaded from the Internet) then please contact the Support Technical Operations Center and make sure you have anti-virus software loaded on your PC.

Change Control

Users must not install new or upgraded operating systems or application software on personal computers or other machines used to process Torchmark Corporation information. This permits Torchmark Corporation to perform automatic software distribution, automatic software license management, automated remote backup, and related functions on a centralized and coordinated basis. While change control will be maintained through the above-mentioned access control packages, users can, however, change the preferences on software packages, such as the fonts for a word processing package.

USE OF REMOVABLE MEDIA

Removable Media

The following guidelines should be followed regarding removable media (Diskettes, USB External Drives, USB drives, Memory Sticks, CDs or DVDs, etc):

- Handle carefully to prevent damage to data.
- Do not attach paper clips to diskettes.
- Do not expose to magnetic items.
- Store securely so they cannot be removed or copied.

If you are handling diskettes frequently, you may not be effectively using the network environment, such as sharing files over the network or via e-mail. Feel free to contact Network Support to discuss more effective use of the network. Customer information may not be removed from any Torchmark facility unless approved by management and it is logged in and out. For Disposal please see Disposal of Equipment, Computer Components & Media in this document.
**DISPOSAL OF EQUIPMENT, COMPUTER COMPONENTS & MEDIA**

**What is Covered**

Torchmark Corporation will ensure that the master lifecycle inventory system is appropriately updated upon the disposal of equipment, components or media containing sensitive corporate data. Sensitive corporate data consists of customer, employee, private, privileged, financial, health or any information or data deemed not to be public corporate information. This policy covers the following list of equipment, components and media:

- Computer Hard Drive
- Copier
- Memory Sticks
- Network Hard Drive
- Scanner
- MP3 Players
- External Hard Drive
- CDs
- Floppy Disks
- Computers / Servers
- DVDs
- Tapes
- Storage Arrays
- Blue-Rays
- PDAs
- Fax Machine
- USB Drives
- Mobile \ Cell Phones
- Printer
- Thumb Drives

**Corporate Owned Assets**

Torchmark Corporation will ensure that prior to disposal, return or decommission of a company asset containing sensitive corporate data, either the data will be securely overwritten, degaussed or physically destroyed. Also, these actions will be logging and appropriately maintained in a centralized company lifecycle tracking system. It will be the responsibility of IT support personnel to record and kept asset records up to date for purchase, deployment, reuse, destruction and return of company assets and associated actions.

**Returning Equipment**

When returning a hard drive or any equipment that could contain sensitive corporate data for warranty repair or replacement, the internal storage drive must be fully degaussed before shipping back to the manufacturer or vendor representative. Contracts should be put in place with major vendors or directly with the manufacture, that allow Torchmark to degauss any hard drive storage device before returning.

**Sending Offsite**

Items being sent offsite for destruction, such as tapes and hard drives, will be degaussed before leaving the facility. Complete destruction accounting must be received from vendor showing serial or tape number and certificated of destruction. These certificates must be in a form that allows us to tie back the item being destroyed to any associated company asset being tracked in our lifecycle tracking system. Additionally, secure transport of all items must be provided by vendor and stated in a written contract.

**Internal Storage**

When disposing of computer equipment including, but not limited to Servers, Desktop Computers, Storage Arrays, Fax Machines, Printers, Copiers, and Scanners; the internal storage devices that could house sensitive corporate data, must be removed and disposed of in accordance with Torchmark Policy. Additionally, all actions must be recorded in our lifecycle tracking system and associated with the proper asset if applicable.
Removable Media

Single or Multi-use disk media will be destroyed after it has completed its lifecycle. These items can be disposed of by placing in special “Media Only” Security Destruction locked collection bins. This includes Optical or Floppy Disks.

Multi-write memory chip based media containing sensitive corporate data that have reached the end of their lifecycle, will first be degaussed and then physically destroyed before being appropriately disposed of. This includes, but is not limited to USB Drives, Thumb Drives, Memory Sticks, MP3 Players, PDAs, and Mobile Devices. Additionally, this will be recorded in lifecycle tracking system if applicable.

Testing Prohibition

Users must not test or attempt to compromise any information security mechanism unless specifically authorized to do so by Information Security. Users must not possess software or other tools that are designed to compromise information security.

