MUTUAL TRUST LIFE INSURANCE COMPANY,
A PAN-AMERICAN LIFE INSURANCE GROUP STOCK COMPANY

PRIVACY PRACTICES AND PROCEDURES
PERSONAL INFORMATION PROTECTION

Effective July 2002

Background *Rev. 11/2018*

Mutual Trust Life Insurance Company, A Pan-American Life Insurance Group Stock Company ("Mutual Trust") has been in business since 1904. During that time, we have had continuous access to the personal information of customers, employees, and agents alike. We have always understood the importance of protecting personal information and have lived up to our commitment to privacy protection for over 100 years.

Privacy is an important issue. We are all concerned about protecting the details of our lives from access by strangers. This concern is heightened when the information involves finances, results of medical tests or other personal matters. The increased interest in safeguarding information can be attributed, in many respects, to the proliferation of e-commerce, the deregulation of the financial services business and the creation of large, multi-purpose financial institutions.

Identify Theft and Social Security Numbers

Among other issues, identity theft has become a major criminal activity. When someone's identity is stolen, the imposter may only act for several hours or the activity could last for years. An enormous hardship can be inflicted during that time. It is for these reasons that Mutual Trust has adopted a corporate Red Flag Policy specifically directed at addressing the issue of identity theft.

Identity theft usually needs a Social Security number linked to a name. For that reason, we take great effort in our organization to keep Social Security numbers confidential as a part of our Privacy protection processes. Specifically, we generally do not include the Social Security number in communications with our clients, unless absolutely necessary and permitted by law. Policy numbers are sufficient for most communications.

Social Security numbers can be linked with a name and address in a number of ways. Problems can arise from stolen or misdirected mail. However, a major problem can also arise when paperwork is discarded since garbage can be <u>legally</u> taken by anyone (since it is discarded property). Thus, identity theft could potentially originate from our premises as a result of the paperwork we discard. In recognition of this, we implemented strict shredding requirements for paperwork disposal as a way of safeguarding against any identity theft activity.

In recognition of the potential for identity theft and all associated issues requiring a heightened sense of security and sensitivity, Mutual Trust has adopted a formal Data Security Policy to enhance ongoing protection efforts of this information.

Procedures

We limit purposeful or inadvertent access to information by our employees. Only employees who have a business reason have access to personal information about our customers, employees or agents. We maintain physical, electronic, and procedural safeguards to protect information.

- *Physical Safeguards:*

    - We operate in a secure environment. Our offices are locked and inaccessible to all but authorized vendors and Mutual Trust personnel. All guests, other vendors, agents and General Agents need to sign in with our receptionist and be accompanied by an employee during their visit to our offices. Employees must never allow a door key or passkey to be used by unauthorized persons.
    - If a passkey is misplaced by an employee, the Office of the Building must immediately be contacted so that the lost passkey can be deactivated and a new passkey issued to the employee. Borrowing/loaning passkeys is not permitted.
    - Employees must take reasonable care to protect the confidentiality of all files, including client, agent, and employee files or similar information in their possession. To that end, we have instituted a detailed Clean Desk Policy as of October 2005 which is included here as an Appendix.

- *Electronic Safeguards:*

    - Employees are allowed access to secure areas on a limited basis.
    - Employees must view only that information necessary to do their jobs.
    - Employees must keep passwords confidential and make them unique.
    - Employees must change passwords every three months.
    - Employees must never allow passwords to be used by unauthorized personnel.
    - Unattended computers will automatically lock up after 15 minutes of nonuse. The authorized operator can log back in easily, but unauthorized personnel are blocked from access.
    - Installed secure messaging with encryption technology which automatically encrypts emails to safeguard sensitive information such as policy numbers, social security numbers, credit card numbers and health information.
    - Installed encryption technology to laptops and any mobile media so as to protect data maintained on these systems.