INTELLECTUAL PROPERTY RIGHTS

Legal Ownership

With the exception of material clearly owned by third parties, Torchmark Corporation is the legal owner of all business information stored on or passing through its systems. Unless the Chief Information Officer has signed a specific written agreement, all business-related information developed while a user is employed by Torchmark or its affiliates, is Torchmark Corporate property.

Labeling

In addition to maintaining the labels mentioned in “Information Sensitivity Classification,” users must maintain information about source, date, and usage restrictions for all information provided by third parties. These labels will be important for management decision-making purposes, and will demonstrate that Torchmark Corporation observed appropriate copyright and other intellectual property laws. Users must assume that all materials on the Internet are copyrighted unless specific notice states otherwise.

PERSONAL USE OF INFORMATION SYSTEMS

Personal Use

All user activity is subject to logging and subsequent analysis. Users must not perform any activity on Torchmark Corporation information systems that could damage the reputation of Torchmark Corporation. Unbecoming conduct could lead to disciplinary action including revocation of access control privileges. Incidental personal use of Torchmark Corporation information systems including the telephone is permissible as long as the usage does not interfere with job performance, does not deny other users access to the system resources, and does not incur significant costs. Personal use of Torchmark Corporation information, such as a mailing list, requires the advance approval of the relevant information Owner. Use of software licensed to Torchmark Corporation on a personal computer owned by a user is not authorized unless the system has been designated a system that is used to process Torchmark Corporation information.
CONFIDENTIAL AND PROPRIETARY INFORMATION

When employees store highly restricted, confidential, internal use only or proprietary data, they must follow the guidelines below:

- Information residing on computers, whether a PC, network resource, or the mainframe, and information generated from computers, is proprietary and should not be disclosed to non-company personnel, except with the approval of departmental management.

- Erase highly restricted, confidential, internal use only or proprietary data that is no longer needed. (Subject to any legal request to retain such data)

- Do not store highly restricted, confidential, internal use only or proprietary data on a PC hard drive without controlling access. Controlling access can be achieved by password protecting the data. If necessary, contact the Support Technical Operations Center for assistance.

- Confidential data can also be stored on a secured network directory. Contact the Support Technical Operations Center if you need a secured network directory.

- Backup data on hard disks on a secured network directory regularly.

- Keep removable media containing confidential or proprietary data locked up when not being used.

SECURITY BREACHES

Employees should immediately report any suspected theft of equipment, or breaches of security to their management. Department management should then notify both the Human Resources department and Information Systems Management. Reporting of such breaches will then be handled according to Security Incident Reporting Procedure.

CORPORATE SOFTWARE POLICY

SOFTWARE LICENSES

If a system that is used to process Torchmark Corporate information has been set up by the Infrastructure Technology Group, users can rely on the fact that all software on this system is licensed and authorized. Questions about licensing must be directed to the Support Technical Operations Center, which maintains documentation reflecting software licenses throughout Torchmark Corporation. Making regular backups of software for contingency planning purposes is permissible. All software required to conduct business will be provided to employees by the company. All software used by the company is governed by software license agreements, which set forth contract obligations and restrictions. Therefore, employees must follow the Policy below:

CORPORATE POLICY REGARDING THE USE OF SOFTWARE

Torchmark Affiliates license the use of computer software from a variety of outside companies. The Affiliate does not own this software or its related documentation, and unless authorized by the software developer, does not have the right to reproduce it except for backup purposes.

1. Torchmark Affiliate employees shall use the software only in accordance with the license agreements and will not install unauthorized copies of commercial software.

2. Torchmark Affiliate employees shall not download or upload unauthorized software over the Internet.

3. Torchmark Affiliate employees learning of any misuse of software or Company IT equipment which could be detrimental to the business of the Company shall notify their immediate supervisor.

4. According to applicable copyright law, persons involved in the illegal re-production of software can be subject to civil damages and criminal penalties including fines and imprisonment. Torchmark Affiliates do not condone the illegal duplication of software.

5. Any doubts concerning whether any employee may copy or use a given software program should be raised with a responsible manager before proceeding.