- *Procedural Safeguards:*

    - No information that is obtained from any Company record should ever be disclosed by an employee to any other person or entity in accordance with our Employee Handbook.

- Care must be taken during telephone service assistance to protect the personal and confidential information of policyholders.
- All sensitive information must be shredded after use. We provide shredding bins in multiple locations so as to promote the use of them.

To assure service providers and contractors also abide by our security measures, we add appropriate material provisions to our contracts with them or ask that they execute Mutual Trust's Confidentiality Agreement as needed so as to make sure that they take the security steps necessary to maintain the confidentiality of the information given to them. In addition, we will require service providers and contractors to properly execute a confidentiality agreement that meets and complies with our mandated security requirements.

Any situation not specifically addressed needs to be handled in a way that remains consistent with our commitment to confidentiality. Questions should be directed to a Manager, John P. Seneczko, Deputy General Counsel, Ext. 5481 or Rod Gross, Internal Audit, Ext. 5366.

Responsible Official

The Deputy General Counsel, John P. Seneczko, at 630-684-5481, also serves as Privacy Officer and is the individual with overall responsibility for implementation of our Privacy initiatives.

Our Privacy Policy is consistently made available to all employees via the HUB, the Company's internal corporate web page used to communicate all policies and procedures. Plus, each employee's manager will emphasize our Privacy requirements during the new employee's training period. Furthermore, our Privacy Policy is made available to all independent producers via the Company's Agent Website.

Audit

Our Audit Department will maintain responsibility for monitoring our practices regarding Privacy. In addition, our Audit Department continually assesses our Privacy Policy in many of the matters it handles throughout the year. Any discrepancies, shortfalls and/or recommendations will be reported to the Privacy Officer.

Disciplinary Action

Mutual Trust requires its employees to follow the Company's written instructions and procedures. Consistent with these requirements, Mutual Trust may impose disciplinary measures for actions that breach these Privacy Practices and Procedures.

Ongoing Oversight

Additional oversight of Privacy related issues, topics, regulations and requirements are provided by the Company's Information Security and Privacy Protection Committee. This Committee is comprised of the Vice President of Internal Audit, the Vice President of Information Systems, the Director of Technical Services, the Systems/Network Administration Manager, the Deputy General Counsel, and the Law Department Paralegal.

APPENDIX

MUTUAL TRUST LIFE INSURANCE COMPANY,
A PAN-AMERICAN LIFE INSURANCE GROUP STOCK COMPANY

Effective October 1, 2005

Policy Title
Clean Desk

Purpose
To establish protection guidelines for sensitive information

Policy
It is the policy of the Company to establish, promote, and maintain a secure work environment and to protect the privacy of our policy owners, beneficiaries, General Agents, registered representatives and employees.

1. Employees are expected to securely safeguard all sensitive information during the normal working hours and at the end of the workday. These items include all correspondence, reports, contracts, and applications that include personal information such as social security number, date of birth, financial data, or personal medical history.

2. Each supervisor has a responsibility to maintain the workplace in a secure manner and provide lockable storage space for sensitive information. This space includes the file drawers and overhead files available in each workstation.

3. Printing of imaged documents should be limited to only those necessary items needed to complete the work assignment and should be placed in the shredder bins provided when no longer needed. Printouts should be removed from printers before leaving the office.

4. Filing cabinets containing records of personal information should be locked. Access arrangements should be established.

5. Periodic monitoring shall be conducted to assure compliance.

Do not use bookshelves to store binders with sensitive information. Procedure documentation that includes samples of live transactions should be edited to remove all information that would violate the privacy of our customers or employees.

When leaving your workstation, appropriate arrangements must be made to prevent unauthorized persons from having access to applications, data media (diskette, hard disk) or to documents, including test documentation.

Do not post sensitive documents: Examples include:

User ID's and Passwords
Contracts
Account Numbers
Client lists
Intellectual property
Employee records
Anything you would not want disclosed