6. The connecting of non-company owned devices into Torchmark systems is not allowed. Therefore, any software used to support and/or connect non-company owned devices with corporate systems,
including workstations, is strictly prohibited.

7. All Torchmark systems, including user workstations, and the files on these systems are the property of Torchmark. This includes all work and non-work related items that can be found on the company system. Items such as email, contacts, pictures, documents, and music found on company systems are legally discoverable and should not be considered private by the user. Torchmark has the right to view any and all information contained on any of its systems at any time.

Guidelines to Responsible Software Use

Only company-approved, licensed software should be used on your PC. Never install personal software from home on a company PC (especially screen savers). Do not download software from the Internet or other sources without approval from Information Systems. This includes Freeware, Trial and licensed software. Never copy software from someone else’s PC to use on your PC. If additional software is needed, complete the appropriate request, obtain your management’s approval and submit the Support Technical Operations Center’s ticketing system. All licenses for software will be kept by Information Technology in a central location.

Software Inventory and Policy Enforcement

All company PCs attached to the network are periodically inventoried automatically by network software so that compliance to the above can be ensured. Additionally, PCs not attached to the network will be audited manually from time to time. If unapproved, unauthorized or illegal software is found on your PC, it will be removed, and your management will be notified. An employee who makes unauthorized copies of software or is caught using unauthorized or illegal software faces disciplinary action from the company up to and including termination.

SYSTEMS DEVELOPMENT

Production System Definition

Information systems that have been designated production systems have special security requirements. A production system is a system that is regularly used to process information critical to Torchmark Corporate business. Although a production system may be physically situated anywhere, the production system designation is assigned by an Information Technology Director.

Special Production System Requirements

All software developed in-house that runs on production systems must be developed according to the Information Technology’s development methodology. This methodology must ensure that the software will be adequately documented and tested before it is used for critical Torchmark Corporation information. This development methodology must ensure that production systems include adequate control measures. Production systems also must have designated Owners and Custodians for the critical information they process. Information Security must perform periodic risk assessments of production systems to determine whether the controls employed are adequate. All production systems must have an access control system to restrict who can access the system and restrict the privileges available to these users. A designated access control administrator who is not a regular user on the system must be assigned for all production systems.

Separation Between Production, Development, And Test Systems

Where resources permit, there must be a separation between the production, development, and test environments. Where these distinctions have been established, development and test staff must not be permitted to have access to production systems. All production software testing must proceed with sanitized information where Confidential or Secret information is replaced with dummy data. All security fixes provided by software vendors must go through the systems development methodology testing.
process, and must be promptly installed. Application programmers must not be given access to production information. A formal and documented change control process must be used to restrict and approve changes to production systems. All application program-based access paths other than the approved user access paths must be deleted or disabled before software is moved into production.

User Programming

Users must not write production computer programs unless specifically authorized by the Chief Information Officer. Spreadsheet formulas, macros, databases or automated reports are not considered programming for purposes of this document. Both users and programmers must be careful never to embed user IDs, readable passwords, encryption keys, or other security parameters in any file.

REPORTING PROBLEMS

What To Report

All workers must promptly report to Information Security any loss of, or severe damage to, their hardware or software. Workers must report all suspected compromises to Torchmark Corporate information systems. All serious information security vulnerabilities known to exist must be reported. All instances of suspected disclosure of Confidential or Secret information also must be reported.

How To Report

Contact the Technical Operations Center. Once it is received and evaluated, it will be passed on to the appropriate group to investigate and act on accordingly.

NON-COMPLIANCE SITUATIONS

Risk Acceptance

Non-compliance with these and other information security requirements can result in disciplinary action up to and including termination. In rare cases, a business case for non-compliance can be established. In all such cases, the non-compliance situation must be approved in advance through a risk acceptance process. This process requires a risk acceptance memo signed by a department manager and approved by Information Security, Information Technology, and Internal Audit departments. Further details on the risk acceptance process can be obtained through Internal Audit.

Enforcement

As mentioned earlier, software on PCs will be periodically inventoried, and e-mail and Internet usage can, and will be monitored if requested by management. Additionally, Internal Audit will periodically conduct audits to insure compliance with the various policies and rules contained herein. If an employee is found to be in violation of company policies or misusing company equipment or property, the employee could face disciplinary actions up to and including termination.